МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова праця
на правах рукопису

ЯРОВЕНКО ГАННА МИКОЛАЇВНА

УДК 330.5:330.3:004.056(043.5)

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ДРАЙВЕР РОЗВИТКУ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

Спеціальність 08.00.03 – Економіка та управління національним господарством

08 – Економічні науки

Подається на здобуття наукового ступеня
доктора економічних наук

Дисертація містить результати власних досліджень.
Використання ідей, результатів і текстів інших
авторів мають посилання на відповідне джерело _____ Г. М. Яровенко

Наукова консультантка:
Кузьменко Ольга Віталіївна
докторка економічних наук, професорка

Суми – 2021

АНОТАЦІЯ

Яровенко Г. М. Інформаційна безпека як драйвер розвитку національної економіки. – Рукопис.

Дисертація на здобуття наукового ступеня доктора економічних наук за спеціальністю 08.00.03 – економіка та управління національним господарством. – Сумський державний університет Міністерства освіти і науки України, Суми, 2021.

Розвиток новітніх інформаційних технологій та цифровізація національної економіки супроводжуються зростанням кіберзлочинності та втратами від інформаційних витоків. Це потребує створення надійної системи інформаційної безпеки на всіх рівнях управління національною економікою не тільки для попередження різного роду кіберзагроз, але й для стимулювання її розвитку. Дана робота була направлена на вирішення таких питань, як обґрунтування сутності та ролі інформаційної безпеки в національній економіці, розробки методології оцінювання та визначення її місця у забезпеченні її розвитку, встановлення причинно-наслідкових зв'язків у дослідженні впливу інформаційної безпеки на збалансованість національної економіки, розвитку прикладного методичного інструментарію підвищення рівня інформаційної безпеки.

У роботі досліджено тенденції розвитку національної економіки у світлі формування цифрового простору, для чого було проаналізовано складові ВВП України за секторами національної економіки. За допомогою поліноміального тренду зроблено прогнози динаміки зміни частки ІТ-сектору окремо у четвертинному секторі та у ВВП України. Це дозволило отримати висновок щодо трансформації національної економіки у напрямку її цифровізації завдяки зростання обсягу ІТ-сектору у 2024 р. до 38 % від четвертинного сектору та 6 % від ВВП. Для порівняння у 2010 р. ці показники становили 19,15 % та 3,06 % відповідно.

Запропоноване власне поняття «інформаційна безпека» з урахуванням її багатокомпонентності та динамічності дозволило сформувати концепцію її

забезпечення в системі управління національною економікою, яка формалізує загрози як передумови порушення цілісності, конфіденційності та доступності об’єктів інформаційної безпеки, визначає суб’єкти, засоби та механізми контролю. Проведений бібліометричний аналіз наукових праць дозволив визначити, що актуальність проблематики інформаційної безпеки зросла тільки за останні 20 років, а також окреслити домінуючи вектори її дослідження в розрізі економічних напрямків: економіка інформаційних систем, інформаційного захисту та інформації; забезпечення конфіденційності персональної інформації; прийняття рішень у сфері інформаційної безпеки; ризики інформаційної безпеки; правове забезпечення інформаційної безпеки; інформаційний менеджмент.

Застосування канонічного аналізу для групи показників цифрової спроможності національної економіки і кібербезпеки та семи груп показників, що характеризують економічний, соціальний та фінансовий розвиток національної економіки, зовнішньо-економічну діяльність, інноваційну активність, якість інформаційної інфраструктури та інституційної спроможності держави дозволило визначити, що найбільший взаємний вплив, який підтверджено статистичною значущістю, здійснюють індекси цифрової спроможності національної економіки і кібербезпеки та інституційної спроможності. Дані результати сприяли розробці інтегрального індексу інформаційної безпеки національної економіки за допомогою методу переваг та функції Харрінгтона-Менчера, а також здійснити рейтинг країн світу за ним. Виявилося, що Україна має задовільний рівень інформаційної безпеки національної економіки.

Проведена кластеризація країн за методом побудови карт Кохонена дозволила сформувати сім груп кластерів, які є найбільш близькими за співвідношенням фактичних рівнів складових інтегрального індексу інформаційної безпеки національної економіки. На основі отриманих результатів кластерного аналізу груп проведено аналіз порівняльної ефективності складових системи інформаційної безпеки національної економіки

за методом DEA-аналізу, який дозволив виявити структурну неефективність субіндексів інтегрального індексу інформаційної безпеки національної економіки для забезпечення його максимального рівня. Для України значення його ефективності становить 63,7%, що є наслідком неефективності блоку показників інституційної спроможності. Їх покращення від 8,91% до 88,57% забезпечить максимальне зростання ефективності інформаційної безпеки національної економіки на 57,04%.

В роботі підтверджено, що існує вплив заходів органів державної влади на наслідки кіберінцидентів та існують залежності між рівнем добробуту, національних суспільних традицій, ментальних та культурних особливостей країни та заходів персональної безпеки, яким надає переваги населення європейських країн. Для емпіричної перевірки цієї гіпотези використано результати моніторингу громадської думки в країнах-членах ЄС, який проводився в межах програми Євробарометр у 2014 та 2019 рр. Інструментарієм дослідження став кластерний аналіз за методом k-means, проведений із використанням аналітичної платформи Deductor Academic.

На основі гравітаційного моделювання було доведено, що на рівень привабливості країн для здійснення легалізації кримінальних доходів впливає й рівень їх інформаційної безпеки. Результати дозволили визначити перелік тих країн, для яких Україна є найбільш привабливою для відмивання коштів, а саме: Кенія, Індія, Гватемала, Гана, Болівія та ін. Для таких країн, як Данія, Естонія, Ісландія, Норвегія, Нова Зеландія та ін., Україна виявилася найменш привабливою для легалізації кримінальних доходів. Отримані результати дозволяють удосконалити регуляторну політику та сприятимуть конвергенції систем кібербезпеки та фінансового моніторингу для підвищення їх функціонування та можливостей попередження операцій з ознаками фінансових кіберзагроз.

Результати моделювання інформаційних активностей, які ідентифікують кіберзагрози в глобальному цифровому середовищі, за допомогою моделі Сєдова-Тейлора довели існування дестабілізаційних впливів інформаційного

середовища на національну економіку країни. Це дозволило визначити кількість бульбашок у світі в трирічній ретроспективі, середню тривалість періоду поширення дезінформації внаслідок глобальних кіберінцидентів, середній період дестабілізації цифрових економічних операцій після розриву бульбашки. Використання запропонованої моделі дозволить прогнозувати інформаційні атаки, а також вчасно виявляти ознаки колапсів в різних секторах економіки.

На основі застосування методів багатоатрибутного прийняття рішень (TOPSIS, VICOR та MAAM) було виявлено для України, що найбільш критичними таргетами інформаційної безпеки є система аналізу та інформації про кіберзагрози, менеджмент кіберкриз, діяльність України щодо її внеску у глобальну кібербезпеку та щодо організації військових кібероперацій. Виходячи з отриманих результатів запропоновано заходи щодо підвищення рівня національної системи інформаційної безпеки: розроблення та впровадження системи збору та аналізу інформації щодо випадків кіберінцидентів, стандартів захисту цифрових послуг, створення спеціальної державної комісії по роботі із міжнародними органами, які займаються питаннями глобальної кібербезпеки, формування спеціальних груп реагування на здійснення масштабних кібератак, розроблення системи попередження інцидентів, тощо.

Проведене обґрунтування пріоритетів формування державних секторальних та галузевих програм у напрямку забезпечення інформаційної безпеки національної економіки, дозволило визначити найбільш вразливі до наслідків кіберзагроз підприємства та встановити економічно доцільний граничний діапазон витрат на інформаційну безпеку. Це дозволило виявити, що найбільш вразливими до кіберінцидентів є малі та середні компанії, які відносяться до сфери сервісних послуг.

Методологія побудови чотириполюсної барицентричної моделі, реалізована в дисертації за допомогою методу центру мас, дозволяє визначати рівень збалансованості економічного, політичного, соціального розвитку та розвитку цифрової спроможності і кібербезпеки країн. Виявлено, що Україна є аутсайдером серед незбалансованих країн, для якої найбільш перспективним

чинником є композитний індикатор цифрової спроможності та кібербезпеки. Також визначено, що високий рівень збалансованості за всіма вимірами розвитку національної економіки можуть досягати країни як із високим, так і з низьким рівнем добробуту, що дозволяє їм бути більш стійкими до внутрішніх та зовнішніх загроз.

Для забезпечення розвитку прикладного методичного інструментарію підвищення рівня інформаційної безпеки запропоновано методику експрес-оцінювання ризиків втрати інформації та даних, яка дозволяє визначати найбільш ймовірні каталізатори інцидентів з урахуванням частоти їх повторення та грошової оцінки збитків від втрати інформації не залежно від суб'єкту інформаційної безпеки. Запропонований у роботі підхід системно-динамічного моделювання дозволяє здійснити симуляцію варіантів реалізації новітніх технологій захисту порівняно з традиційними. Апробація методики для умов упровадження блокчейн-технології в систему інформаційної безпеки дозволила визначити її ефективність за такими параметрами: середнім ризиком невиявлення кіберзагроз побудованою на основі блокчейн-технології системою та рівнем вразливості системи.

Запропоноване авторкою методичне підґрунтя створення прикладної трирівневої системи попередження фінансових і кіберзагроз дозволяє виявляти «вузькі» місця в системі захисту, які є причиною неконтрольованого витоку інформації або втручання кіберзлочинців; проводити ідентифікацію суб'єктів операцій за різними критеріями, що відповідають ознакам кіберзлочинів; ідентифікувати операції за ознаками кіберзлочинів. Апробовані на даних фінансового сектору методики сприяли попередженню фінансових і кіберзагроз.

Ключові слова: національна економіка, інформаційна безпека, збалансованість, розвиток, державна політика, інституційна спроможність, цифрова спроможність, система попередження, кібербезпека, кіберзагроза.

ABSTRACT

Yarovenko H. M. Information Security as a Driver of National Economic Development. – Manuscript.

Dissertation for the Degree of Doctor of Economic Sciences by the specialty 08.00.03 − Economics and Management of a national economy. − Sumy State University, Sumy, 2021.

The development of the latest information technologies and the digitalization of the national economy are accompanied by an increase in cybercrime and losses from information leaks. Thus, the creation of a reliable information security system at all levels of management of the national economy is required to prevent various kinds of cyber threats and stimulate its development. This research was aimed at solving such issues as substantiating the essence and role of information security in the national economy, developing an assessment methodology and determining its place in ensuring the national economic development, establishing cause-and-effect relationships in studying the impact of information security on the balance of the national economy, developing applied methodological tools for increasing the information security.

The tendencies of national economy development in the light of the formation of digital space are investigated in the work for what components of GDP of Ukraine on sectors of the national economy were analysed. Using the polynomial trend, forecasts were made of the dynamics of changes in the share of the IT sector separately in the Quaternary sector and in the GDP of Ukraine. This allowed us to draw a conclusion about the transformation of the national economy in the direction of its digitalization due to the growth of the IT sector in 2024 to 38% of the Quaternary sector and 6% of GDP. For comparison, in 2010 these indicators were 19.15% and 3.06%, respectively.

The suggested concept of “information security”, taking into account its multicomponent and dynamism, made it possible to form the concept of its provision in the national economy management system, which formalizes threats as prerequisites

for violating the integrity, confidentiality, and availability of information security objects, defines the agents, means, and mechanisms of control. The bibliometric analysis of scientific papers allows determining the relevance of information security issues and defining the dominant vectors of its research in the context of economic areas: economics of information systems, information protection and information; ensuring the confidentiality of personal information; decision making in the field of information security; information security risks; legal support of information security; information management.

The use of canonical analysis for a group of indicators of the digital capacity of the national economy and cybersecurity and seven groups of indicators characterizing the economic, social and financial development of the national economy, foreign economic activity, innovative activity, the quality of information infrastructure and the institutional capacity of the state revealed that the digital national economic and cybersecurity capabilities and institutional capacity have the most significant mutual influence. These results contributed to the development of an integral index of information security of the national economy using the method of advantages and the Harrington-Mencher function and to create a rating of the countries according to them. It turned out that Ukraine has a satisfactory level of information security of the national economy.

The clustering of countries by the method of construction of Kohonen maps allowed to form seven groups of clusters that are closest in the ratio of the actual levels of the components of the integrated index of information security of the national economy. Based on the results of cluster analysis of groups, an analysis of the comparative efficiency of the components of the information security system of the national economy by DEA-analysis, which revealed the structural inefficiency of subindexes of the integrated index of information security of the national economy to ensure its maximum level. For Ukraine, the value of its effectiveness is 63.7 %, which is a consequence of the inefficiency of institutional capacity indicators. Their improvement from 8.91 % to 88.57 % will ensure the maximum increase in the efficiency of information security of the national economy by 57.04 %.

The cluster analysis confirmed an influence of measures of public authorities on the consequences of cyber incidents and dependencies between the level of well-being, national social traditions, mental and cultural characteristics of the country, and personal security measures that are preferred by the population of European countries. To empirically test this hypothesis, we used the results of public opinion monitoring in EU member states, which was conducted under the Eurobarometer program in 2014 and 2019. The research tool was cluster analysis using the k-means method, conducted using the analytical platform “Deductor Academic”.

Gravity modelling was used to prove that the level of their information security affects the level of attractiveness of countries for money laundering. The results allowed to determine the list of those countries for which Ukraine is the most attractive for money laundering, namely: Kenya, India, Guatemala, Ghana, Bolivia and others. For countries such as Denmark, Estonia, Iceland, Norway, New Zealand, etc., Ukraine has proved to be the least attractive for money laundering. The obtained results allow to improve the regulatory policy and will promote the convergence of cybersecurity and financial monitoring systems to improve their functioning and the ability to prevent transactions with signs of financial cyber threats.

The results of modelling information activities, which identify cyber threats in the global digital environment, using the Sedova-Taylor model have proven the existence of destabilizing effects of the information environment on the national economy. This allowed us to determine the number of bubbles in the world in three years, the average length of the period of disinformation due to global cyber incidents, the average period of destabilization of digital economic transactions after the rupture of the bubble. The use of the proposed model will allow predicting information attacks, as well as timely detection of signs of collapse in various sectors of the economy.

The multiple attribute decision making methods (TOPSIS, VICOR and MAAM) were used to found that the most critical targets of information security for Ukraine are the system of analysis and information about cyber threats, cyber crisis management, Ukraine’s activities regarding its contribution to global cybersecurity, and the organization of military cyber operations. Based on the results, measures are proposed

to improve the national information security system: development and implementation of a system for collecting and analysing information on cyber incidents, digital service protection standards, creating a special state commission to work with international bodies dealing with global cybersecurity, forming special groups responding to large-scale cyberattacks, developing an incident prevention system, etc.

The justification of the priorities for the formation of state sectoral and industrial programs towards ensuring the information security of the national economy made it possible to identify enterprises that are most vulnerable to the consequences of cyber threats and to establish an economically feasible limit range of costs for information security. This revealed that the most vulnerable to cyber incidents are small and medium-sized companies in the service sector.

The methodology for constructing a four-pole barycentric model implemented in the dissertation using the method of the centre of mass allows determining the level of balance between economic, political, social development and the development of digital capabilities and cybersecurity of countries. Ukraine was found to be an outsider among unbalanced countries, for which the most promising factor is a composite indicator of digital capability and cybersecurity. It is also determined that a high level of balance in all dimensions of national economic development can be achieved by countries with both high and low levels of welfare, which allows them to be more resilient to internal and external threats.

To ensure the development of applied methodological tools for increasing information security, methods are proposed for express assessment of the risks of information and data loss, which can be used to determine the probable catalysts of incidents, taking into account the frequency of their recurrence and the monetary assessment of damage from loss of information, regardless of the information security subjects. The approach of system-dynamic modelling offered in the work allows to carry out simulation of variants of realization of the newest technologies of protection in comparison with traditional. Approbation of the methodology for the conditions of introduction of blockchain technology in the information security system allowed to determine its effectiveness by the following parameters: the average risk of non-

detection of cyber threats based on blockchain technology system and the level of system vulnerability.

The developed method of system dynamics modelling allows substantiating the processes of rebuilding security systems, and its testing for blockchain technology showed its efficiency. The proposed methodology for creating an applied three-tier system for preventing financial and cyber threats allows identifying “bottlenecks” in the protection system that cause uncontrolled information leakage or cybercriminals’ interference; identify the agents of operations according to various criteria corresponding to the elements of cybercrimes; identify operations based on cybercrime elements. The methods tested on financial sector data have helped prevent financial and cyber threats.

Key words: national economy, information security, balance, development, state policy, institutional capacity, digital capacity, warning system, cybersecurity, cyber threat.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ

Монографії:

1. Яровенко Г. М., Бояджян М. М. Оцінка впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері. *Сучасні інструменти боротьби з кібершахрайствами у банках* / за заг. ред. О. В. Кузьменко, Г. М. Яровенко. Суми : Видавництво «Ярославна», 2018. С. 47–61 (0,50 друк. арк.). *Особистий внесок: розроблено методику оцінювання впливу макроекономічних факторів на схильність до фінансових кібершахрайств (0,40 друк. арк.).*

2. Інформаційна система фінансового моніторингу: особливості розробки та реалізації в сучасних умовах протидії легалізації кримінальних доходів / О. В. Кузьменко, Г. М. Яровенко, А. О. Бойко, С. В. Миненко; за заг. ред. О. В. Кузьменко. Суми : Видавництво «Ярославна», 2019. 145 с. (9,9 друк. арк.).

3. Яровенко Г. М. Моделювання та автоматизація обліку, контролю, аудиту. Суми : Видавництво ПП Вінниченко М. Д., ФОП Литовченко Є. Б., 2016. 156 с. (9,07 друк. арк.).

Публікації у наукових фахових виданнях України:

4. Яровенко Г. М. Наслідки інформаційних війн як фактор економічної дестабілізації країни. *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки»* (Index Copernicus та ін.). 2020. № 9 (1). С. 94–103 (0,85 друк. арк.).

5. Yarovenko H., Kuzmenko O., Stumpo M. Strategy for Determining Country Ranking by Level of Cybersecurity. *Financial Markets, Institutions and Risks* (Index Copernicus та ін.). 2020. № 4 (3). P. 124–137 (1,17 друк. арк.). *Особистий внесок: розроблений підхід до реформування системи ІБ України (1,05 друк. арк.).*

6. Yarovenko H., Kuzmenko O., Stumpo M. DEA-Analysis Of The Effectiveness Of The Country's Information Security System. *SocioEconomic Challenges* (Index Copernicus та ін.). 2020. № 4 (3). P. 142–153 (1,04 друк. арк.). *Особистий внесок: проведено оцінювання ресурсного потенціалу ІБ країн (0,94 друк. арк.).*

7. Yarovenko H. Evaluating the threat to national information security. *Problems and Perspectives in Management* (Scopus та ін.). 2020. Vol. 18, Issue 3. P. 195–210 (1,23 друк. арк.).

8. Яровенко Г. М. Бібліометричний аналіз досліджень інформаційної безпеки в розрізі розвитку національної економіки. *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки»* (Index Copernicus та ін.). 2020. № 8 (40). С. 53–63 (0,90 друк. арк.).

9. Яровенко Г. М. Використання карт Кохонена для аналізу рівня інформаційної безпеки країн з урахуванням їх розвитку. *Економічний простір* (Index Copernicus та ін.). 2020. № 157. С. 118–124 (0,73 друк. арк.).

10. 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 (Index Copernicus та ін.). 2020. № 31. С. 160–167 (0,83 друк. арк.).

11. Яровенко Г. М. Вплив рівня економічного розвитку країни на залежність використання персональних засобів інформаційної безпеки та наслідків кібер-злочинів. *Вісник Сумського державного університету. Серія «Економіка»* (Scientific Indexing Services та ін.). 2020. № 1. С. 188–198 (0,87 друк. арк.).

12. Яровенко Г. М., Доценко Т. В., Кушнерьов О. С. Формування інтегрального індексу загрози національної економіки. *Вісник Сумського державного університету. Серія «Економіка»* (Scientific Indexing Services та ін.). 2020. № 2. С. 16–28 (0,93 друк. арк.). *Особистий внесок: обґрунтовано механізм врахування ІБ під час оцінювання загроз НЕ (0,05 друк. арк.).*

13. Яровенко Г. М., Колотіліна О. В. Оцінка ризиків соціо-економіко-політичного розвитку України. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Економіка і управління* (Index Copernicus та ін.). 2020. Т. 31 (70), № 4. С. 151–159 (0,71 друк. арк.). *Особистий внесок: досліджено ризик зменшення ІБ в системі макроекономічних ризиків (0,35 друк. арк.).*

14. Яровенко Г. М., Ковач В. О. Перспективи застосування технології блокчейн в системах забезпечення кібербезпеки банків. *Підприємництво та інновації* (Index Copernicus та ін.). 2020. № 12. С. 206–214 (0,90 друк. арк.). *Особистий внесок: проведено порівняльний аналіз перспектив використання технології блокчейн та штучного інтелекту в системах кіберзахисту (0,45 друк. арк.).*

15. Кузьменко О. В., Бойко А. О., Яровенко Г. М., Доценко Т. В. Сценарії реформування національної системи фінансового моніторингу. *Економіка та держава* (Index Copernicus та ін.). 2020. № 1. С. 9–15 (0,74 друк. арк.). *Особистий внесок: досліджено місце системи забезпечення кібербезпеки в національній системі фінансового моніторингу (0,07 друк. арк.).*

16. Кузьменко О. В., Яровенко Г. М., Бойко А. О., Миненко С. В. Розробка інтерфейсів автоматизованого модуля фінансового моніторингу. *Інвестиції: практика та досвід* (Index Copernicus та ін.). 2020. № 1. С. 11–18 (0,73 друк. арк.). *Особистий внесок: розроблено пропозиції щодо підсилення кіберзахисту в процесі автоматизації фінансового моніторингу (0,65 друк. арк.).*

17. Яровенко Г. М. Тенденції розвитку національної економіки в умовах її цифровізації. *Причорноморські економічні студії* (Index Copernicus та ін.). 2019. № 39, ч. 1. С. 159–164 (0,63 друк. арк.).

18. Lyeonov S., Kuzmenko O., Yarovenko H., Dotsenko T. The Innovative Approach to Increasing Cybersecurity of Transactions Through Counteraction to Money Laundering. *Marketing and Management of Innovations* (Web of Science та ін.). 2019. № 3. P. 308–326 (1,65 друк. арк.). *Особистий внесок: побудовано гравітаційну модель для врахування рівня кібербезпеки країни під час оцінювання її привабливості для відмивання кримінальних доходів (1,25 друк. арк.).*

19. Яровенко Г. М. Аналіз макропоказників, що характеризують рівень складових інформаційної безпеки. *Вісник Хмельницького національного університету*. *Економічні науки* (Index Copernicus). 2019. № 4, т. 3. С. 47–54 (0,79 друк. арк.).

20. Кузьменко О. В., Яровенко Г. М., Левченко В. П., Миненко С. В. Автоматизація процесу фінансового моніторингу легалізації коштів, отриманих незаконним шляхом. *Наукові записки Національного університету «Острозька академія» серія «Економіка»* (Index Copernicus та ін.). 2019. № 43. С. 162–171 (0,97 друк. арк.). *Особистий внесок: розроблено автоматизовану систему кіберзахисту для боротьби з легалізацією коштів (0,25 друк. арк.).*

21. Яровенко Г. М. Аналіз видів загроз та їх наслідків щодо забезпечення інформаційної безпеки держави. *Вісник Хмельницького національного університету*. *Економічні науки* (Index Copernicus). 2018. № 6, т. 3. С. 103–109 (0,87 друк. арк.).

22. Яровенко Г. М. Системний підхід до формалізації поняття «Інформаційна безпека». *Причорноморські економічні студії* (Index Copernicus та ін.). 2018. № 34. С. 239–244 (0,80 друк. арк.).

23. Яровенко Г. М. Розробка інформаційної моделі виявлення ознак шахрайств у банках. *Інвестиції: практика та досвід* (Index Copernicus та ін.). 2018. № 14. С. 23–28 (0,57 друк. арк.).

24. Яровенко Г. М., Сковронська А. І., Бояджян М. М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу. *Ефективна економіка* (WorldCat та ін.). 2018. № 7. URL: http://www.economy. nayka.com.ua/pdf/7_2018/39.pdf (0,61 друк. арк.). *Особистий внесок: розроблено нейромережеву модель виявлення ознак кіберзагроз (0,49 друк. арк.).*

25. Яровенко Г. М., Бояджян М. М. Аналіз наслідків кібершахрайств в банківській системі України. *Економіка та суспільство* (Google Scholar та ін.). 2018. № 18. С. 836–843. URL: http://economyandsociety.in.ua/journals/ 18_ukr/116.pdf (0,54 друк. арк.). *Особистий внесок: проаналізовано макроекономічні наслідки фінансових кібершахрайств (0,43 друк. арк.)*.

26. 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* (Web of Science та ін.). 2018. № 4. P. 221–233 (1,27 друк. арк.). *Особистий внесок: запропоновано методологію побудови чотириполюсної барицентричної моделі (1,02 друк. арк.).*

27. Яровенко Г. М., Ковач В. О. Моделювання портретів потенційних шахрая та жертви банківських шахрайств. *Ефективна економіка* (Index Copernicus та ін.). 2018. № 10. URL: http://www.economy.nayka.com.ua/pdf/ 10_2018/63.pdf (0,65 друк. арк.). *Особистий внесок: розроблено портрет потенційного кібершахрая щодо кредитних операцій (0,33 друк. арк.).*

28. Яровенко Г. М., Коркішко А. В. Моделювання ймовірності виникнення шахрайських операцій з кредитними картками. *Проблеми і перспективи розвитку банківської системи України: збірник наукових праць*.

2015. № 41. С. 237–248 (0,49 друк. арк.). *Особистий внесок: досліджено напрями фінансових кібершахрайств та запропоновано інструменти боротьби з ними (0,39 друк. арк.).*

29. Яровенко Г. М. Автоматизація як перспективний напрям розвитку зовнішнього аудиту. *Інвестиції: практика та досвід* (Index Copernicus та ін.). 2012. № 4. С. 34–38 (0,48 друк. арк.).

30. Яровенко Г. М. Моделювання в бухгалтерському обліку як засіб підвищення ефективності його автоматизації. *Інвестиції: практика та досвід* (Index Copernicus та ін.). 2012. № 6. С. 100–104 (0,58 друк. арк.).

31. Яровенко Г. М., Титаренко А. К. Методи дослідження ринку автоматизованих інформаційних систем. *Ефективна економіка*. 2011. № 6. URL: http:// www.economy.nayka.com.ua/index.php?operation=1&iid=590 (0,42 друк. арк.). *Особистий внесок: проведено кластеризацію сегмента ринку інформаційних систем у межах латерального зрушення (0,34 друк. арк.).*

Публікації в інших наукових виданнях

32. Subeh Musa A., Yarovenko H. Data Mining of Operations with Card Accounts of Bank Clients. *Financial Markets, Institutions and Risks* (Index Copernicus та ін.). 2017. № 1 (4). P. 87–95 (0,58 друк. арк.). *Особистий внесок: розроблено нейромережеву модель виявлення кіберзагроз у транзакціях (0,50 друк. арк.).*

Тези доповідей на наукових конференціях

33. Yarovenko H. Research of relationship between information security and country development factors. *Theoretical and empirical scientific research: concept and trends* : Collection of scientific papers «ΛΌГОΣ» with Proceedings of the International Scientific and Practical Conference, July 24, 2020. Oxford, UK : Oxford Sciences Ltd. & European Scientific Platform, 2020. Vol. 1. P. 37–38 (0,12 друк. арк.).

34. Sadigov M., Kuzmenko O., Yarovenko H. Blockchain technology based system-dynamic simulation modeling of enterprise's cyber security system. *Economic and Social Development* : Book of Proceedings 55th International Scientific Conference on Economic and Social Development Development, 2020. Vol. 1/4. P. 399–408. URL: https://www.esd-conference.com/upload/book_of_proceedings/

Book_of_Proceedings_esdBaku2020_Vol1_Online.pdf (0,75 друк. арк.). *Особистий внесок: розроблено системно-динамічну модель системи ІБ (0,68 друк. арк.).*

35. Leonov S., Yarovenko H., Boiko A., Dotsenko T. Information system for monitoring banking transactions related to money laundering. *CEUR Workshop Proceedings* (Scopus). 2019. Vol. 2422. P. 297–307. URL: http://ceur-ws.org/Vol-2422/paper24.pdf (0,62 друк. арк.). *Особистий внесок: розроблено прототип інформаційної системи фінансового моніторингу (0,45 друк. арк.).*

36. Яровенко Г. М., Нечепоренко І. Д. Сучасні технології кіберзахисту щодо виявлення шахрайств, які здійснюються персоналом банку. *Проблеми та перспективи розвитку фінансово-кредитної системи України* : зб. матеріалів IV Всеукр. наук.-практ. on-line-конф., 21–22 листоп. 2019 р. Суми : Сумський державний університет, 2019. Ч. 2. С. 149–153 (0,17 друк. арк.). *Особистий внесок: проаналізовано технологію машинного навчання для попередження кіберзагроз із боку інсайдерів (0,09 друк. арк.).*

37. Яровенко Г. М. Системний підхід до побудови інформаційної моделі виявлення передумов виникнення шахрайств в банках. *Актуальні проблеми моделювання та управління соціально-економічними системами в умовах глобалізації* : матеріали Міжнар. наук.-практ. конф. Дрогобич, 2018. С. 66–69 (0,15 друк. арк.).

38. Яровенко Г. М., Бояджян М. М. Концептуальна модель виявлення ознак кібершахрайств в банках. *Сучасні міжнародні економічні відносини: становлення та шляхи перспективного розвитку* : зб. тез наук. робіт учасн. Всеукр. наук.-практ. конф., 9–10 лют. 2018 р. Одеса : ЦЕДР, 2018. С. 98–100 (0,14 друк. арк.). *Особистий внесок: сформовано гіпотези ознак кібершахрайств (0,07 друк. арк.).*

39. Яровенко Г. М., Бояджян М. М. Оцінка впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері. *Проблеми та перспективи розвитку фінансово-кредитної системи України* : зб. матеріалів III Всеукр. наук.-практ. on-line-конф., 22–23 листоп. 2018 р. Суми : ННІ БТ «УАБС» СумДУ, 2018. С. 294–297 (0,13 друк. арк.). *Особистий внесок: класифіковано методи кібершахрайств* (0,07 друк. арк.).

40. Яровенко Г. М. Методика визначення витрат на обробку інформації при впровадженні автоматизованої системи управління. *Сучасні шляхи стабілізації економічного стану країни* : матеріали Міжнар. наук.-практ. конф., 1–2 квіт. 2016 р. Дніпро : НО «Перспектива», 2016. Ч. 2. С. 99–101 (0,14 друк. арк.).

41. Яровенко Г. М. Формування інформації для оцінки джерел ефективності використання автоматизованої інформаційної системи підприємства. *Економіка, менеджмент, фінанси: теоретичні та практичні аспекти розвитку* : зб. тез наук. робіт учасн. Міжнар. наук.-практ. конф., 22–23 трав. 2015. Київ : Аналітичний центр «Нова Економіка». 2015. Ч. 2. С. 101–102 (0,14 друк. арк.).

42. Яровенко Г. М. Метод оцінки економічної ефективності автоматизованих інформаційних систем на основі статистики результатів впроваджень. *Формування фінансової системи в умовах глобалізації* : XXIV Міжнар. наук.-практ. конф., 9–10 серп. 2013 р. Київ, 2013. С. 71–74 (0,21 друк. арк.).

43. Яровенко Г. М. Використання математичних методів та моделей у забезпеченні ефективності корпоративних інформаційних систем. *Актуальні проблеми теорії та практики менеджменту* : зб. матеріалів Міжнар. наук.-практ. конф., 16–17 серп. 2013 р. Сімферополь, 2013. С. 92–94 (0,21 друк. арк.).

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Четверта промислова революція впродовж останнього десятиліття сприяла стрімкому розвитку новітніх інформаційних технологій та цифровізації національної економіки. У той самий час ці процеси супроводжуються зростанням кіберзлочинності та втратами від інформаційних витоків. У світовому масштабі ці втрати за 2014–2017 рр. зросли з 500 млрд дол. до 600 млрд дол. (із 0,7 % до 0,8 % від світового ВВП), а у 2021 р., за прогнозами, досягнуть 6 трлн дол. Таким чином, підтримання інформаційної безпеки на належному рівні перетворюється у сучасних умовах на один із найважливіших чинників захисту національного фінансово-економічного суверенітету, посилення конкурентоспроможності національної економіки на світовому рівні та драйвера розвитку національного господарства.

Обґрунтування ролі та місця інформаційної безпеки в системі управління національним господарством закладене в працях таких зарубіжних учених: Р. Андерсона, К. Веня, Л. Гордона, М. Гупти, Л. Кардгольма, Н. Кшетрі, Дж. Лі, М. Лоєба, Т. Мура, А. Сінгха, З. Сонні, Г. Стефанідеса, М. Столла, Т. Цякіса, Ю. Ши та ін. Це питання досліджували й вітчизняні вчені, зокрема, В. Бабенко, А. Бойко, Т. Васильєва, Г. Гайдур, І. Гонтарева, Р. Грищук, Т. Затонацька, А. Качинський, С. Лєонов, О. Кузьменко, В. Маргасова, С. Онищенко, Т. Полозова, О. Сороківська, В. Хаустова та ін.

Аналіз наукового доробку з проблематики дослідження засвідчив, що потребує остаточного вирішення низка питань щодо уточнення сутності інформаційної безпеки, методології її оцінювання, визначення її місця в забезпеченні збалансованості розвитку національної економіки, ефективності системи її забезпечення, розроблення механізмів її підвищення, тощо. Відсутність системного розуміння ролі інформаційної безпеки як драйвера розвитку національної економіки обумовили актуальність дослідження, його мету, завдання та зміст.

Зв’язок роботи з науковими програмами, планами, темами. Тема дисертації узгоджується з положеннями «Стратегії кібербезпеки ЄС на цифрове десятиліття» (схвалена Єврокомісією 16.12.2020 р.), Стратегічного порядку денного ЄС «Витоки Стратегічної програми ЄС на 2019–2024 рр.: майбутнє дебатів Європи та Європейської ради в Сібіу» (схвалений Радою Європи 20.06.2019 р.), Стратегії національної безпеки України (затверджена Указом Президента України № 392/2020 від 14.09.2020 р.), Доктрини інформаційної безпеки України (затверджена Указом Президента України № 47/2017 від 25.02.2017 р.), Стратегії кібербезпеки України (затверджена Указом Президента України № 96/2016 від 15.03.2016 р.), ін.

Робота відповідає пріоритетним напрямкам наукових досліджень Сумського державного університету. Так, зокрема, до звіту за темою «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України» (номер д/р 0118U003574) ввійшли пропозиції щодо моделювання впливу макроекономічних факторів на формування схильності до фінансових шахрайств; за темою «Сучасні інформаційні технології в соціально-економічних системах» (номер д/р 0116U000930) – щодо дослідження галузевої структури національної економіки за ризиком кібершахрайств, а також обґрунтування атракторів боротьби з ними; за темою «Моделювання сталого розвитку складних соціально-економічних систем» (номер д/р 0116U000929) – щодо структуризації найпоширеніших кіберзагроз; за грантом Президента України на тему «Розробка прототипу автоматизованого модуля фінансового моніторингу діяльності економічних агентів для протидії легалізації кримінальних доходів» (номер д/р 0119U103189) – щодо гравітаційного моделювання ризику легалізації кримінальних доходів у національній економіці.

Мета і завдання дослідження. Метою дослідження є розроблення нових та вдосконалення існуючих методологічних підходів і методичного інструментарію формування ефективної системи інформаційної безпеки з урахуванням її впливу на розвиток національної економіки в цілому та її окремих секторів.

Поставлена мета зумовила необхідність вирішення таких завдань:

– уточнити змістовну сутність інформаційної безпеки та сформувати

концептуальну модель її забезпечення в системі управління національною економікою;

– поглибити структуризацію наукового доробку щодо напрямів дослідження інформаційної безпеки як драйвера розвитку інформаційної безпеки національної економіки;

– сформувати склад показників для оцінювання рівня інформаційної безпеки національної економіки шляхом канонічного аналізу взаємного впливу індикаторів розвитку та інформатизації національної економіки;

– розробити методологію інтегрального оцінювання рівня інформаційної безпеки національної економіки;

– розробити методологію аналізу ефективності функціонування системи інформаційної безпеки національної економіки;

– дослідити залежність національних патернів забезпечення інформаційної безпеки населення від рівня економічного розвитку країни та суспільних традицій;

– обґрунтувати вплив рівня кібербезпеки країни на її привабливість для легалізації кримінальних доходів;

– визначити часові характеристики впливу «інформаційних бульбашок» на функціонування глобального цифрового економічного простору;

– вдосконалити методологічні засади обґрунтування таргетів та напрямків реформування системи забезпечення інформаційної безпеки в Україні;

– поглибити методологію обґрунтування пріоритетів формування державних секторальних і галузевих програм у напрямку забезпечення інформаційної безпеки національної економіки;

– розробити методологію визначення ролі цифрової спроможності та кібербезпеки країни щодо забезпечення збалансованості розвитку національної економіки;

– поглибити методичні засади експрес-оцінювання ризиків втрати інформації;

– на засадах системно-динамічного імітаційного моделювання поглибити підхід до вибору найбільш ефективної системи захисту інформації;

– запропонувати трирівневу систему попередження фінансових кіберзагроз.

Об'єктом дослідження є економічні відносини, що виникають між органами державної влади, місцевого врядування, суб'єктами господарювання та домогосподарствами в процесі забезпечення інформаційної безпеки та здійснення регуляторних інтервенцій щодо підвищення її ефективності.

Предметом дослідження є науково-методологічні засади та методичний інструментарій реалізації державної політики забезпечення інформаційної безпеки як елемента системи управління національною економікою.

Методи дослідження. Методологічну базу дослідження складають фундаментальні положення економічної теорії, макро- і мікроекономіки, теорії стратегічного управління, державного регулювання економіки, економіко-математичного моделювання, наукові праці з питань інформаційної безпеки та управління національною економікою.

Відповідно до визначених завдань використано такі методи дослідження: логічне узагальнення та групування, наукову абстракцію – під час визначення тенденцій розвитку національної економіки у світлі формування цифрового суспільства; системний аналіз – при уточненні сутності інформаційної безпеки та розробленні концепції її забезпечення в системі управління національною економікою; динамічний та бібліометричний аналізи – під час дослідження наукового доробку щодо ролі та місця інформаційної безпеки в економічній системі; кореляційний аналіз – під час обґрунтування впливу інформаційної безпеки країни на ймовірність її використання в незаконних операціях; канонічний аналіз – під час обґрунтування взаємного впливу показників розвитку національної економіки, цифрової спроможності та кібербезпеки країни; кластерний аналіз методом k-means – під час дослідження закономірностей формування в національній економіці домінуючих моделей забезпечення персональної інформаційної безпеки населення; метод побудови карт Кохонена – під час визначення груп країн, близьких за рівнем інформаційної безпеки національної економіки; метод переваг та функція Харрінгтона – Менчера – під час інтегрального оцінювання інформаційної безпеки національної економіки; DEA-

аналіз – під час визначення порівняльної ефективності складових системи інформаційної безпеки національної економіки; метод головних компонент – при визначенні вагів індикаторів під час проведення DEA-аналізу; модель Сєдова – Тейлора – для ідентифікації часових характеристик реакцій економічних агентів у глобальному цифровому економічному просторі на розриви «інформаційних бульбашок»; метод визначення центра мас – під час розроблення чотириполюсної барицентричної моделі збалансованості розвитку національної економіки; гравітаційне моделювання – при доведенні впливу рівня інформаційної безпеки на привабливість країн для легалізації кримінальних доходів; BPMN-моделювання – в процесі оптимізації бізнес-процесів забезпечення інформаційної безпеки; дерева рішень – під час побудови портретів кібершахрая та жертви; нейромережеве моделювання – під час розроблення інструментарію виявлення ознак кіберзагроз; бінарне оцінювання – під час експрес-оцінювання ризиків втрати інформації; системно-динамічне моделювання – при виборі найбільш ефективних програмно-технологічних рішень для захисту інформації; методи багатокритеріального прийняття рішення VICOR, TOPSIS, MAAM – під час обґрунтування таргетів та напрямків реформування системи забезпечення інформаційної безпеки в Україні. Розрахунки здійснено з використанням програмних продуктів STATISTICA 10, Deductor Academic, MS Excel, Mathcad; імітаційно-симуляційні експерименти – за допомогою платформ Vensim, Bizagi Modeler; аналітичне зіставлення – Global Web Statistics; динамічний аналіз – Scopus Citation Overview Tool, Dimensions Tool; бібліометричний аналіз – інструментарію VOSviewer v. 1.6.10; геометричну інтерпретацію барицентричної моделі – програми GeoGebra.

Інформаційно-фактологічну базу дослідження сформували закони України, укази Президента України, нормативно-правова база профільних міністерств та відомств, звітно-аналітична інформація Державної служби статистики України; дані Світового банку, Євростату, Global Web Statistics “Statoperator”; аналітичні огляди міжнародних рейтингових агенцій Deloitte, IBM, e-Governance Academy, International Telecommunication Union, Ponemon Institute та ін.; внутрішня документація банків і підприємств; результати наукових досліджень.

Наукова новизна одержаних результатів полягає в розробленні нових та вдосконаленні існуючих методологічних підходів і методичного інструментарію формування ефективної системи інформаційної безпеки з урахуванням її впливу на розвиток національної економіки в цілому та її окремих секторів.

Найбільш вагомими науковими результатами дослідження є такі:

вперше:

– розроблено методологію інтегрального оцінювання інформаційної безпеки національної економіки шляхом системного поєднання за допомогою методу переваг та функції Харрінгтона – Менчера індикаторів інституційної та цифрової спроможності національної економіки, а також кібербезпеки. Це дозволило сформувати рейтинг країн світу за інтегральним рівнем інформаційної безпеки національної економіки та окреслити таргети реалізації державної політики України для її підвищення;

– запропоновано методологію аналізу порівняльної ефективності складових системи забезпечення інформаційної безпеки національної економіки шляхом комбінації кластерного аналізу (на основі карт Кохонена) та методу лінійного непараметричного програмування DEA (на основі Input- і Output-oriented CCR-моделей). Це дозволило визначити максимальний рівень ефективності функціонування системи інформаційної безпеки, якого може досягти країна за наявного потенціалу, а також прихованих резервів його забезпечення;

– на основі системного поєднання інструментарію Global Web Statistics та моделі Сєдова – Тейлора описано часові характеристики реакції економічних агентів у глобальному цифровому економічному просторі на розриви «інформаційних бульбашок» (паразитарних інформаційних вкидів, несанкціонованих витоків інформації, масштабних хакерських атак тощо). Це дозволило визначити кількість бульбашок у світі в трирічній ретроспективі, середню тривалість періоду поширення дезінформації внаслідок глобальних кіберінцидентів, середній період дестабілізації цифрових економічних операцій після розриву бульбашки;

– розроблено чотириполюсну барицентричну модель (із використанням методу визначення центра мас) для визначення рівня збалансованості розвитку національної економіки, що інтегрує композитні індикатори економічного, соціального й політичного розвитку країни, а також рівня її цифрової спроможності та кібербезпеки. Це дозволило проранжувати країни світу за рівнем збалансованості їх розвитку за розривами між розрахунковими та еталонними значеннями центрів мас як за окремим індикатором розвитку національної економіки, так і за інтегральним рівнем центра мас у моделі, а для України – окреслити напрямки реалізації державної політики для підвищення збалансованості розвитку національної економіки;

вдосконалено:

– методологічний базис обґрунтування взаємного впливу індикаторів розвитку НЕ та інформатизації в країні, що відрізняється від існуючих застосуванням канонічного аналізу за групами показників цифрової спроможності національної економіки і кібербезпеки, економічного, соціального й фінансового розвитку національної економіки, зовнішньо–економічної діяльності, інноваційної активності, якості інформаційної інфраструктури, інституційної спроможності держави. Це дозволило сформувати перелік релевантних індикаторів інтегрального оцінювання інформаційної безпеки національної економіки та визначити пріоритети в реалізації державної політики її підвищення;

– методологічний базис дослідження закономірностей формування в національній економіці домінуючих моделей забезпечення персональної інформаційної безпеки населення, що відрізняється від існуючих застосуванням кластерного аналізу та дозволило підтвердити гіпотезу, що здійснювана державою політика підвищення інформаційної грамотності та інклюзії населення формує стійкі національні патерни заходів забезпечення персональної інформаційної безпеки і наслідків її порушення, які залежать від рівня економічного розвитку країни та історично сформованих суспільних традицій;

– методологію обґрунтування впливу інформаційної безпеки на

привабливість країни для легалізації кримінальних доходів, що відрізняється від існуючих системним поєднанням гравітаційного моделювання та методу експертного оцінювання для формалізації зв'язку між рівнем кібербезпеки країни і рівнем її привабливості для використання економічними агентами в процесах легалізації незаконно отриманих коштів та відмивання брудних грошей. Це формує наукове підґрунтя для коригування заходів реалізації державної політики боротьби з тінізацією національної економіки та вдосконалення вітчизняної системи державного фінансового моніторингу;

– методологічні засади обґрунтування таргетів та напрямків реформування системи забезпечення інформаційної безпеки в Україні, що на відміну від існуючих здійснене шляхом визначення методами багатоатрибутного прийняття рішення (VIKOR, TOPSIS, MAAM) розривів між фактичними й еталонними значеннями основних параметрів національного індексу кібербезпеки. Це дозволило визначити критично необхідні напрямки регуляторних інтервенцій та встановити кількісні орієнтири для реалізації заходів державної політики забезпечення інформаційної безпеки національної економіки;

– методологію обґрунтування пріоритетів формування державних секторальних та галузевих програм у напрямку забезпечення інформаційної безпеки національної економіки, що на відміну від існуючих здійснено шляхом визначення середнього рівня втрат від внутрішніх і зовнішніх кіберзагроз на одного працівника залежно від розміру компаній, а також для компаній різної галузевої належності – граничний діапазон витрат на інформаційну безпеку, додержання якого є економічно доцільним. Це дозволило емпірично встановити, що у фокусі підвищеної державної уваги в разі забезпечення інформаційної безпеки національної економіки повинні перебувати суб'єкти малого та середнього бізнесу, передусім із сфери послуг, а також розробити систему державних регуляторних заходів із стандартизації та сертифікації, контролю і моніторингу для підвищення рівнів їх кібербезпеки;

набули подальшого розвитку:

– розуміння сутності поняття «інформаційна безпека», що відрізняється від існуючих її трактуванням як складної багатокомпонентної та динамічної системи, яка комплексно враховує мету її функціонування, суб'єктно-об'єктну узгодженість інструментів і механізмів впливу з урахуванням специфіки структури національної економіки. Це дозволило розробити концепцію забезпечення інформаційної безпеки в системі управління національною економікою, що формалізує зовнішні та внутрішні загрози як передумови порушення цілісності, конфіденційності й доступності об'єктів інформаційної безпеки, визначити суб'єкти, засоби і механізми контролю, обґрунтувати системно-структурні взаємозв'язки між наслідками забезпечення інформаційної безпеки для розвитку національної економіки в цілому та окремих її секторів;

– теоретичні основи структуризації наукового доробку щодо напрямів дослідження інформаційної безпеки як драйвера розвитку національної економіки, що відрізняється від існуючих системним поєднанням динамічного (Scopus Citation Overview Tool, Dimensions Tool) та бібліометричного (VOSviewer v. 1.6.10) аналізів і дозволило визначити домінуючі вектори досліджень та побудувати мережеву карту за актуальністю напрацювань науковців у розрізі предметних галузей економічного напрямку;

– методичні засади експрес-оцінювання ризиків втрати інформації, що відрізняються від існуючих побудовою за матричним принципом карти ризиків, у яких на засадах теорії ймовірності та теорії множин зіставлено грошову оцінку збитків від втрати інформації й частоту повторення інцидентів, обумовлених діями персоналу, вірусними атаками, технічними несправностями, незаконними діями кіберзлочинців, некоректною роботою програмного забезпечення. Це дозволило визначити найбільш релевантні каталізатори інцидентів, пов'язаних із втратою інформації, критичні місця та слабкі зони в системі забезпечення інформаційної безпеки;

– науково-методичний підхід до вибору найбільш ефективних програмно-технологічних рішень для захисту інформації та зменшення її витоків,

попередження зовнішніх і внутрішніх кіберзагроз, що відрізняється від існуючих складом критеріїв оцінювання ефективності та застосуванням системно-динамічного імітаційного моделювання. Це створює наукове підґрунтя для підвищення ефективності рішень щодо ребілдингу системи інформаційної безпеки;

– методологічне підґрунтя формування трирівневої системи попередження фінансових кіберзагроз, що передбачає: на організаційному рівні – оптимізувати бізнес-процеси (на основі BPMN-моделювання), на інформаційному рівні – побудувати портрети ймовірних жертв та кіберзлочинців (за допомогою дерева рішень), на алгоритмічному рівні – виявляти ознаки кібершахрайств (за допомогою нейромережевого моделювання). Це створює наукове підґрунтя підвищення ефективності систем забезпечення цілісності, доступності та конфіденційності інформації економічних агентів та органів державної влади.

Практичне значення одержаних результатів полягає в тому, що основні наукові положення дисертації доведено до рівня методичних розробок і практичних рекомендацій, які можуть бути використані: органами державної влади – під час розроблення та вдосконалення стратегії розвитку інформаційної безпеки національної економіки; профільними міжнародними інституціями – для стандартизації, сертифікації, контролю й моніторингу процесів кіберзахисту; інститутами громадянського суспільства – у процесі моніторингу прогресу реформ щодо забезпечення цифрової інклюзії населення та його інформаційної грамотності; суб’єктами господарювання – під час розроблення корпоративних політик забезпечення інформаційної безпеки; домогосподарствами – в процесі вибору ефективних інструментів захисту персональної інформації.

Пропозиції щодо композитних індикаторів економічного, політичного, соціального розвитку, а також цифрової спроможності та кібербезпеки країни в межах чотириполюсної барицентричної моделі впроваджено в діяльність міжнародної аудиторської компанії «ЕЙЧ ЕЛ БІ ЮКРЕЙН» (довідка № 375-03/21 від 04.03.2021 р.); щодо оцінювання ризиків втрати інформації – у діяльність ТОВ «Європейський консалтинговий сервіс» (довідка № 110-12/19 від 04.12.2019 р.); щодо оптимізації бізнес-процесів під час забезпечення

інформаційної безпеки – у діяльність відділення Сумської ОД АТ «ПРАВЕКС БАНК» (довідка № 534-10/19 від 09.10.2019 р.); щодо гравітаційного моделювання рівня привабливості країн для легалізації кримінальних доходів та кібершахрайств – у діяльність ТВБВ № 10018/0172 Філії – Сумського обласного управління АТ «Ощадбанк» (довідка № 17/20 від 07.09.2020 р.); щодо методів індивідуального кіберзахисту – у діяльність ГО «Освітньо-правозахисний координаційний центр» (довідка № 05/20 від 28.09.2020 р.).

Результати дисертації використовуються в навчальному процесі Сумського державного університету під час викладання дисциплін «Ефективність інформаційних систем», «Моделювання емерджентної економіки», «Прогнозування соціально-економічних процесів» (акт від 02.11.2020 р.).

Особистий внесок здобувачки. Дисертаційна робота є завершеним науковим дослідженням. Наукові положення, розробки, результати, висновки і рекомендації, що виносяться на захист, одержані самостійно. Особистий внесок у працях, опублікованих у співавторстві, зазначено в списку публікацій.

Апробація результатів дисертації. Основні результати дисертації оприлюднені та одержали позитивну оцінку на 11 міжнародних і всеукраїнських наукових конференціях ([33–43] в наведеному в авторефераті списку праць).

Публікації. Основні результати дисертаційної роботи опубліковано в 43 наукових працях загальним обсягом 45,78 друк. арк., з яких особисто авторці належить 40,39 друк. арк., зокрема, 1 одноосібна та 2 колективні монографії, 28 статей у наукових фахових виданнях України та 1 стаття в інших наукових виданнях (із яких 27 – у виданнях, що входять до міжнародних наукометричних баз, зокрема, 3 – до баз Scopus та Web of Science), 11 публікацій у збірниках матеріалів конференцій, зокрема, 1 входить до бази Scopus.

Структура та обсяг дисертації. Дисертаційна робота складається із вступу, п’яти розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації – 590 с., зокрема 398 с. основного тексту, 39 табл., 154 рис., 13 додатків та список використаних джерел, що налічує 410 найменувань.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ СУТНОСТІ ТА РОЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В НАЦІОНАЛЬНІЙ ЕКОНОМІЦІ

1.1 Тенденції розвитку національної економіки у світлі формування цифрової економіки

Базисом для розвитку суспільства є економіка, яка забезпечує всі сфери життєдіяльності людини, країни та світу. Вивченню проблем її формування, становлення та розвитку присвячено безліч наукових праць вітчизняних вчених та закордонних науковців. В контексті окремої держави основний акцент дослідження робиться на питаннях, пов’язаних із національною економікою, особливо її структурою, індикаторами виміру її стану, факторами впливу, етапами розвитку, тощо. Але перед усім треба розуміти, що вкладається у її поняття.

Класики політичної економії А. Сміт та Д. Рікардо розглядали національну економіку з позиції ринку капіталу та праці. Ф. Кене, як основний представник школи фізіократів, досліджував її з боку суспільного виробництва [352, с. 88]. Відомий у наукових колах французький вчений Р. Барр, один із засновників європейського Економічного та монетарного союзу, запропонував визначати національну економіку через центр економічної діяльності, центр сил та центр привілейованої згуртованості, що врешті решт сприяло виробленню «економічної концепції нації» [273, с. 63].

У сучасних дослідженнях такі науковці, як Карінцева О. [309, с. 63], Панчишина С., Остоверха П. [270], Гринів Л., Кічурчак М. [287, с. 16], Мельникова В., Мельникова О., Сідлярук Т., Тур І., Шведова Г. [327, с. 9], розглядають національну економіку у вузькому розумінні. Вони вважають, що вона є системою взаємопов’язаних галузей та сфер діяльності, обумовлених територіальною належністю до певної країни, які формують господарський комплекс для задоволення матеріальних та соціальних потреб населення. Деякі автори розглядають національну економіку у широкому значенні у вигляді

«соціально-економічних відносин, які склалися на певному етапі розвитку продуктивних сил, під впливом об'єктивних економічних законів, і визначають модель економічної системи з властивим їй способом організації та саморегуляції суспільного життя, забезпечують дотримання загальноекономічних, міжгалузевих, внутрішньогалузевих, територіальних пропорції у виробництві та розподілі суспільного продукту» [309, с. 63; 270; 287, с. 16].

Переважна кількість науковців підходять до розгляду національної економіки як системи, що формується із множини взаємопов'язаних елементів, для яких характерні територіальні, галузеві, соціально-економічні, технологічні, функціональні, інституційні ознаки. Так, Круш П.В. описує національну економіку як «економіку певної країни, що має ознаки економічної системи (загальне) та власні особливості і принципи розвитку (особливе), що проявляються в таких формах: економічний потенціал, структура господарського комплексу та галузей господарства, внутрішні чинники соціально-економічного розвитку, господарський механізм регулювання та координації та ін.» [315, с. 8]. Савченко П.В. представляє національну економіку у вигляді соціально-економічної системи, функціонування якої забезпечується єдиною територією, державним устроєм, правовими інститутами, єдиним ринком, культурою, мовою, ідеєю [356, с. 23]. Золотогоров В.Г. описує її як «сукупність господарських одиниць (уряд, фізичні особи, приватні безприбуткові компанії, підприємства, фірми, компанії, тощо), діяльність яких переважно здійснюється на економічній території країни» [304, с. 320]. Старостіна А., Прушківська Е. визначають національну економіку як «систему економічних відносин між суб'єктами господарювання (які є резидентами даної країни) з приводу виробництва, обміну, розподілу та споживання для реалізації своїх економічних інтересів» [363, с. 30]. Автори МочернийС.В., Ларіна Я.С., Устенко О.А., Юрій С.І. вважають, що вона є «системою економічних відносин між людьми в процесі взаємодії з розвитком продуктивних сил у всіх сферах суспільного виробництва, цілісність якої в межах єдиної централізованої

держави забезпечує й відповідний господарський механізм» [331, с. 576]. Гринчуцька С.В. характеризує національну економіку як «конституційно, економічно та організаційно єдину систему, взаємопов'язаних галузей і сфер діяльності людей, що характеризується відповідною пропорційністю та взаємозумовленим розміщенням на обмеженій державними кордонами території» [288, с. 6].

Аналізуючи наведені визначення національної економіки та її поняття, що приводять у своїх працях Тарасевич В.М. [274, с. 24], Градов А.П. [286, с. 40], Бункіна М.К. [281, с. 484], Старостенко Г.Г., Онишко С.В., Поснова Т.В. [362, с. 14], Проданова І.І. [351, с. 206], Кузьмін О., Когут У., Процик І., Вербицька Г. [321, с. 7], Задоя А.А., Петруня Ю.Е. [294] та інші, можна вивести загальні характеристики, яким повинна відповідати національна економіка з позиції її визначення:

- національна економіка представляє собою складну систему;
- елементами національної економіки як системи є економічні відносини;
- суб'єктами національної економіки виступають окремі індивіди, домогосподарства, економічні агенти, регіональні групи, країна в цілому, світові організації та інші країни;
- для національної економіки характерні ряд ознак, а саме: обмеження певною територією; підпорядкування певним правовим нормам та правилам, основам розвитку та функціонування економічних відносин; відповідність конкретним історичним умовам та особливостям існування конкретної нації.

Проведений аналіз поняття «національна економіка» є фундаментом для подальшого розуміння її структури. Науковці виділяють наступні види структури національної економіки: відтворювальну, галузеву, інституційну (секторальну), технологічну, просторову (регіональну, територіальну), соціальну, зовнішньоекономічну. Дослідження наукових праць [310, 378, 349, 289, 309, 353, 360, 344, 373] дозволило визначити, що:

- відтворювальна структура характеризується співвідношенням елементів процесу суспільного відтворення;
- галузева структура показує внесок певних видів економічної діяльності з урахуванням їх взаємозв'язків у національний обсяг виробництва;
- секторальна структура відображає виділення секторів економіки, які відповідають певним сферам економічної діяльності;
- технологічна структура характеризується технологічним устроєм країни, який відображає можливості перетворення інформації, ресурсів, енергії;
- просторова відображає розміщення продуктивних сил на певній території у відповідності із її економіко-географічним та адміністративним аспектом;
- соціальна визначається на основі соціально-економічних взаємовідносин між різними прошарками суспільства;
- зовнішньоекономічна структура характеризується кількістю та якістю міжнародних економічних зв'язків із іншими країнами з урахуванням експорту та імпорту товарів, робіт, послуг, капіталу, тощо.

Виходячи з наведеного опису різних видів структур національної економіки, проведемо аналіз секторної структури економіки України. Класично виділяють три сектори, які характерні для економік країн із доіндустріальним суспільством. Але в умовах трансформаційних процесів та розвитку економіки доцільно застосовувати п'ятисекторну модель, яка характерна для індустріального та постіндустріального суспільства [320, с. 10-11]. У даній моделі первинний сектор охоплює добуток та виробництво сировини; вторинний – виробництво кінцевого продукту; третинний – сферу послуг; четвертинний – інформаційне та наукове обслуговування секторів; п'ятинний – виробництво знань та інформаційних продуктів [309, с. 65]. Кожен сектор економіки формується в залежності від певних видів діяльності згідно до національної та міжнародної класифікації. Використаємо міжнародну класифікацію, згідно якої відбувається розрахунок ВВП у фактичних цінах.

На рисунку 1.1 представлено розподіл складових ВВП за секторами національної економіки України за 2019 рік, де можна побачити, що в Україні превалює третинний сектор, що характерно для індустріальної стадії економіки. На фоні зниження вторинного та первинного секторів відбувається зростання п’ятинного та четвертинного, що говорить про збільшення напрямів діяльності у сфері виробництва знань.

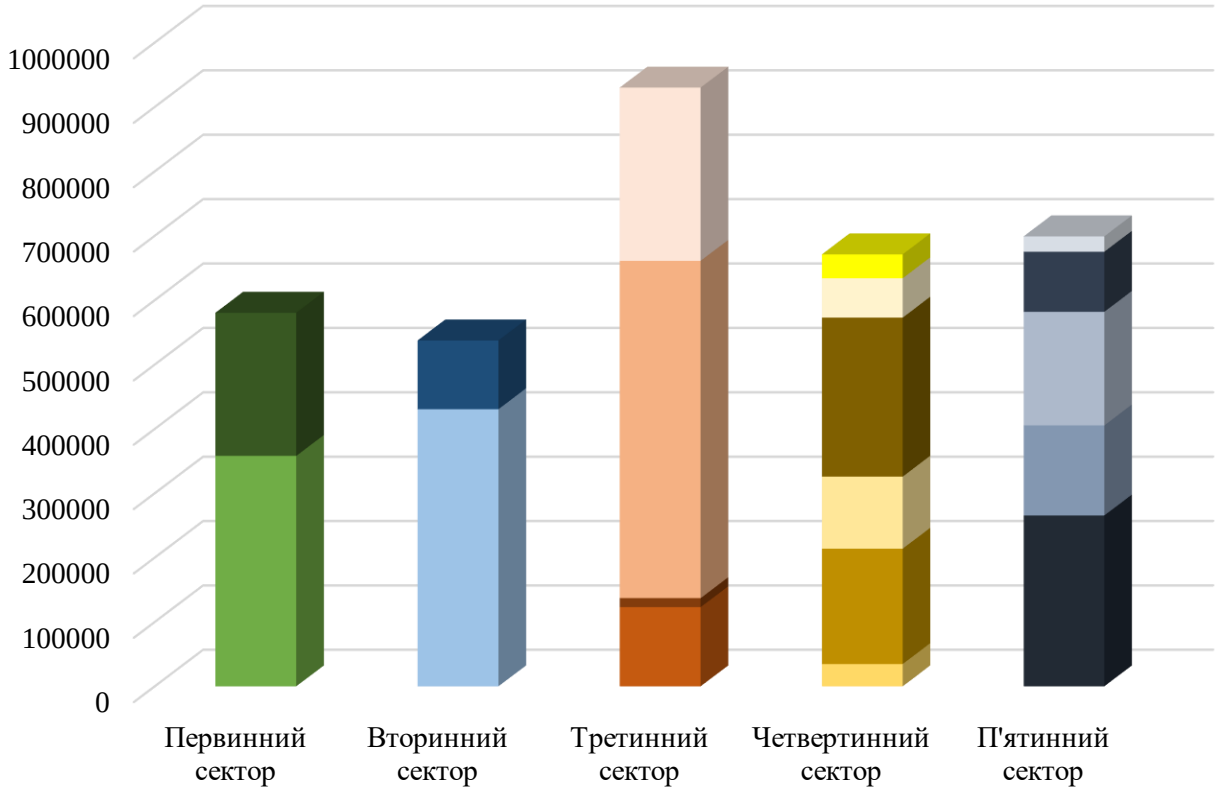


Рисунок 1.1 – Складові ВВП України за секторами національної економіки (2019 р., у фактичних цінах, млн. грн.)

Джерело: авторські розрахунки на основі [282]

На рисунках 1.2 - 1.6 деталізовано складові ВВП України, представлені на рисунку 1.1, у відповідності із секторами національної економіки за 2019 рік.

Рисунок 1.2 – Первинний сектор (млн. грн.)

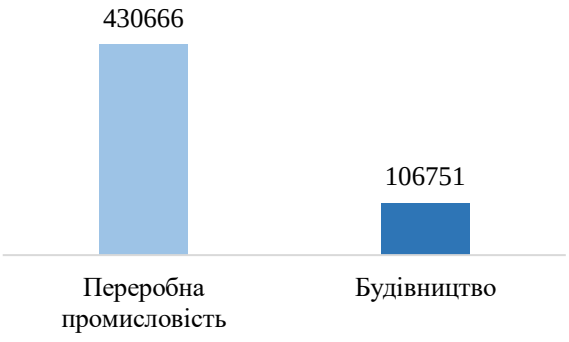


Рисунок 1.3 – Вторинний сектор (млн. грн.)

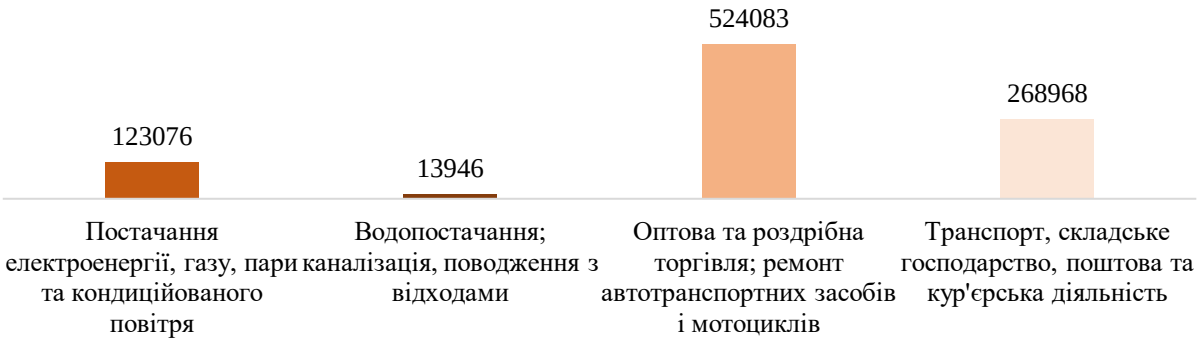


Рисунок 1.4 – Третинний сектор (млн. грн.)

Рисунок 1.5 – Четвертинний сектор (млн. грн.)

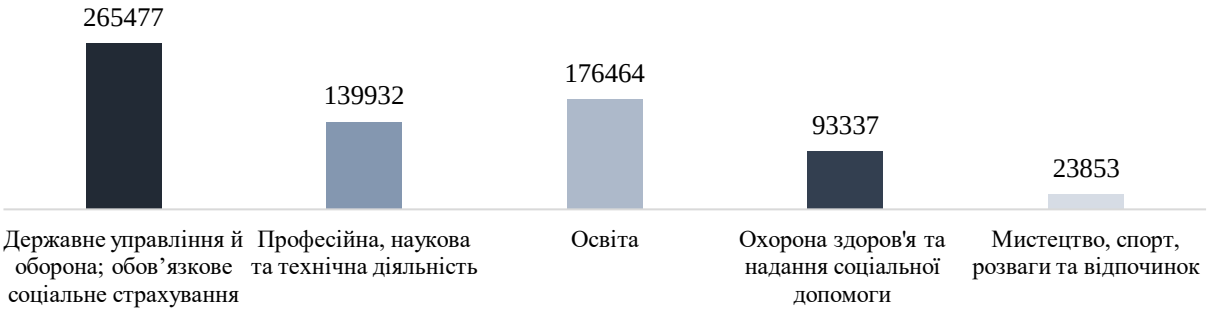


Рисунок 1.6 – П’ятинний сектор (млн. грн.)

Джерело: авторські розрахунки на основі [282]

У первинному секторі превалює сільське, лісове та рибне господарство (рисунок 1.2), у вторинному – переробна промисловість (рисунок 1.3), у третинному - оптова та роздрібна торгівля, ремонт автотранспортних засобів і мотоциклів (рисунок 1.4), у четвертинному - операції з нерухомим майном (рисунок 1.5), у п’ятинному – державне управління й оборона, обов’язкове соціальне страхування (рисунок 1.6). Такий розподіл свідчить про те, що основу національної економіки України становлять сільське господарство, торгівля та промисловість із зростанням долі державного управління та оборони, що пов’язано із існуванням військового конфлікту на сході країни. Позитивною тенденцією є зростання четвертинного та п’ятинного секторів, що свідчить про нарощення можливостей інформаційно-телекомунікаційного обслуговування секторів та виробництва інформації та знань. Дану тенденцію можна прослідкувати, починаючи із 2010 року (рисунок 1.7), де чітко спостерігається окрім стрімкого збільшення третинного сектору, поступове нарощування четвертинного та п’ятинного.

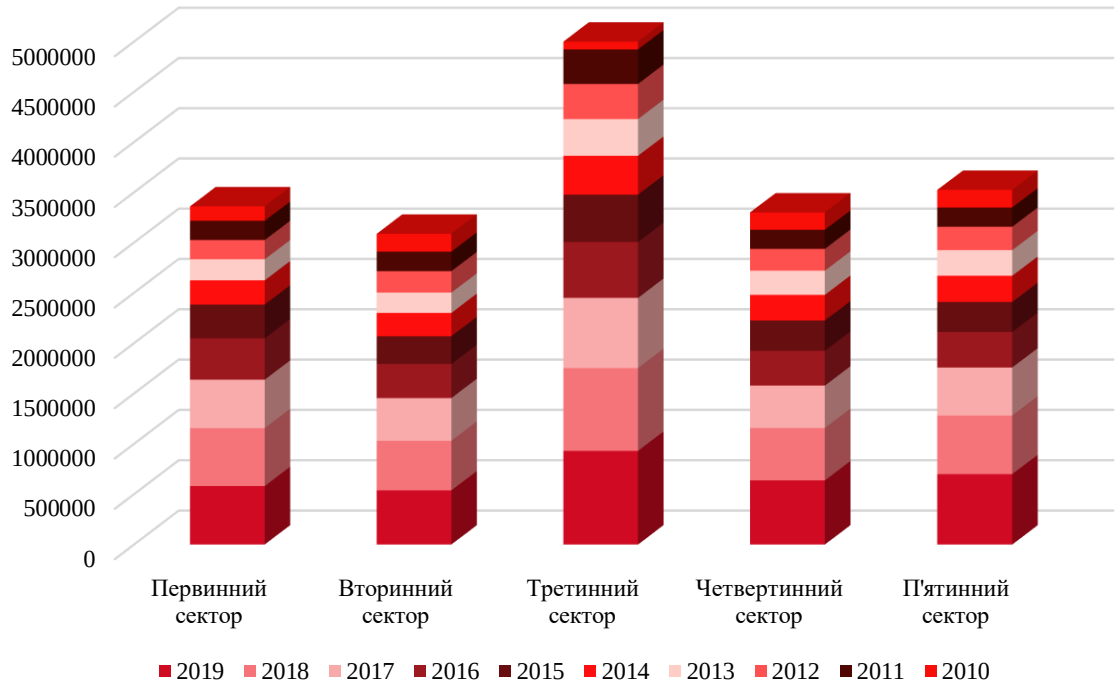


Рисунок 1.7 – Складові ВВП України за секторами національної економіки (2010-2019 рр., у фактичних цінах, млн. грн.)

Джерело: авторські розрахунки на основі [282]

Тобто відбувається поступовий розвиток економіки у напрямку подальшого зростання інформатизації, цифровізації та телекомунікації її сфер. На підтвердження даних тенденцій можна проаналізувати динаміку зміни частки інформації та телекомунікації окремо у четвертинному секторі та у ВВП України (рисунок 1.8).

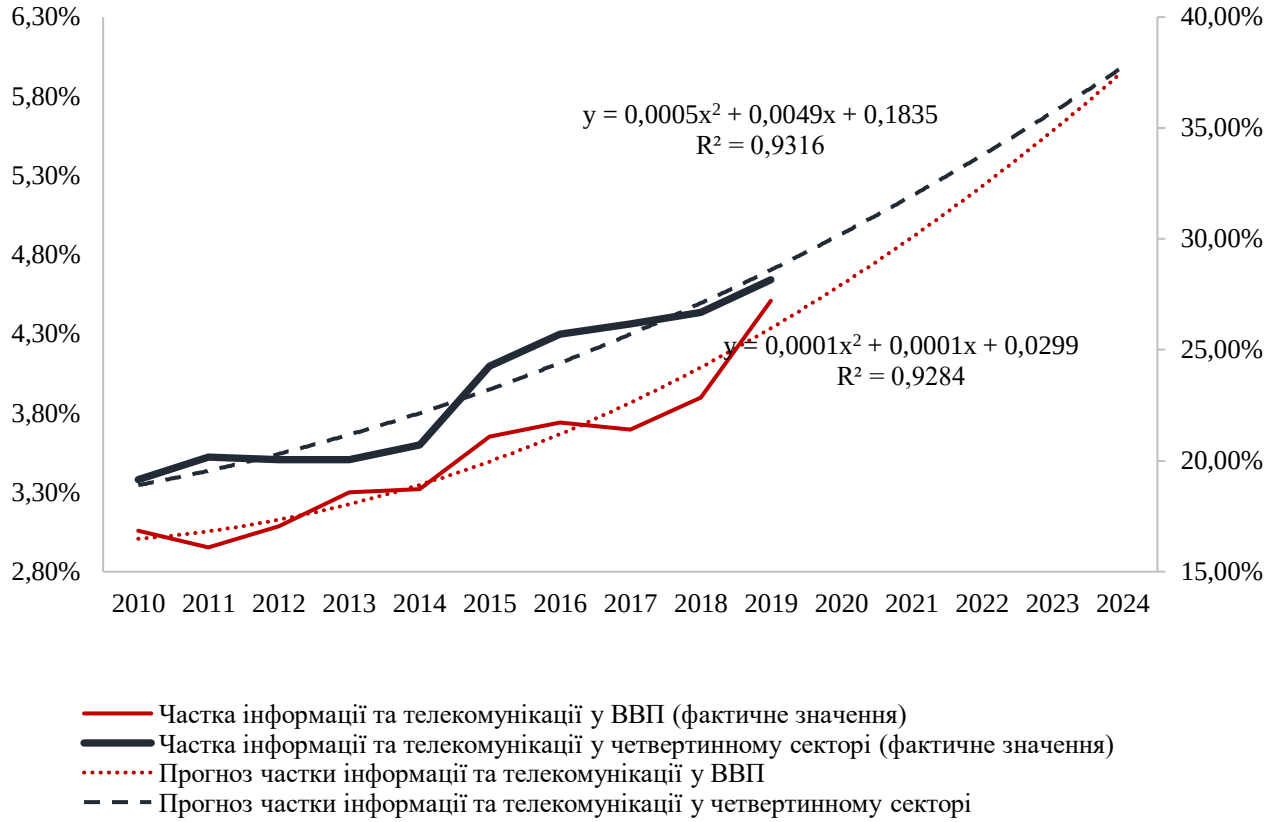


Рисунок 1.8 – Тенденції зміни інформації та телекомунікації (фактичне та прогнозне значення)

Джерело: авторські розрахунки на основі [282]

На рисунку 1.8 представлено фактичне значення зміни частки інформації та телекомунікації з 2010 по 2019 роки. Так, у 2010 році вона складала 19,15% у четвертинному секторі, а у 2019 році – вже 28,16%, тобто практично третину формування четвертинного сектора забезпечує саме інформація та телекомунікація. На графіку 1.8 можна побачити прогноз на 5 років уперед, зроблений із використанням поліноміального тренду другого ступеня, обраного як більш точного та такого, що дозволяє робити оптимістичні прогнози. Тобто у

2024 році зростання інформації та телекомунікації у структурі четвертинного сектору прогнозовано досягне близько 38%. Позитивна тенденція зросту також спостерігається, якщо аналізувати частку інформації та телекомунікації у ВВП України. Так, у 2010 році вона складала 3,06%, а у 2019 році її значення становило 4,51%. Зроблений оптимістичний прогноз із використанням поліноміального тренду показує досягнення значення даного показника у 2024 році близько 6,00%. Характер даних тенденцій підтверджується розрахунками, проведеними експертами ініціативи «Цифрова адженда України» [372, 367], які відображають прогнози показників цифровізації економіки України, хоча вони є занадто оптимістичними (див. табл. 1.1):

Таблиця 1.1 – Прогнозні показники цифровізації економіки України

Показники	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Внутрішній ринок (споживання ІКТ), млрд дол.	2,0	2,5	3,0	4,5	6,0	8,0	10,0	12,0	14,0	16,0
Вплив на ВВП, % зростання	+0,5	+1,0	+2,0	+3,5	+4,5	+6,0	+7,5	+9,0	+11,0	+14,0
Частка цифрової економіки у загальному ВВП, %	3	5	8	11	15	20	28	40	52	65

Джерело: [372, 367]

У сучасних економічних умовах розвитку України відбувається зростання рівня споживання інформаційно-комунікаційних технологій, що, в свою чергу, впливає на темпи їх модернізації у різних сферах економічної діяльності. Оскільки рівень її фінансування є низьким у порівнянні із іншими сферами та іншими країнами, то це відчувається у повільному зростанні темпів розвитку ІТ-індустрії в Україні. Експерти прогнозують, що у 2030 році частка цифрової економіки у загальному ВВП зросте до 65%, що призведе до його збільшення на 14% (див. табл. 1.1). На нашу думку, це можливо лише завдяки припливу інвестицій закордонних компаній, зацікавлених у високо-технологічному виробництві, а також впровадженні сучасних технологій для забезпечення більш ефективного функціонування бізнес-процесів різних суб’єктів економіки.

Можна порівняти тенденції розвитку національної економіки, які притаманні українським реаліям, із змінами, що відбуваються в інших країнах. З цією метою проаналізуємо долю ІТ-сектора у ВВП розвинутих країн Європейського Союзу (рисунок 1.9).

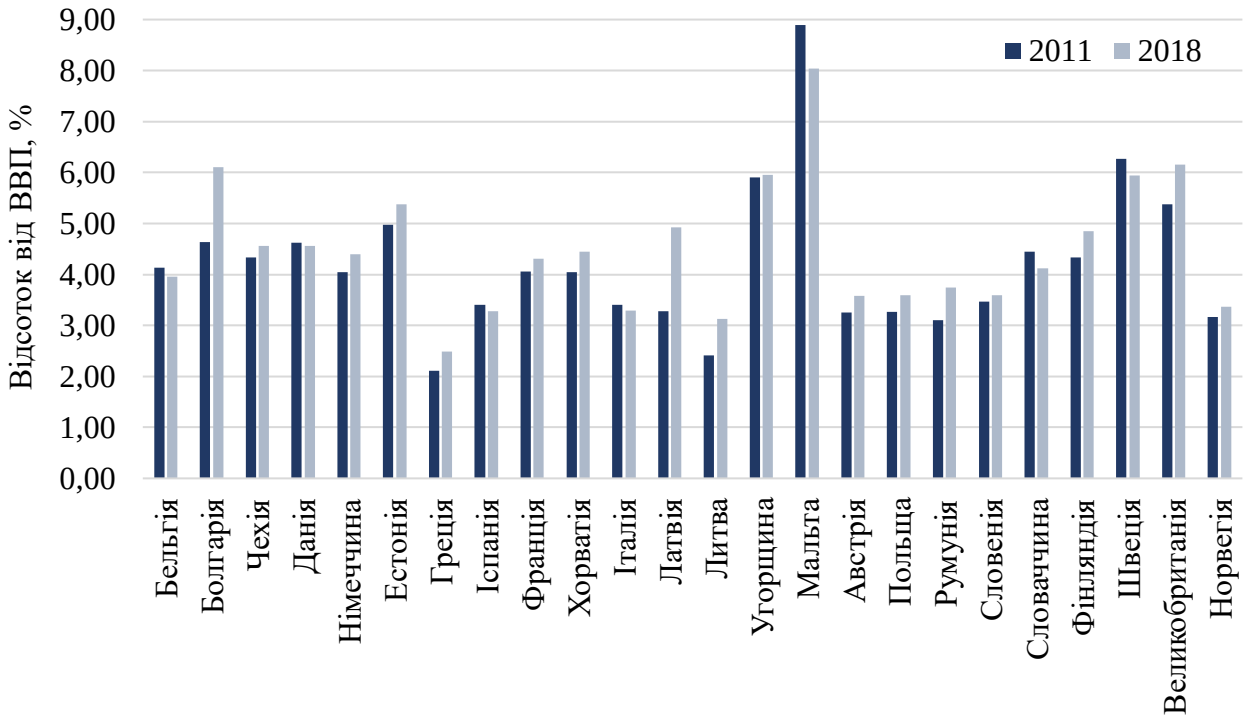


Рисунок 1.9 – Частка ІТ-сектору у ВВП (% від ВВП)

Джерело: побудовано авторкою на основі даних [193]

За період із 2011 по 2018 роки спостерігається зростання частки ІТ-сектору у ВВП для таких країн як: Болгарія (+1,46%), Чехія (+0,22%), Німеччина (+0,36%), Естонія (+0,40%), Греція (+0,38%), Франція (+0,25%), Хорватія (+0,41%), Латвія (+1,46%), Литва (+0,72%), Угорщина (+0,04%), Австрія (+0,33%), Польща (+0,32%), Румунія (+0,64%), Словенія (+0,12%), Фінляндія (+0,52%), Великобританія (+0,77%), Норвегія (+0,21%) (рисунок 1.9). В середньому за 8 років зростання відбулося на 0,30%, що говорить про уповільнене збільшення процесів інформатизації. Найвищий рівень ІТ-сектору у складі ВВП характерний для Мальти та дорівнює 8,04%, мінімальний рівень – для Греції, який становить 2,49%. В середньому за 2018 рік доля ІТ склала

приблизно 4,49%. Для таких країн, як Бельгія, Данія, Іспанія, Італія, Мальта, Словаччина та Швеція відбулося зниження частки ІТ-сектору у ВВП у середньому на 0,28%. Можливо це обумовлено уповільненням зростання інформатизації різних видів діяльності та збільшенням частки інших складових секторів економіки, але в цілому спостерігається позитивна тенденція для більшості країн Європи. У 2018 році доля ІТ-сектору у ВВП України склала 3,9% (рисунок 1.8), що хоча і нижче середнього рівня, який характерний для країн ЄС, але зростання даного показника у 2019 році до 4,51% свідчить про закономірне нарощення ІТ-галузі.

Таким чином, відбувається розвиток національної економіки не тільки України, але й інших країн світу, у напрямку її інформатизації та цифровізації. На підтвердження цього факту можна навести дані, які показують, що даний факт є актуальним для різних сфер діяльності. Так, на рисунку 1.10 представлено дані по відсотку підприємств, які використовують ERP-системи для повної автоматизації усіх бізнес-процесів.

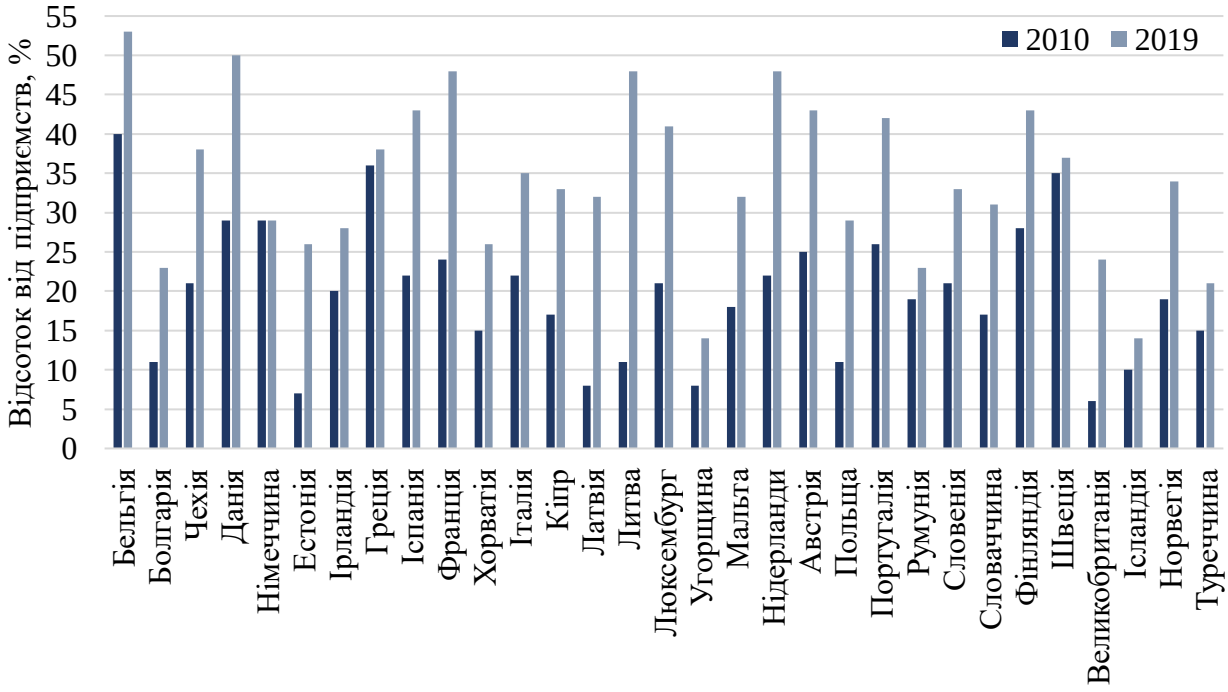


Рисунок 1.10 – Частка підприємств, що застосовують ERP-системи (% від підприємств)

Джерело: побудовано авторкою на основі даних [126]

Використання компаніями ERP-систем є ознакою ефективності управління діяльністю у відповідності із міжнародними стандартами якості ISO 9000. Цей показник характеризує економічного агента як надійного партнера, спроможного задовольняти вимоги зацікавлених сторін: власників, клієнтів, постачальників, співробітників, а також діяльність якого спрямована на забезпечення стійкого успіху. Саме тому в процесі оцінці тенденцій розвитку національної економіки необхідно звертати увагу на даний фактор.

Дані рисунку 1.10 свідчать про те, що за період з 2010 по 2019 роки відбувається стрімке зростання частки компаній, які застосовують ERP-системи, для країн ЄС. Так, максимальне збільшення даного показника серед країн ЄС відбулося для Литви й склало 37%, для Німеччини його зміна дорівнює 0%, але оскільки у 2015 році частка таких підприємств складала 56%, то таке значення у 2019 році можна пояснити або зростанням кількості нових підприємств, або переходом ERP-систем на стандарт SCRP. В середньому збільшення відбулося на 14% та склало 34% за 2019 рік по всім країнам ЄС. Отримані результати свідчать про те, що рівень автоматизації та інтеграції бізнес-процесів економічних агентів зріс за останні 10 років та є характерним для всіх європейських країн, що підтверджує напрямок інформатизації економічних процесів та відносин між суб’єктами економіки на мікро- та макрорівні.

Також проаналізуємо показник, який відображає відсоток користувачів Інтернет-банкінгу. Сфера банківських послуг є найбільш розвинутою у плані використання різних інформаційних технологій, які застосовуються для підвищення ефективності надання банківських послуг, результатом чого є інтеграція банківських технологій у інформаційні системи економічних агентів та мобільні пристрої окремих індивідів. Практично всі платіжні операції здійснюються у безготівковій формі із використанням Інтернет-банкінгу або мобільного банкінгу. Саме даний напрямок призвів до формування інформаційних зв’язків між споживачами банківських послуг та тими, хто їх надає у різних сегментах. Тому проведемо аналіз показника відсотка

користувачів Інтернет-банкінгу, дані якого узяті для країн ЄС за 2007 та 2019 роки (рисунок 1.11).

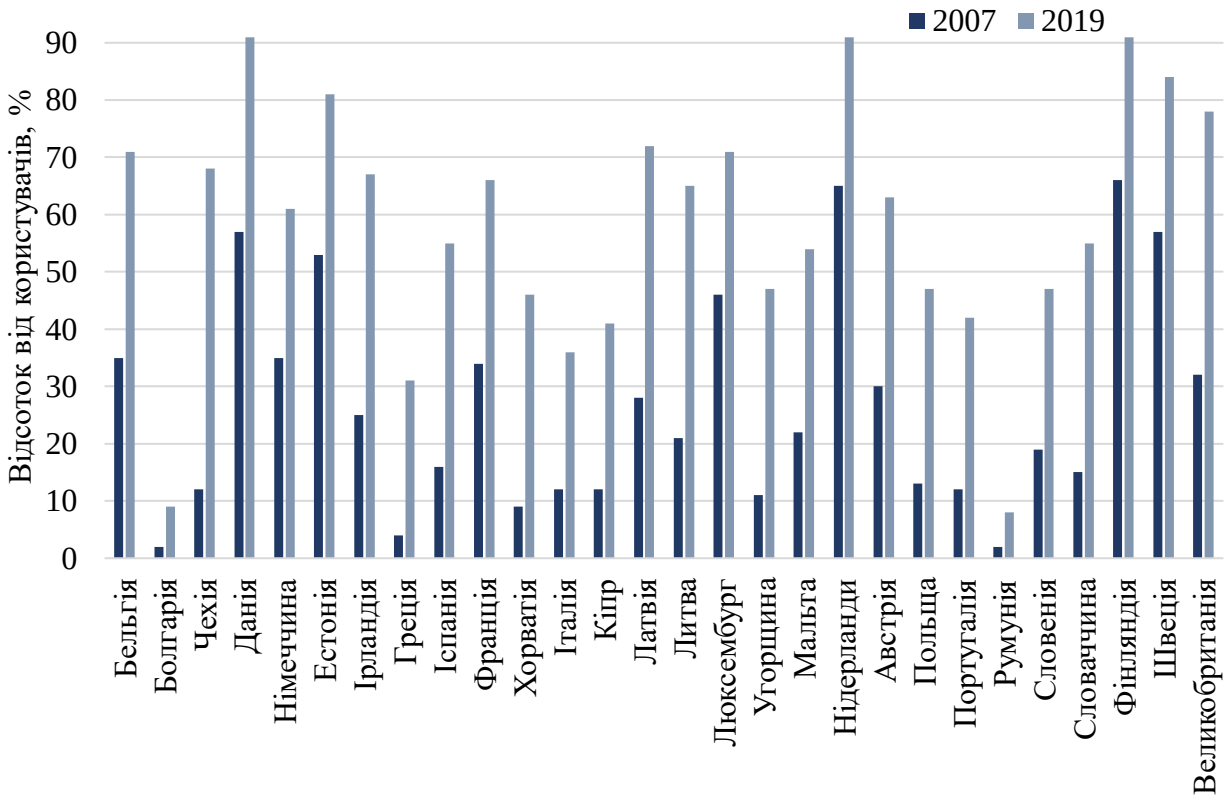


Рисунок 1.11 – Відсоток користувачів Інтернет-банкінгу (% від користувачів)

Джерело: побудовано авторкою на основі даних [123]

На рисунку 1.11 спостерігається тенденція стрімкого збільшення кількості користувачів Інтернет-банкінгу для більшості країн. Так, максимальне зростання відбулося для Чехії й склало 56%, мінімальне – для Румунії на 6%. В середньому збільшення відбулося на 32% та склало 59% за 2019 рік по всім країнам ЄС. Такі країни як Данія, Нідерланди та Фінляндія мають 91% користувачів Інтернет-банкінгу, що говорить про високий ступінь інтеграції банківських ІТ у життєдіяльність суспільства та процеси компаній. Такі країни як Болгарія та Румунія мають менше 10% користувачів, але за останні 10 років їх кількість збільшилася, що в перспективі дозволяє говорити про тенденції зростання даного показника. Отримані результати свідчать на користь розвитку банківського сектора та національної економіки у напрямку їх інформатизації та цифровізації.

Таким чином, сучасна національна економіка України та багатьох інших країн світу зазнає трансформації з урахуванням тенденцій залучення новітніх інформаційних та комп'ютерних технологій до вирішення різного роду задач, що призводить до їх інтеграції у більшість сфер економічної діяльності. Зростання ІТ-складових четвертинного та п'ятинного секторів економіки врешті решт призведе до перетворення постіндустріального суспільства у цифрове. Тому можна казати, що вже сьогодні є актуальним саме цифровий варіант розвитку економіки, який забезпечуватиметься шляхом використання суб'єктами економіки інструментів впливу на різні сфери діяльності. Виходячи з даного твердження та з урахуванням основних його тез представимо структуру національної економіки, формування якої обумовлено застосуванням системного підходу до визначення систем – хто (суб'єкт), що (об'єкт) та як (інструмент) (рисунок 1.12).

На рисунку 1.12 можна побачити, що у якості суб'єктів національної економіки виступають індивіди (нанорівень), сімейні господарства (мінірівень), економічні агенти (мікрорівень), регіони (мезорівень), країна (макрорівень) та світ (мегарівень). В процесі здійснення ними різного роду діяльності виникають відносини, в результаті яких відбувається формування відповідних сфер національної економіки. Для досягнення ефекту у даних процесах застосовуються різного роду технології, які розвиваються у відповідності із тенденціями та темпами розвитку суспільства. Так, на початку другого десятиліття 21-го сторіччя закінчилася епоха цифрової революції (промислової революції 3.0), яка почалася у 1980-х роках та дозволила розробити і впроваджувати у сфери діяльності людини ERP-системи, сховища даних, автоматизовані системи управління технологічним процесом (АСУ ТП), хмарні технології; промислові мережі; мобільні технології; SCADA / HMI; APS / MES; APC / OTS; DCS / FI; роботи. 2011 рік ознаменувався початком четвертої промислової революції (Індустрія 4.0). Її реалізація сприяє впровадженню не тільки в економіку, але й у інші галузі людської діяльності, пов'язані із побутом, працею, дозвіллям, тощо, найбільш прогресивних технологій, таких як:

технології кібербезпеки та штучного інтелекту, VR/AR, Blockchain, Wearable, дрони, 3D-друк, платформи IIoT, Digital Twins, коботи.

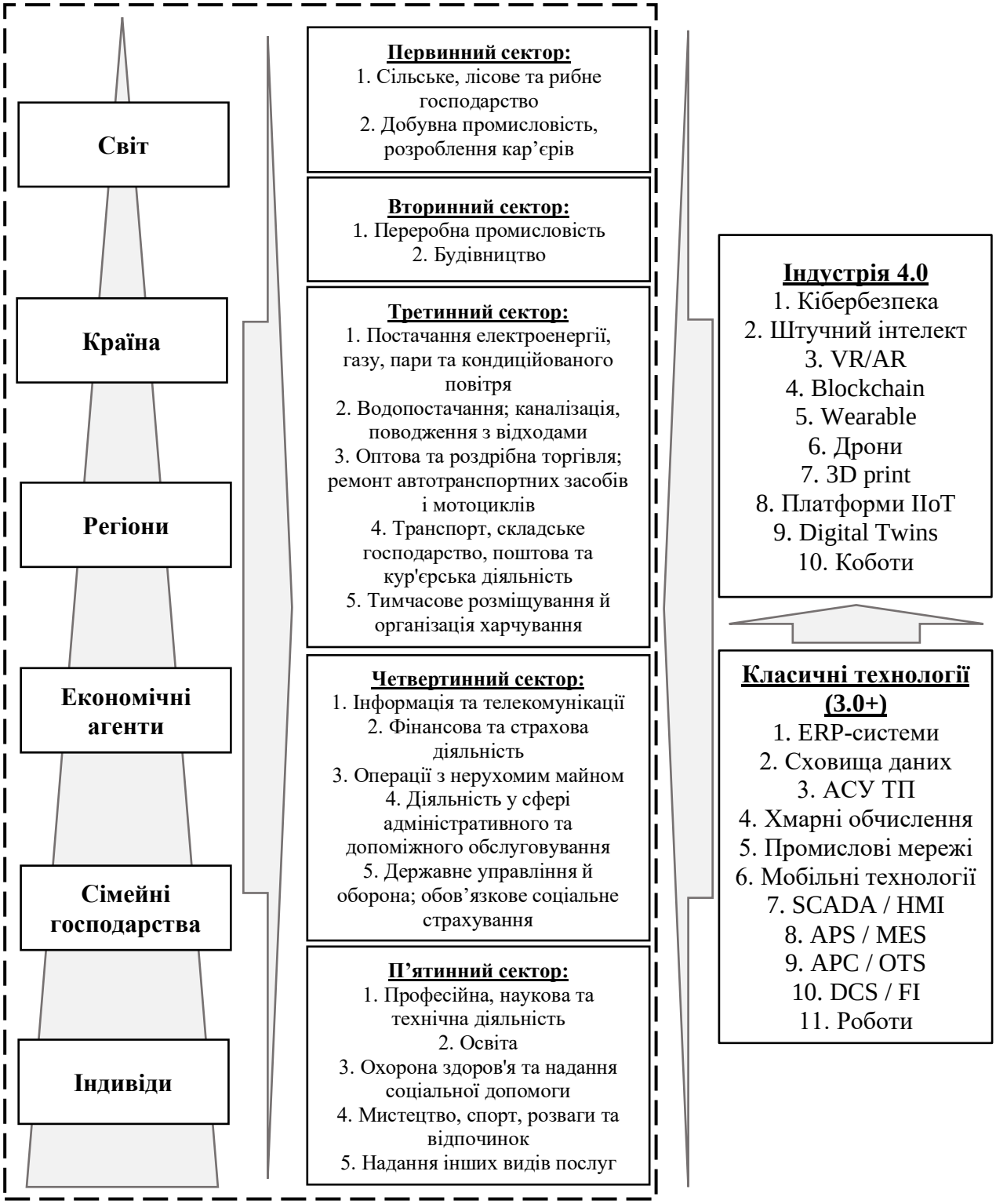


Рисунок 1.12 – Структура національної економіки з урахуванням її суб'єктів, секторів та інструментів впливу (складено авторкою)

Сьогодні дуже важко уявити різні сфери діяльності суспільства без використання комп'ютерних та інформаційних технологій. Але їх стрімкий розвиток призводить також й до того, що новітні технології стають інструментами для незаконного збагачення різного роду злочинців. Це проявляється у збільшенні випадків хакерських атак на бізнес підприємств з метою отримання фінансової інформації, викрадення технологій, новітніх розробок, оприлюднення персональних даних клієнтів. Наприклад, у 2019 році співробітники 27% компаній у всьому світі стали об'єктами кібертерористів через застосування програмного забезпечення смартфонів [78].

Збільшується кількість кібершахраїв, які застосовують програмно-технологічні можливості для ошукування населення, отримання доступу до особистих даних, рахунків та грошових коштів. Наприклад, багато злочинців намагаються скористатися ситуацією, яка склалася у світі через пандемію COVID 19, та від імені Всесвітньої організації охорони здоров'я надсилають фейкові посилання з інформацією про вірус. В результаті, велика кількість людей втратили особисті та платіжні дані, а шахраї отримали доступ до їх рахунків [14]. У липні 2020 року було зламано 280 000 з 1,45 млн. профілів користувачів різних країн у базі даних ДНК «GEDmatch», що призвело до доступності інформації для хакерів та сторонніх осіб [10].

На рівні держави може відбуватися інформаційний вплив на суспільство із використанням соціальних мереж, пропаганди, фейкових новин, що врешті решт призводить до виникнення інформаційних війн, проведення масових хакерських та кібертерористичних операцій. Як наслідок, такі дії можуть порушувати баланс соціальних настроїв у суспільстві, розстановку політичних сил, приводити до фінансово-економічних втрат, змінювати політику міжнародних фондів, організацій та інвесторів щодо співпраці із такими країнами.

Перелічені факти є свідченням того, що сьогодні існують загрози, які можуть призводити до порушення національної безпеки країни саме в частині її інформаційної безпеки. Це може відбуватися, як на рівні окремого суб'єкта, так й країни в цілому, при чому наслідки можуть бути помітними в економічній,

соціальній, політичній або інших сферах діяльності. Так, прогнозується зростання збитків компаній по всьому світу в результаті порушення їх інформаційної безпеки та подолання наслідків до 5 трлн. дол. у 2024 році проти 3 трлн. дол., які було втрачено у 2018 році [179], що свідчить про зростання рівня інформаційних загроз в майбутньому та актуальності даної проблеми.

Тому важливо розуміти, що представляє собою інформаційна безпека, які існуючі загрози пов'язані із нею, та як їх наслідки впливатимуть на рівень розвитку окремого суб'єкта або економічного агента, або країни в цілому. При цьому також релевантним є визначення напрямів дослідження даної проблеми в контексті її зв'язку із національною економікою, що дозволить сформувати пріоритетні вектори даної наукової роботи.

1.2 Сутність інформаційної безпеки та концептуальні засади її забезпечення в системі управління національною економікою

Зростання рівня інформатизації та комп'ютеризації суспільства призвело до необхідності появи інформаційної безпеки. Вважається, що це було пов'язано із потребою захисту інформації про торгові угоди, майно, фінансові операції, тощо, яка фіксувалася на офіційних паперах до початку 19 сторіччя. Тобто її необхідно було вберегти від фізичних пошкоджень та викрадення злочинцями. Із розповсюдженням радіо- та електрозв'язку з'явилась потреба у захисті даних, які передавалися, від сторонніх впливів. Особливо це було важливо в умовах ведення країнами військових дій, в результаті чого почали вдаватися до кодування та декодування сигналів. Починаючи із 1935 року, коли активно розроблялися та використовувалися засоби радіолокації та гідроакустики, акцент безпеки змістився на підвищення їх захисту шляхом створення маскувально-імітувальних перешкоджальних засобів. Впровадження перших електронно-обчислювальних комп'ютерів у практичну діяльність на при кінці 40-х та на

початку 50-х років 20-го сторіччя сприяли формуванню нових завдань інформаційної безпеки, пов'язаних із розробкою заходів, що обмежували на фізичному рівні доступ до пристроїв збору, обробки та виведенням інформації [271; 342; 303, с. 166].

Початком формування інформаційної безпеки, як окремого самостійного напряму розвитку інформаційних систем, є шістдесяті роки 20-го сторіччя, оскільки саме в той час у суспільстві та фінансово-господарській діяльності компаній масово стали траплятися випадки втрати інформації через зовнішні та внутрішні джерела, що було обумовлено створенням локальних мереж (рисунок 1.13). Множина таких інцидентів призвела до того, що більшість підприємств почали впроваджувати нові інструменти захисту. Головним із них було створення паролів доступу користувачів у відповідності із їх функціональними обов'язками.

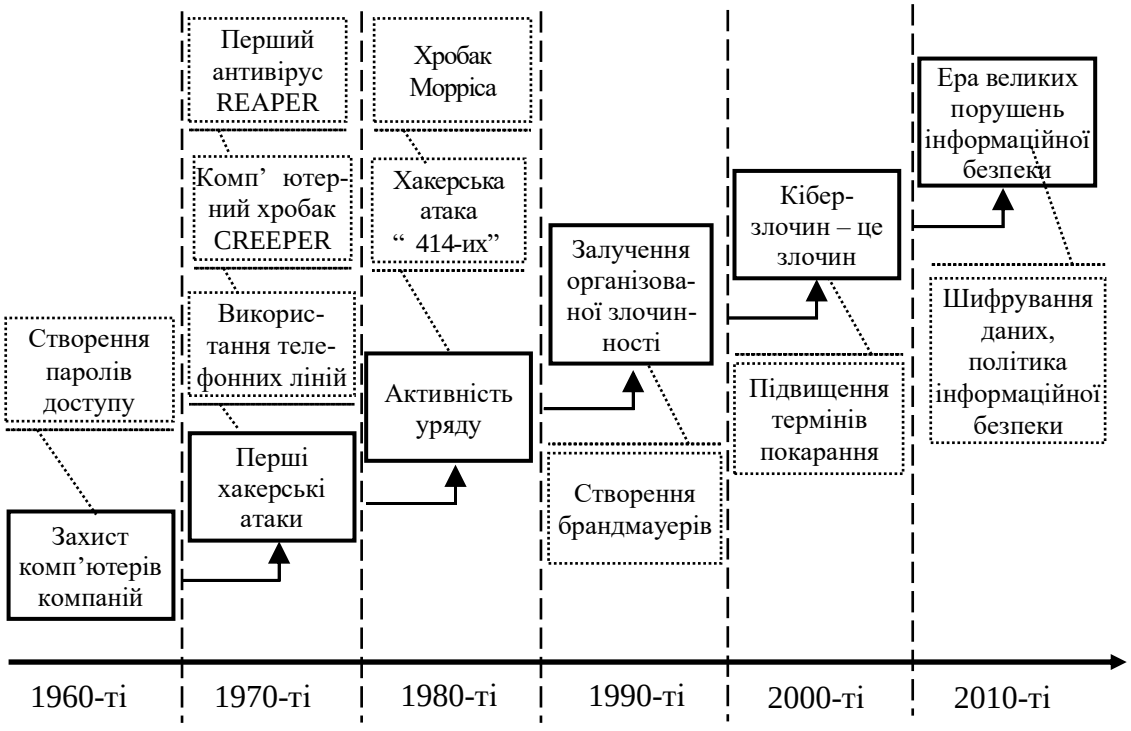


Рисунок 1.13 – Етапи розвитку інформаційної безпеки

Джерело: складено авторкою на основі [170, 181]

Сімдесяті роки 20-го сторіччя пов’язані із появою перших хакерських атак, що стало можливим за рахунок використання телефонних ліній, за допомогою яких великі організації з’єднували комп’ютери (рисунок 1.13). Також в ці роки відбувався розвиток проекту ARPANET (Мережа агентства з перспективних дослідницьких проектів), що сприяло появі першого комп’ютерного хробака "CREEPER" (розробники Боб Томас та Рей Толінсон) та першого антивірусного програмного забезпечення "Reaper" (розробник Рей Толінсон) [372, 367].

Вісімдесяті роки 20-го сторіччя характеризуються активізацією комп’ютерних мереж, розповсюдженням ARPANET, який перетворився на світову мережу Інтернету (рисунок 1.13). Хакерство почало охоплювати різні сфери діяльності людини. Найбільшою подією, яка отримала назву «414-ті», було зламування більше 400 військових комп’ютерів, що було виконано російськими спецслужбами з метою викрадення американських військових таємниць. Це був початок використання кіберзброї країнами. Їх уряди почали залучатися до питань інформаційної безпеки. Також протягом даного десятиліття Робертом Моррісом було створено комп’ютерного хробака, від дій якого було завдано серйозні збитки, в результаті чого винахіднику висунули звинувачення згідно «Закону про комп’ютерне шахрайство та зловживання» [372, 367].

Після того, як Інтернет набув розповсюдження та став доступним, масово з’явились випадки шахрайств, пов’язаних із викраденням особистої інформації, що відбувалось організованими злочинними групами. В результаті для захисту були створені брандмауери, які знижали кількість хакерських атак (рисунок 1.13). Із часом стали змінюватися закони, згідно з якими кібрзлочини каралися на рівні із іншими видами тяжких злочинів. Але починаючи з 2010 року, кількість кіберзлочинів тільки зростає, при чому відбувається ускладнення технологій, які застосовуються для їх здійснення. Так, за результатами дослідження, проведеного компанією Dell Technologies, у 2019 році від кібератак постраждало 82% компаній, що на 6% більше ніж у 2018 році. Тільки 4% компаній мають надійну систему захисту, що підтверджено компанією Softline [306].

Тобто інформаційна безпека існувала в різні епохи розвитку суспільства, починаючи від паперових технологій та завершуючи програмно-технічними комплексами. Вона стосується різних сфер діяльності та впроваджується з метою попередження втрат інформації та протидії кіберзлочинності. Її порушення пов'язано із кримінальною відповідальністю. Отримані знання щодо історичного розвитку інформаційної безпеки дозволили провести аналіз існуючих підходів до її визначення.

Так, можна виділити два напрями. Перший стосується підходів, які визначають інформаційну безпеку, виходячи з її властивостей функціонування як стану, процесу та сфери діяльності. Результати його узагальнення наведені у таблиці 1.2.

Таблиця 1.2 – Узагальнення підходів до визначення інформаційної безпеки з позиції її функціонування

Зміст підходу	Автор та джерело	Визначення інформаційної безпеки
Інформаційна безпека як стан	Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки» [300]	Це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації».
	Кормич Б.А. [314, с. 109]	Це «стан захищеності встановлених законодавством норм, параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини, суспільства як суб'єктів процесів та відносин».
	Петрик В. [341, с. 122]	Це «стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток, технічний, інтелектуальний, соціально-політичний, морально-етичний, за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди».
Інформаційна безпека як процес	ISO/IEC 27000:2009 [128]	Це «збереження конфіденційності, цілісності та доступності інформації. Примітка. Крім того, можуть бути задіяні й інші властивості, такі як достовірність, підзвітність, відмова та надійність».
	SNSS [54]	Це «захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації, знищення для забезпечення конфіденційності, цілісності та доступності».

Продовження таблиці 1.2

Зміст підходу	Автор або джерело	Визначення інформаційної безпеки
Інформаційна безпека як процес	ISACA [105]	Вона «забезпечує таким чином, що лише авторизовані користувачі (конфіденційність) мають доступ до точної та повної інформації (цілісність), коли це потрібно (наявність)».
	SANS Institute [124]	Вона «відноситься до процесів та методологій, які розроблені та впроваджені для захисту друкованої, електронної чи будь-якої іншої форми, приватної та конфіденційної інформації, чи даних від несанкціонованого доступу, використання, розкриття, зловживання, знищення, модифікації чи порушення».
	Wikipedia [125]	«Інформаційна безпека означає захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення».
Інформаційна безпека як сфера діяльності	Черданцева Ю., Хілтон Дж. [46]	Це «мультидисциплінарна сфера вивчення та професійної діяльності, яка займається розробкою та впровадженням усіх доступних типів механізмів безпеки (технічних, організаційних, орієнтованих на людину, юридичних) з метою збереження інформації у всіх її місцях (усередині та поза периметром організації) і, отже, в інформаційних системах, де інформація створюється, обробляється, зберігається, передається та знищується, вільна від загроз».

Перший підхід пов’язує інформаційну безпеку із станом захищеності, що не зовсім вірно, оскільки вона забезпечує його, використовуючи різні засоби. Тобто подібні визначення акцентують увагу на меті функціонування інформаційної безпеки. Другий підхід передбачає те, що інформаційна безпека є процесом, який включає застосування різного роду програмних, технічних, правових, інформаційних та організаційних інструментів для забезпечення її функціонування. Також некоректним буде вважати інформаційну безпеку тільки процесом, тобто послідовністю виконання дій щодо захисту, оскільки вона може передбачати реалізацію ряду взаємопов’язаних процесів, спрямованих на виявлення та попередження загроз. Третій підхід є досить широким, оскільки наголошує, що інформаційна безпека є мультидисциплінарною сферою. Хоча можна погодитися із тим, що вона є саме сферою діяльності, але такий підхід робить її тільки різновидом надання послуг.

Представлені поняття тільки відображають один аспект інформаційної безпеки, пов'язаний з її функціонуванням, та не розкривають інші, які є досить важливими для розуміння її сутності. Оскільки наслідки інформаційних загроз, попередження яких є головною задачею інформаційної безпеки, є суттєвими для суспільства, то не погоджуємося із такими трактуваннями в повній мірі, оскільки вони знижують цінність інформаційної безпеки для суспільства.

Другий напрям, досліджений в науковій літературі, відображає підходи, які акцентують увагу на суб'єктах інформаційної безпеки, які її забезпечують, а саме держави, економічних агентів, особистості (див. табл. 1.3).

Таблиця 1.3 – Узагальнення підходів до визначення інформаційної безпеки з позиції суб'єкту

Зміст підходу	Автор та джерело	Визначення інформаційної безпеки
Інформаційна безпека держави	Ільницька У. [307, с. 28]	Це «інтегрована складова національної безпеки і її розглядають як пріоритетну функцію держави».
	Боднар І.Р. [277, с. 69]	Це «сукупність засобів забезпечення інформаційного суверенітету України, які забезпечують захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз та ефективну протидію сукупності інформаційних загроз».
	Нашинець-Наумова А. [333, с. 110]	«Інформаційна безпека суспільства й держави характеризується ступенем їх захищеності, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості тощо) щодо небезпечних, дестабілізуючих, деструктивних дій, які шкодять інтересам країни».
Інформаційна безпека економічних агентів	Микитенко Т.В., Петровська І.О., Рогов П.Д., Гаркуша А.О. [329, с. 25]	Це «одна із складових частин економічної безпеки, яка формує модель захищеності підприємства. Забезпечення (у тому числі і гарантія) безпеки підприємства пов'язана з інформаційною безпекою внаслідок широкого використання інформаційних технологій в його діяльності».
	Зубок М.І. [305, с. 78]	«Інформаційну безпеку підприємницької діяльності можна розуміти, як стан інформаційної роботи суб'єктів підприємництва за якого забезпечується ефективне інформаційне супроводження їх діяльності, надійний захист інформаційного ресурсу та результативна протидія негативному інформаційно-психологічному впливу на них».

Продовження таблиці 1.3

Зміст підходу	Автор та джерело	Визначення інформаційної безпеки
Інформаційна безпека особистості	Остроухов В., Петрик В. [338, с. 136]	«Інформаційна безпека особистості – це: 1) належний рівень теоретичної і практичної підготовки особистості, при якому досягається захищеність і реалізація її життєво важливих інтересів і гармонійний розвиток незалежно від інформаційних загроз; 2) здатність держави створити можливості для гармонійного розвитку і задоволення потреб особистості в інформації, незалежно від інформаційних загроз; 3) гарантування, розвиток і використання інформаційного середовища в інтересах особистості; 4) захищеність від різного роду інформаційних небезпек».

У визначеннях другого напрямку увага акцентується тільки на тому, хто впроваджує інформаційну безпеку, регулює та використовує. Також дані поняття не враховують спільні риси, притаманні безпеці різних суб'єктів, що дозволяє використовувати загальні підходи та інструменти в процесі організації захисту інформації. Все це обмежує розуміння даного поняття тільки на рівні окремого суб'єкта чи окремої сфери.

Виходячи з проведеного аналізу та синтезу отриманої інформації, узагальненої в таблицях 1.2 та 1.3, застосуємо системний підхід, який дозволить сформувати поняття інформаційної безпеки з урахуванням визначених вище недоліків. Для цього виділимо риси, характерні для більшості визначень інформаційної безпеки, та представимо їх у вигляді схеми (рисунок 1.14). Системний підхід передбачає розгляд та дослідження будь-яких систем з позиції: мети їх функціонування; суб'єктів, які приймають участь у її забезпеченні; об'єктів, які функціонують у певній сфері діяльності та на які направлено інструменти впливу; а також механізмів, що забезпечують виконання та регулювання системи. Згідно із цим, представлення на рисунку 1.14 основних компонент інформаційної безпеки як системи, дозволило сформулювати власне її поняття: інформаційна безпека – це комплексна система, мета функціонування якої – захист об'єктів (інформація, знання, інформаційні системи), що належать до фінансово-господарської, політичної, військової, технологічної сфер діяльності, від різного

роду загроз (несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення) із застосуванням програмних, технічних, методичних, інформаційних та правових засобів, що використовують окремі особи або спеціалізовані підрозділи та фахівці державних органів, економічних агентів.

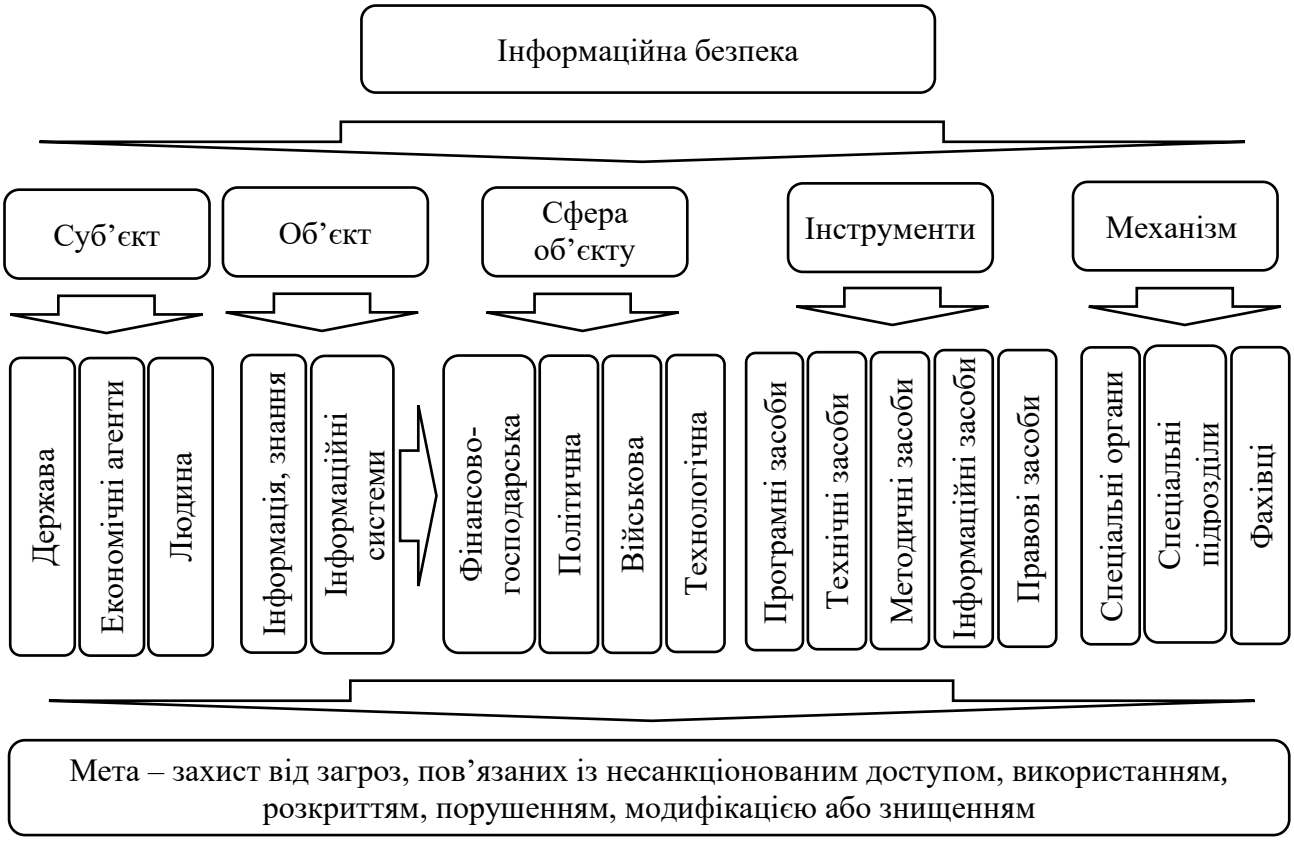


Рисунок 1.14 – Риси інформаційної безпеки (складено авторкою)

Надане поняття є комплексним та охоплює всі складові інформаційної безпеки. Його розуміння дозволяє виділити її ключові компоненти для формування концептуальної моделі її забезпечення в системі управління національною економікою безпосередньо для кожного з її суб'єктів.

Головним тригером, який ініціює необхідність формування інформаційної безпеки, є загрози. Результатом їх впливу, як правило, є негативні наслідки. Для зниження їх рівня слід застосовувати спеціальні заходи інформаційної безпеки, які дозволять виявляти та попереджати загрози. Їх організація потребує фінансових ресурсів, які інвестуються у придбання, розробку та впровадження інструментів безпеки. При чому обсяг фінансування буде залежати від рівня та

важливості наслідків інформаційних загроз для кожного суб'єкта національної економіки. З метою чіткого розуміння процесу забезпечення інформаційної безпеки проаналізуємо, як це здійснюється у державному, підприємницькому секторах та для окремих осіб.

На рисунку 1.15 представлена концептуальна модель забезпечення інформаційної безпеки держави з урахуванням загроз та їх наслідків, де можна побачити, що різного роду загрози впливають на інформацію, знання та інформаційні системи, результатом чого є негативні наслідки для країни. Для попередження загроз повинні існувати відповідні заходи інформаційної безпеки, організація яких пов'язана із джерелами фінансування. Відповідно з представленою моделлю, проведемо характеристику окремих її компонентів.

Рисунок 1.15 – Концептуальна модель забезпечення інформаційної безпеки держави з урахуванням загроз та їх наслідків (складено авторкою)

«Великий тлумачний словник сучасної мови» надає визначення загрози як «можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь» та «те, що може заподіювати яке-небудь зло, якусь неприємність» [292]. «Фізико-технічний словник-мінімум» пропонує розуміти загрозу як «потенційно можливу будь-яку несприятливу дію на інформацію, що може призвести до порушень хоча б однієї з фундаментальних властивостей захищеної інформації» [293]. Тобто визначення, надане словником, пов'язує загрозу із інформацією та її захистом, що вже вказує на її відношення до інформаційної безпеки. Поняття «загроза» наведено також у офіційному нормативно-правовому акті – «Інструкції з проведення аналізу ризиків у Державній прикордонній службі України», згідно з яким загроза – це «наявні та потенційно можливі явища і чинники, що негативно впливають на сферу безпеки державного кордону» [308], хоча дана дефініція більше асоціюється із національною безпекою, ніж із інформаційною.

«Термінологічний навчальний довідник із інформаційної безпеки» визначає загрозу як «будь-яку обставину або подію, що виникають у зовнішньому середовищі, які можуть бути причиною порушення політики безпеки інформації і (або) нанесення збитків автоматизованій системі» [293, с. 177]. Також автори Богуш В.М., Кривуца В.Г., Кудін А.М. виділяють поняття: «загроза безпеці інформації – загроза викрадення, зміни або знищення інформації» [293, с. 177]; «загроза для інформації – витік, порушення цілісності інформації або відмова в авторизованому доступі до неї»; «інформаційна загроза – вплив з боку дестабілізуючих факторів на стан інформованості, що піддає небезпеці інтереси життєво важливі особистості, суспільства і держави» [293, с. 179]; «загроза інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку інтересам життєво важливим особистості, суспільства і держави в інформаційній сфері» [293, с. 180].

Виходячи з представлених дефініцій, сформуємо уточнене поняття інформаційної загрози, яке буде використовуватися в подальшому у даній роботі та яке буде асоціюватися саме із інформаційною безпекою. Інформаційна

загроза – це сукупність цілеспрямованих дій, які ініціюють або пов’язані із об’єктом загрози, або сторонні: особи або групи осіб, або уряд іншої країни з метою здійснення несприятливого або незаконного впливу на інформацію (інформаційну систему, знання та дані), що призводять до порушення цілісності, конфіденційності та доступності, та тим самим створюють небезпеку інтересам особистості, економічним агентам та державі в цілому.

В залежності від суб’єкта інформаційної безпеки, тобто того, для кого її організація є важливим атрибутом збереження інформації та даних, розрізняються й інформаційні загрози. Так, для держави – це інформаційна та кібер-війна, інформаційне та кібер-шпигунство, інформаційний та кібер-тероризм, масштабні кіберзлочини, хактивізм, атаки на електронний уряд (рисунок 1.15).

В сучасних умовах серед країн, які домінують на світовій суспільно-політичній та економічній арені, широкого розповсюдження набуває такий вид інформаційної зброї, як інформаційна війна, яка представляє собою «вид протиборства між різними суб'єктами (державами, неурядовими структурами, економічними агентами, тощо), який здійснюється з метою досягнення односторонніх воєнних, соціально-політичних чи економічних переваг над супротивником» [338, с. 137]. Цей термін вперше було використано Томасом Роном у звіті «Системи зброї й інформаційна війна», де було зазначено, що «інформаційна структура є ключовим компонентом американської економіки», при цьому це найбільш вразлива ціль як у військовий, так й у мирний час [379]. В основному до даної загрози вдаються країни, які при цьому застосовують економічну, психологічну, хакерську, електронну, кібернетичну, розвідувальну, командно-управлінську її форми [332, с. 41]. Для реалізації інформаційної війни використовуються такі інструменти, як пропаганда, чутки, поширення фейків, дезінформація, блокування теле- та радіоефірів. Її наслідки є відчутними у різних сферах – економічній, політичній, соціальній, та полягають у: появі недовіри у населення до дій уряду, що може привести до його розколу та масової еміграції; накладанні міжнародних санкцій на урядові особи або компанії, наслідком чого

може бути міжнародна ізоляція країни; розв'язанні інформаційної війни у відповідь з боку іншої країни.

Інформаційна війна є узагальненим поняттям. Оскільки її основна мета – це викривлення, знищення або викрадення інформації, то будь-яка інша форма буде формою її прояву. Так, окремим її випадком є кібервійна, яка представляє собою масово скоординований цифровий напад однієї країни або великих груп громадян на комп'ютерну периферію та мережі іншої нації з метою заподіяння шкоди чи зриву [208, с. 16]. Для її ведення використовуються наступні інструменти: кібератаки на об'єкти інфраструктури, важливої для здійснення життєдіяльності суспільства та країни; втручання у роботу обладнання, яке виконує адміністративно-контрольні функції у громадських, урядових, комерційних та військових організаціях; порушення роботи програмного забезпечення та веб-сайтів; зламування серверів та веб-сторінок компаній та осіб з метою викрадення інформації [323, с.56–57]. В результаті кібервійн виводиться з ладу програмно-технічне обладнання, що також призводить до втрат інформації. Тому можна вважати кібервійни підвидом інформаційних війн.

Наступним видом загроз є кібершпигунство або комп'ютерне шпигунство, під яким розуміють злочинну діяльність, яка відбувається у вигляді таємного збирання та передачі інформації, що є державною таємницею, представникам іншої держави. Також сюди можна віднести факти здійснення спостереження за окремими громадянами для збору інформації про їх дії, поведінку, тощо. Як правило, це відбувається через інформацію соціальних мереж та профілів користувачів. Тут мова вже йде про інформаційне шпигунство. Кібершпигунство може здійснюватися також через хакерство та проникнення до комп'ютерів та мереж за допомогою шпигунських програм («кротів»)». Дана загроза є досить небезпечною для держави, оскільки критично важлива інформація (військова, наукова, енергетична, тощо) опиняється у руках зловмисників, в результаті це може призвести до дестабілізації різних сфер. Ці види інформаційних загроз призводять до таких критичних наслідків, як соціальна дестабілізація, що проявляється у зміні настроїв населення по відношенню до дій уряду або різних

економічних агентів. Також це може завдати критичних наслідків для політичної ситуації в країні, привести до змін в уряді, тощо. Економічні результати у випадку інформаційного та кібершпигунства будуть найбільш відчутними, оскільки вони, як правило, у більшості випадків націлені на збір інформації щодо фінансових потоків країни.

Наступною серйозною загрозою для суспільства та країни в цілому є інформаційний та кібер-тероризм. Під інформаційним та кібер-тероризмом розуміють навмисну атаку на інформацію та інформаційну систему, а також комп'ютерні мережі, яка має під собою певні політичні або економічні причини, що створює небезпеку для життя та здоров'я людини, або пов'язана із настанням різних тяжких наслідків у випадку, якщо такі дії відбувалися з метою порушення безпеки населення, здійснення провокацій та створення військових конфліктів [285]. Не дивлячись на те, що інформаційний тероризм більше спрямований на загрозу інформації та інформаційним системам, а кібертероризм – на технічне забезпечення та мережі, їх мета – це встановлення незаконного контролю над певними об'єктами задля отримання економічних, політичних та інших переваг. У випадках, коли вимоги терористів не будуть виконані, це може призвести до важких наслідків, головними з яких можуть бути військовий конфлікт, блокування роботи уряду, прийняття несприятливих для країни рішень.

Масштабні кіберзлочини – це різновид хакерських атак, який набуває великих масштабів в межах однієї або декількох країн. Їх мета – це дестабілізація економічної, політичної, соціальної сфер. Вони здійснюються задля викрадення великого обсягу інформації стосовно різних важливих об'єктів державної інфраструктури, а також для порушення їх роботи та виведення з ладу протягом певного періоду часу. Як правило, атаки відбуваються з метою враження певного напряму діяльності, наприклад, на підприємства енергетичної галузі, або урядові органи, або оборонно-промисловий комплекс. При своєчасному їх попередженню такі види загроз можуть призвести до незначних втрат. Це можливо у випадку їх моніторингу по усім країнам світу за допомогою спеціальних сервісів та ресурсів, наприклад, «Лабораторії Касперського» [62].

В останні роки масовості набув такий вид загроз, як хактивізм, пов'язаний із впливом на думку та обізнаність індивідуумів через використання соціальних мереж. Деякі науковці вважають, що це є безкорисливе хакерство, яке здійснюється в політичних цілях [340, с. 345]. Але головна мета даного виду загроз – це порушення цілісності інформації, що призводить до її викривлення. В більшості випадків наслідки хактивізму призводять до дестабілізації політичної ситуації країни, що врешті-решт може вплинути й на інші сфери життєдіяльності суспільства.

Атаки на електронний уряд – це вид інформаційних загроз, які відбуваються з метою зламування урядових електронних ресурсів (веб-сайтів, баз даних, мобільних додатків, тощо) для порушення стабільності їх роботи, організації витоку інформації, викривлення даних. Аналогічного роду атаки використовуються групою осіб однієї країни для втручання у керування іншої. Виникнення подібних інцидентів впливає практично на всі сфери життєдіяльності, а подолання їх наслідків може вимагати великих обсягів фінансових ресурсів та часу.

Перелічені в даній роботі інформаційні загрози за часту траплялися у реальному житті, тому приклад десяти найбільш відомих з них, а також відповідних ним інструментів, за допомогою яких вони були реалізовані, представлений у таблиці 1.4.

Таблиця 1.4 – Десять випадків інформаційних загроз у державному секторі, які мали найбільші наслідки для економіки країни

Рік	Країна – об’єкт загрози	Інформаційна загроза	Інструмент загрози
2007	Естонія	Кібервійна з метою послаблення національної безпеки країни [255]	Кібератаки проти урядових сайтів, серверів, служб
2008	Грузія	Кібервійна з метою послаблення національної безпеки країни [272]	Кібератаки щодо відмови в обслуговуванні урядових веб-сайтів та засобів масової інформації; DoS-атаки великих підприємств

Продовження таблиці 1.4

Рік	Країна – об’єкт загрози	Інформаційна загроза	Інструмент загрози
2008	США	Інформаційне шпигунство з метою викрадення інформації з інформаційної системи Центрального командування Збройними силами США [224]	Вірусна атака, що відбувалася за допомогою комп’ютерного хробака “Agent.btz”
2013-2016	Україна	Російсько-українська кібервійна, направлена на дестабілізацію різних сфер діяльності в Україні [354]	Серія кібератак із використанням: комп’ютерного хробака “Змія”; DoS-атак на автоматизовану систему “Вибори”; троянської програми “BlackEnergy”; шкідливої програми “Прикормка”; троянської програми “KillDisk”
2015	Німеччина	Атака на електронний уряд – на інформаційну систему Бундестагу [101]	Хакерська кібератака, електронні листи із цільовим фішингом
2016	Україна	Атака на електронний уряд – урядовий сайт Держказначейства України [335]	Вірусна атака з використанням троянської програми “KillDisk”
2016	Бангладеш, США	Кіберзлочин з метою викрадення золотовалютних резервів Бангладеш, які знаходились у Федеральному резервному банку Нью-Йорка [16]	Хакерська кібератака, електронні листи із цільовим фішингом
2016	США	Інформаційне шпигунство з метою викрадення інформації з інформаційної системи Національного комітету Демократичної партії США [182]	Кібератака на мережу DNS
2017	США	Атака на електронний уряд – веб-сайт Державного департаменту [256]	Хакерська кібератака
2017	США	Масштабний кіберзлочин – атака на співробітників атомних електростанцій [95]	Електронні листи із цільовим фішингом

З таблиці 1.4 можна побачити, що географія об’єктів загроз, їх мета та інструменти здійснення є достатньо різноманітними. Це свідчить, що на сьогодні вони є масовим явищем. Також слід відмітити, що вони можуть бути, як внутрішніми, так й зовнішніми по відношенню до суб’єкта безпеки, тобто виникати з боку іншої держави, що буде характеризувати їх як зовнішні, або з боку кіберзлочниців, які територіально знаходяться в межах країни – суб’єкта загрози, що буде характеризувати їх як внутрішні.

Можна прослідкувати (див. табл. 1.4), що інструменти загроз є досить схожими, тому заходи безпеки можуть бути типовими для багатьох випадків інцидентів. Як правило, це (рисунок 1.15):

1) правові заходи, які представляють собою норми законодавства та передбачають різні види відповідальності за інформаційні та кіберзагрози, включаючи й кримінальну, що може бути серйозною перепоною для кіберзлочинців. Дане питання потребує чіткої регламентації всіх правових норм;

2) програмні заходи, які є найбільш дієвими та поширеними, оскільки дозволяють попереджувати різні кіберінциденти без участі людини. Вони реалізуються із використанням спеціальних програм захисту та виявлення вірусних та кібернетичних атак, а також шахрайських дій кіберзлочинців. Даний напрям потребує розробки програм для захисту мережі, комп'ютерів, інформаційної системи, тощо;

3) технічні заходи, які представляють собою спеціалізовані технічні пристрої, що здійснюють захист інформації та інформаційної системи. Як правило, вони поєднуються із програмними заходами;

4) технологічні заходи, необхідні для удосконалення технології процесів виявлення вразливостей в системі інформаційної безпеки. Їх реалізація – це спосіб попередження майбутніх інцидентів, тому від ефективності їх здійснення буде залежати й потенційна надійність системи захисту;

5) інформаційні заходи, які включають всі можливі напрямки удосконалення інформаційного забезпечення системи, що також є попереджувальним заходом. Вони повинні передбачати ймовірні злочинні дії із масивами та файлами даних, а також формувати способи їх розподіленого використання та шифрування;

6) організаційні заходи, які полягають у створенні відповідних органів реагування та виявлення інцидентів загроз, а також у розробці методичних інструкцій щодо регулювання процесів, пов'язаних із захистом інформації, даних та інформаційних систем.

Формування дієвих заходів інформаційної безпеки потребує відповідного фінансування (рисунок 1.15). Перший його напрямок – це інвестиції, які здійснюються у розвиток інструментів протидії загрозам. Як правило, він потребує економічного обґрунтування, оскільки заходи безпеки не є прибутковими для державних органів та економічних агентів. Другий напрям пов'язаний із розробкою превентивних заходів безпеки, тобто таких, впровадження яких забезпечить виявлення інцидентів загроз на початковому етапі, або не дозволить проникнення хакерів до комп’ютерів та мережі. Третій напрям необхідний для поточного фінансування заходів безпеки та підтримки їх в актуальному стані. Також можна окремо виділити фінансування тих витрат, які необхідно здійснити у разі відновлення втрачених даних, а також тих втрат, які понесла держава у разі виникнення інформаційних загроз, та попередження яких було невчасним.

Що стосується забезпечення інформаційної безпеки економічних агентів (суб’єктів підприємницької діяльності, банків, страхових компаній, тощо), то її концептуальна модель представлена на рисунку 1.16. Порівнюючи моделі забезпечення інформаційної безпеки держави та економічних агентів (рисунок 1.15 та 1.16), можна виділити багато спільних рис, характерних для заходів, об’єктів безпеки та напрямів фінансування. Відмінності полягають у масштабах та характерах наслідків, а також у різновидах загроз. Так, для економічних агентів вплив інформаційних загроз відчувається на результатах їх господарської діяльності, що може призвести до повної її паралізації, а згодом стати причиною банкрутства. Для держави характер наслідків також може бути масштабним, але вони не призводять до повної руйнації економіки країни, а тільки до гальмування її розвитку.

Що стосується передумов формування системи інформаційної безпеки економічних агентів, то її необхідність також викликана зростанням кількості кіберінцидентів, які відбуваються завдяки впливу різного роду загроз, що зачіпають різні сфери підприємницької діяльності по всьому світу.

Рисунок 1.16 – Концептуальна модель забезпечення інформаційної безпеки економічних агентів (складено авторкою)

Наприклад, електронні напади на систему контролю стічних вод Maroochy Shire в Австралії (2000 р.) [217]; кібератака на нафтову компанію Saudi Aramco та компанію по видобуванню газу RasGas (Саудівська Аравія, Катар, 2012 р.) [29]; кібератаки на енергетичні компанії України (2015 р., 2016 р.) [334]; фішингова атака на інженерні організації та служби промислової системи управління у Великобританії (2017 р.) [59]; фішингова атака на співробітників атомних електростанцій США (2017 р.) [95]; витік конфіденційних даних більше ніж 100 компаній світу, в тому числі Ford, Tesla, Toyota, General Motors, Fiat Chrysler, Volkswagen, ThyssenKrupp, завдяки відсутності обмежень на Rsync-сервері, який належав компанії Level One Robotic (2018 р.) [214]; втрата персональних даних

користувачів MasterCard завдяки збою в платформі лояльності, яка перебувала в управлінні сторонньої компанії (Німеччина, 2019 р.) [30]; викрадення записів платіжних карток з муніципальної платіжної системи Click2Gov США завдяки існуванню вразливостей та порушень у роботі системи (2019 р.) [202]; викладення у відкритий доступ 250 млн. записів особистих даних клієнтів Microsoft за рахунок неправильного налаштування бази даних Elasticsearch (США, 2020 р.) [201]; зламування більше 2000 інтернет-магазинів Magento завдяки впровадженню шкідливого скрипту (2020 р.) [49] та інші.

Що стосується рівня окремих індивідуумів, то концептуальна модель забезпечення їх персональної інформаційної безпеки представлена на рисунку 1.17.

Рисунок 1.17 – Концептуальна модель забезпечення персональної інформаційної безпеки індивідів (складено авторкою)

Можна відмітити, що окрім зазначених вище загроз, характерних також й для рівня держави та економічних агентів, для окремих індивідів найбільш

суттєвою є соціальна інженерія (рисунок 1.17), яка полягає у застосуванні різних способів маніпулювання людьми з метою отримання персональних фінансових даних, а також паролів доступу до особистих сторінок, поштових скриньок та акаунтів. Вона є розповсюдженою кіберзагрозою для клієнтів банків. Низька обізнаність щодо заходів інформаційного захисту є причиною недбалого ставлення людини до персонального захисту в процесі здійснення операцій із використанням мобільних та комп'ютерних пристроїв, що призводить до втрати інформації. Наслідками впливу інформаційних загроз для окремої людини є втрата даних, грошових коштів та пристроїв. За умови використання заходів попередження та заходів поточного захисту можна підвищити рівень персональної безпеки для кожної окремої людини.

Для забезпечення функціонування системи інформаційної безпеки на державному рівні та рівні економічних агентів необхідне формування ефективного механізму, тобто комплексу суб'єктів-виконавців, що будуть безпосередньо здійснювати захист інформації та інформаційних систем з урахуванням нормативно-правових вимог (див. табл. 1.5). Це можливо тільки за рахунок створення низки відповідних виконавчих органів, функції яких будуть безпосередньо пов'язані із захистом, координацією, контролем для забезпечення державної інформаційної безпеки, та захистом, фізичним, логічним та адміністративним контролем безпеки підприємств та фінансових установ. В таблиці 1.5 наведено перелік таких виконавців, хоча для рівня економічних агентів це також можуть бути певні інструменти (політики, процедури, стандарти, керівні принципи та інструменти, а також програмне забезпечення для моніторингу та контролю доступу), використання яких дозволяє підвищити ефективність дії механізму в системі забезпечення інформаційної безпеки. Також це можливо за рахунок комплексного функціонування всіх компонентів системи безпеки під управлінням нормативно-правової бази, яку сформували відповідні закони України, укази Президента, державні та міжнародні стандарти з питань інформаційної безпеки.

Таблиця 1.5 – Механізм забезпечення інформаційної безпеки на рівні держави та економічних агентів

Суб'єкт безпеки	Виконавці (інструменти)		Правова база
	Функція	Представник	
Державний сектор	Координація і контроль	Рада національної безпеки і оборони України	Закони України № 2657-XII [297], № 80/94-ВР [302], № 3855-XII [299], № 2297-VI [296], № 2163-VIII [295], № 537-V [300], №47/98-ВР [301], Концепція ІБ України [313], Укази Президента України № 47/2017 [366], № 96/2016 [365]
	Основні функції захисту	СБУ (Державна служба спеціального зв'язку та захисту інформації України; CERT-UA), МВС України, Міністерство оборони України, Служба зовнішньої розвідки України, Центральний орган виконавчої влади із спеціальним статусом	
Підприємницький та фінансовий сектор	Основні функції захисту	Служби безпеки, служби захисту інформації	ISO 15443: "IT – Методи безпеки – Основи забезпечення IT-безпеки" [131]; ISO /IEC 27002: "IT – Методи безпеки – Кодекс практики управління ІБ" [130]; ISO-20000: "IT – Управління послугами" [127]; ISO / IEC 27001: "IT – Методи безпеки – Системи управління ІБ - Вимоги" [129] *IT – інформаційні технології
	Фізичний контроль	Адміністратори сервера, адміністратори бази даних	
	Логічний контроль	Програмне забезпечення для моніторингу та контролю доступу	
	Адміністра-тивний контроль	Політики, процедури, стандарти, керівні принципи	
	Інші функції	Служби внутрішнього аудиту (Сертифіковані аудитори інформа-ційних систем), служби фінансового моніторингу та НБУ (для банків)	

Підсумовуючи все вище наведене, представимо інформаційну безпеку у вигляді концептуальної моделі її забезпечення в системі управління національною економікою (рисунок 1.18). Основними детермінантами її архітектоніки є зовнішні та внутрішні загрози, що впливають на порушення цілісності, конфіденційності та доступності інформації, знань і безпосередньо інформаційних систем суб'єктів, у результаті чого виникають деструктивні наслідки для економічного, соціального та політичного розвитку країни. Для їх попередження і виявлення інцидентів на рівні держави, суб'єктів господарювання, фінансових інститутів та індивідуумів повинна бути сформована відповідна організаційно-правова структура, ефективність функціонування якої повинна оцінюватися за обсягами зменшення втрат національної економіки від дій інсайдерів та кібершахраїв.

Рисунок 1.18 – Концептуальна модель забезпечення інформаційної безпеки (ІБ) в системі управління національною економікою

Також модель, представлена на рисунку 1.18, дозволяє окреслити потенційні напрями забезпечення ефективної системи інформаційної безпеки національної економіки, такі як: інтегральне оцінювання рівня її загроз, оцінка ресурсного потенціалу країни для забезпечення інформаційної безпеки, формування ефективної моделі національної інформаційної безпеки, оцінювання ефективності інформаційної системи та інформаційної безпеки, ризиків втрат інформації, прийняття рішення щодо ребілдингу інформаційної безпеки із використанням сучасних технологій, оптимізація бізнес-процесів захисту, удосконалення системи інформаційного забезпечення, застосування інтелектуального аналізу даних, конвергенція системи інформаційної безпеки та фінансового моніторингу. Їх дослідженню, удосконаленню та розробці будуть присвячені наступні розділи даної дисертаційної роботи.

1.3 Структуризація наукового доробку щодо напрямів дослідження інформаційної безпеки

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

Але є й негативний бік, пов'язаний із зростанням різного роду інформаційних загроз, які призводять до втрати інформації в результаті здійснення хакерських атак, її незаконного використання у кримінальних цілях. Саме тому виникає необхідність у створенні ефективної системи інформаційної безпеки, яка б забезпечувала захист даних компаній, окремої людини, країни. Відповідно дана потреба заслуговує на увагу з боку науковців, що повинно проявлятися у збільшенні не тільки кількості наукових публікації з даної тематики, але й підвищенні їх якості та рівня за умови їх оприлюднення у виданнях, які індексуються у міжнародних базах, таких як Scopus та Web of Science. Але цінності набувають ті наукові праці, які висвітлюють результати дослідження проблеми не у загальному вигляді, а її вирішення для певної сфери діяльності. Тому важливо дослідити питання інформаційної безпеки в розрізі різних аспектів, особливо у зв’язку із напрямами економіки. Це пов’язано із тим, що в першу чергу, наслідки інформаційних загроз відчуваються через втрати особистих коштів клієнтів банків, секретних даних компанії щодо фінансових операцій, недоотримання прибутків через відновлення втрачених даних та відтік клієнтів, тощо. Тобто спостерігається певний зв'язок між рівнем інформаційної безпеки та економікою країни. Саме тому даний аспект потребує детального вивчення.

Проблемі реалізації інформаційної безпеки в розрізі економічного розвитку країни присвячено ряд публікацій вітчизняних науковців, які в основному спрямовані на вирішення загальних завдань на теоретичному рівні та не мають системного продовження. Так, Світлична В.Ю. досліджує сутність поняття інформаційної безпеки для підприємств [357]. Нехай В.А., Нехай В.В. розглядають її у якості складової економічної безпеки суб’єктів господарювання [336]. Любохинець Л.С., Поплавська О.В. вивчають світову практику забезпечення інформаційної безпеки та аналізують вплив інформаційних загроз на стан економіки [325]. Вашай Ю.В., Самедова Л.Р. [283], Боднар І.Р. [277] досліджують вплив інформаційної безпеки на стан національної та економічної безпеки держави. Колектив авторів – Шевченко Л.С., Гриценко О.А.,

Макуха С.М., Дарнопих Г.Ю., Левковець О.М., Мамалуй О.О., Марченко О.С., Нечипорук Л.В., Овсієнко О.В., Губін К.Г., Єфіменко І.А., розглянули теоретичні основи економічної безпеки на рівні держави в умовах інноваційного її розвитку [376]. Микитенко Т.В., Петровська І.О., Рогов П.Д., Гаркуша А.О. висвітлюють проблеми інформаційної безпеки суб'єктів господарювання та розробили можливі напрями їх вирішення [329].

Вирішенням проблеми, пов'язаної із процесом реформування системи інформаційної безпеки країн, які відносяться до НАТО, займаються Лошицький М., Костенко О., Коропатник І., Терещук Г., Карелін В. [167]. Розробці захисту критичної інфраструктури держави присвячена праця Гнатюка С., Сидоренко В., Положенцева А., Фесенко А. [106]. Вагомий аспект інформаційної безпеки – це виникнення та попередження загроз, серед яких найбільший вплив здійснює інформаційна війна. Тому цю проблему держави висвітлюють Чижмар К., Дніпров О., Коротюк О., Шаповал Р., Сидоренко О. [48]. Вплив інформаційних війн на безпеку підприємств досліджує Сороківська О. [219]. Також можна виділити науковців, які займаються розробкою системи комплексної оцінки рівня культури інформаційної безпеки на рівні персоналу, а саме Шкарлет С., Литвинов В., Дорош М., Трунова Е., Войцеховська М. [213]. Для боротьби із інформаційними загрозами та для забезпечення належного рівня безпеки існує потреба в розробці та впровадженні ряду комплексних підходів. В цій сфері можна виділити дослідження Євсєєва С., Алексієва В., Балакірєва С., Пелешка Ю., Милова О., Петрова О., Раєвнєвої О., Томашевського Б., Тишика І., Шматька О. та інших.

Науковий доробок вітчизняних вчених є значним, але результати більшості наукових праць носять суто теоретичний характер та публікуються переважно у вітчизняних виданнях. Це пов'язано із тим, що проблемами інформаційної безпеки в Україні активно почали займатися тільки протягом останнього десятиліття, коли з'явилася потреба у навчанні фахівців з даного напряму. Також починають формуватися наукові школи, які займаються дослідженням в галузі інформаційної безпеки. Саме тому зарубіжний досвід наукової спільноти з

вирішення проблеми інформаційної безпеки у розрізі її впливу на економічний розвиток країни є необхідним для подальшого формування наукових напрямів в даній сфері.

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

На першому кроці було досліджено динаміку публікацій, які присвячені темі «Інформаційна безпека». Так, однією з перших публікацій у базі даних Scopus, яка розкриває проблематику захисту інформації та інформаційної безпеки, була стаття 1967 року Дж. Б. Денніса під назвою «A position paper on computing and communications» [69]. Автор цієї праці розглядав суто технічні аспекти розробки положень інформаційної безпеки для розвитку публічних комунікаційних послуг з комутацією повідомлень.

Популярність цього напрямку досліджень починає стрімко зростати з 2000 року, тому для подальшого аналізу було узято період 2000-2019 рр. Для порівняння тенденцій публікаційної активності також було використано дані бази даних Dimensions, яка представляє собою інформаційну платформу для пошуку та доступу академічних та інших результатів досліджень. Вона містить більш ніж 128 млн. публікацій, баз даних, грантів, патентів, політик тощо. Результати дослідження представлені на рисунку 1.19.

Було виявлено, що за останні 20 років спостерігається стрімке зростання зацікавленістю проблемами інформаційної безпеки у світі серед науковців (рисунок 1.19). Так, у 2019 році було опубліковано 2347 наукових праць, індексованих у базі Scopus, у порівнянні із 120 публікаціями 2000 року. Різке зростання також спостерігається й по даним Dimensions: 17643 наукових праць у 2019 році на противагу 728 публікацій у 2000 році. Дана тенденція пояснюється тим, що якраз в останні роки відбувається стрімке збільшення комп’ютеризації

та цифровізації різних сфер діяльності суспільства, обумовлене наслідками революції 4.0.

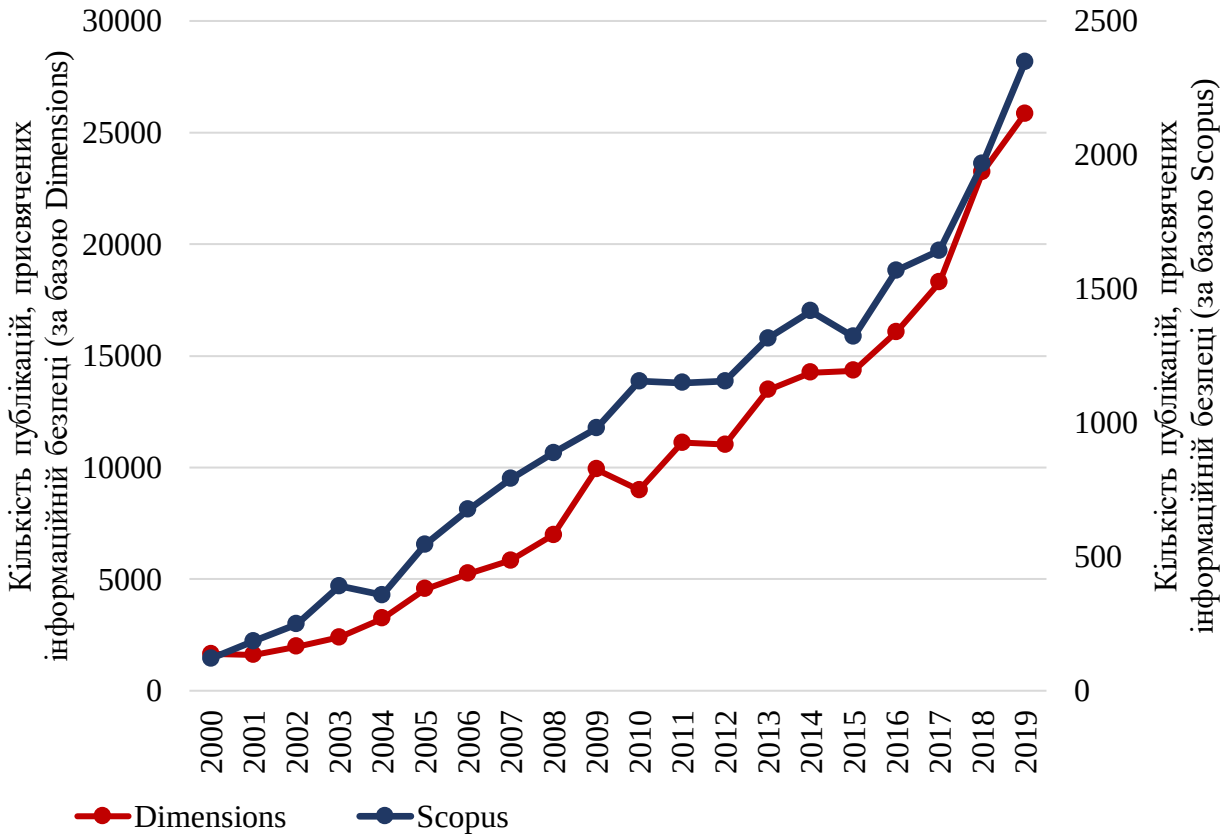


Рисунок 1.19 – Динаміка публікацій, присвячених темі «Інформаційна безпека»
Джерело: побудовано авторкою на основі бази даних Scopus та Dimensions

Зросла кількість користувачів Інтернету, мобільних телефонів, програмних додатків. Основну масу платіжних операцій переведено на мобільні та комп'ютерні платформи. Як наслідок, підвищився рівень кіберзлочинів, що вплинуло на забезпечення потреби інформаційної безпеки для бізнесу, населення та держави в цілому. З розвитком технологій штучного інтелекту, віртуальної, доповненої реальності, роботизації ця потреба тільки зростатиме. Які ж сфери, де гостро стоїть питання підвищення ефективності системи інформаційної безпеки, досліджуються вченими? Так, на рисунку 1.20 представлена діаграма розподілу публікацій, присвячених даній проблемі, за предметною областю. 40% публікацій досліджують проблематику інформаційної безпеки у сфері комп'ютерних наук, тобто вивчаються різні сучасні комп'ютерні технології, які

дозволяють підвищувати ефективність системи інформаційної безпеки, знижувати ризики втрати інформації, забезпечувати захист даних, попереджати виникнення різного роду загроз, тощо (рисунок 1.20).

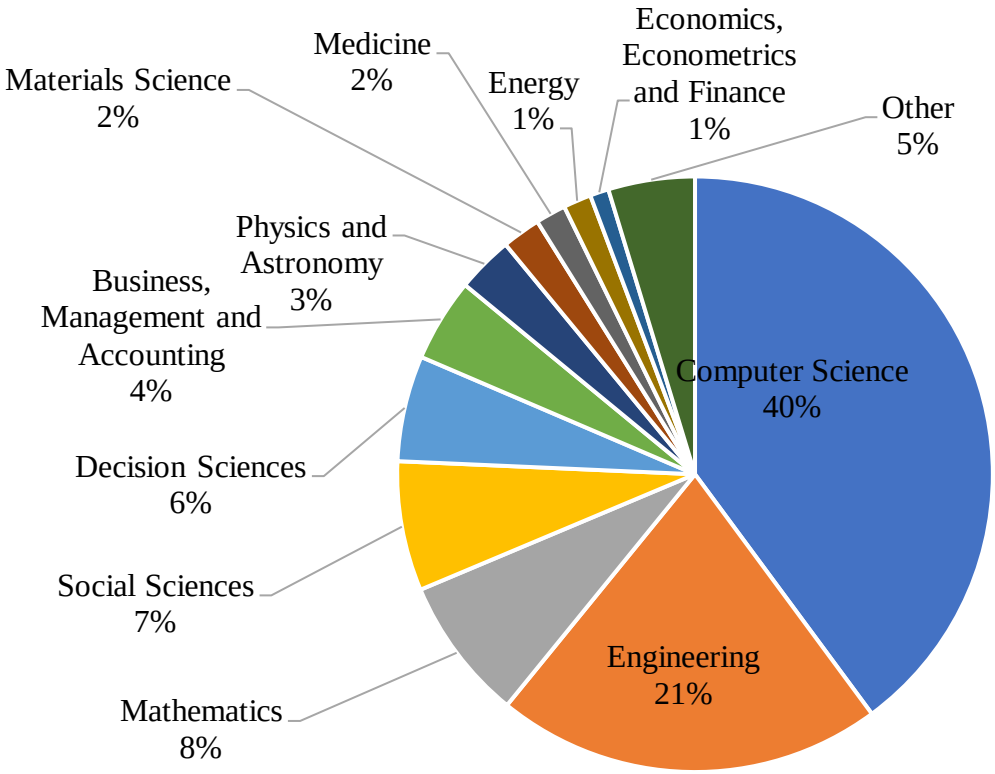


Рисунок 1.20 – Діаграма розподілу публікацій, присвячених темі «Інформаційна безпека», за предметною областю

Джерело: побудовано авторкою на основі бази даних Scopus

Наступний сектор – це інженерія (21%), де проводяться дослідження щодо розробки, удосконалення технічних пристроїв, функціонування яких забезпечують захист інформації на належному рівні. Також можна відмітити вклад науковців (8%), який стосується дослідження проблем інформаційної безпеки із використанням математичних методів та алгоритмів. Що стосується сфери економічного розвитку, то кількість наукових досліджень становить приблизно 1 %, що говорить про незначний рівень зацікавленості з боку наукової спільноти щодо вивчення взаємозв’язків між розвитком економіки країни та рівнем її інформаційної безпеки. Але динаміка публікацій за останні 20 років змінилася (рисунок 1.21).

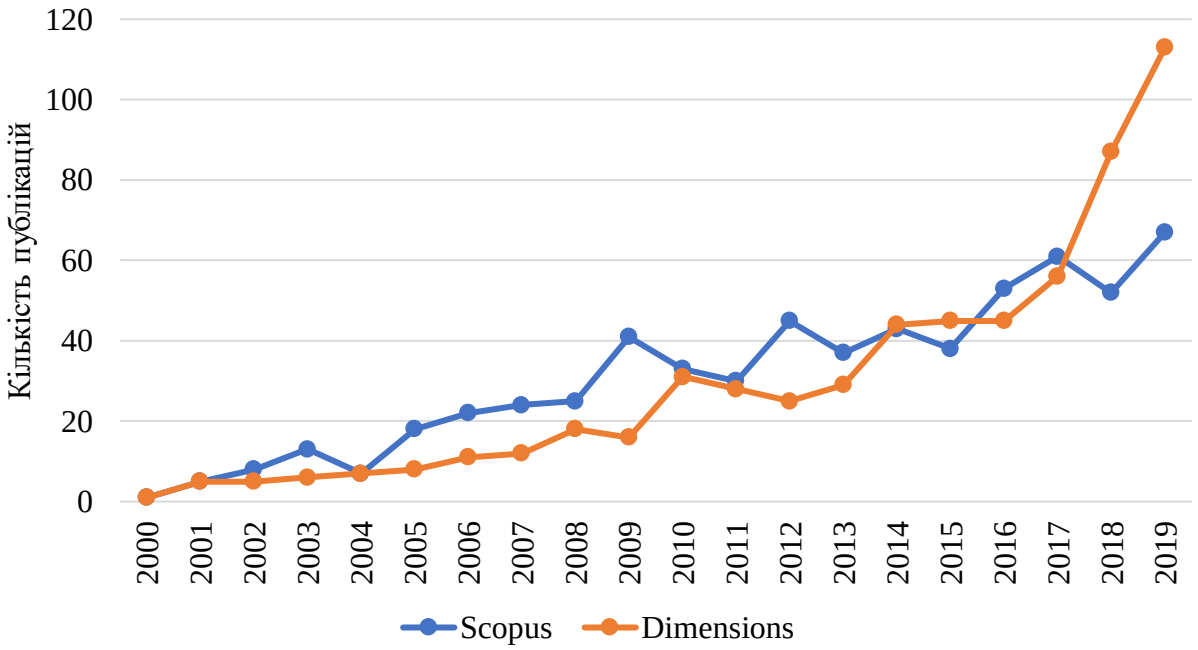


Рисунок 1.21 – Динаміка публікацій, присвячених темі «Інформаційна безпека» з урахуванням сфери економічного розвитку

Джерело: побудовано авторкою на основі бази даних Scopus та Dimensions

Так, при порівнянні даних бази Scopus та Dimensions можна побачити поступове збільшення кількості наукових праць, що свідчить про формування нових векторів розвитку економіки з урахуванням впливу сучасних комп'ютерних технологій, появи суттєвих проблем захисту фінансової інформації компаній та населення країни. Оскільки деякі аналітичні компанії, такі як "Juniper Research", прогнозують збільшення фінансових втрат завдяки підвищенню рівня кіберзлочинності до 5 трлн. дол. у 2024 році [179], то можна з упевненістю сказати, що питання впливу інформаційної безпеки на розвиток економіки буде привертати до себе більше уваги, ніж зараз.

Якщо проаналізувати географію проведених досліджень, то можна виділити 10 країн, науковцям із яких належить найбільша кількість публікацій, присвячених вивченню проблеми інформаційної безпеки та її впливу на розвиток економіки країни (див. рис. 1.22).

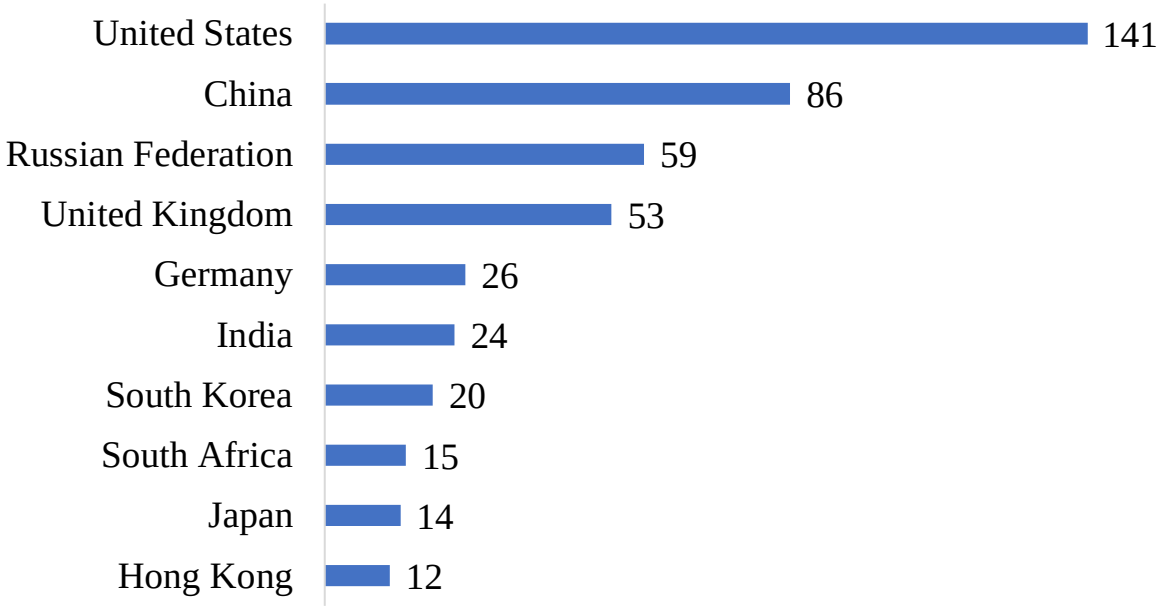


Рисунок 1.22 – Географія проведених досліджень, присвячених проблемі інформаційної безпеки у розрізі її впливу на економічний розвиток

Джерело дослідження: побудовано авторкою на основі бази даних Scopus

Найбільша кількість досліджень проводиться вченими США. Це відбувається у зв'язку із тим, що ця країна є передовою в сфері розробки інноваційних технологій. Також саме в цій країні функціонують інноваційні такі компанії-гіганти, як Apple, Google, Microsoft, IBM, Oracle Corporation, Intel, Cisco Systems та інші, які займаються дослідженнями та практичною реалізацією сучасних програмних, комп'ютерних, електронних та інших технологій в сфері захисту інформації. Друге місце в даній сфері належить китайським вченим. Це обумовлюється стрімким розвитком Китаю та його прагненням бути найсильнішим лідером у світі, що проявляється у створенні корпорацій-гігантів, таких як Lenovo, Huawei, Tencent, Megvii Technology. Також уряд Китаю запровадив програму, згідно з якою відбуватиметься інвестування 1,4 трлн. дол. протягом 6 років до 2025 року приватних технологічних компаній [47], що може визвати сплеск наукових досліджень в сфері інформаційної безпеки.

Що стосується академічних результатів, то було обрано ряд університетів, які опублікували найбільшу кількість статей, присвячених проблемі

інформаційної безпеки в розрізі її впливу на економіку країни. Результати представлені у таблиці 1.6.

Таблиця 1.6 – Рейтинг університетів за кількістю публікацій, присвячених дослідженню інформаційної безпеки в розрізі економічного розвитку країни

№	Назва університету	Країна	Кількість публікацій
1	Університет Карнегі Меллона	США	13
2	Південно-східний університет Нанкіна	Китай	11
3	Кембриджський університет	Великобританія	10
4	Міський університет Гонконгу	Китай	8
5	Університет штату Меріленд	США	6
6	Північно-китайський університет електроенергетики	Китай	6
7	Санкт-Петербурзький державний економічний університет	Російська Федерація	6
8	Техаський університет у Сан-Антоніо	США	5
9	Університет Пердью	США	5
10	Норвезький університет науки і техніки	Норвегія	5
11	Флоридський Атлантичний університет	США	5
12	Токійський університет	Японія	5
13	Російський економічний університет імені Р.В. Плеханова	Російська Федерація	5
14	Індійський інститут технологій у Делі	Індія	5
15	Школа бізнесу Роберта Х. Сміта	США	5

Джерело: побудовано авторкою на основі бази даних Scopus

Серед наведених у таблиці 1.6 університетів найбільша кількість наукових праць належить саме університетам Сполучених Штатів Америки, що підтверджує попередні висновки стосовно провідної ролі даної країни у сфері дослідження інформаційної безпеки. Тобто й бізнес, й академічна спільнота цієї країни працюють більш продуктивно, ніж інші країни, й намагаються синхронізувати результати науки та практики.

Окрім розгляду загальних показників також було проаналізовано рейтинг журналів, в яких було опубліковано найбільшу кількість статей з теми дослідження (див. табл. 1.7). Три журнали мають досить високий імпакт-фактор – SNIP > 1 (кількість публікацій складає 3,67%), три журнали мають значення SNIP > 0,5 (кількість публікацій складає 7,34%). Тобто близько 11%

статей було опубліковано у достатньо рейтингових журналах, що не є високим показником. Це можна пояснити тим, що проблеми інформаційної безпеки найбільше вирішуються для комп'ютерної та програмної сфер, тому такий результат обумовлюється специфікою дослідження захисту інформації саме для потреб економіки.

Таблиця 1.7 – Рейтинг журналів за кількістю публікацій, присвячених дослідженню інформаційної безпеки в розрізі економічного розвитку країни

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

Джерело: побудовано авторкою на основі бази даних Scopus

Також було виділено 10 найбільш цитованих публікацій, присвячених дослідженню інформаційної безпеки в розрізі економічного розвитку країни (див. табл. 1.8).

Серед найбільш рейтингових публікацій можна виділити 2 напрями наукового дослідження: економічні аспекти забезпечення інформаційної безпеки та вивчення взаємозв'язків системи інформаційної безпеки із економічним середовищем. Так, до першого напрямку належать публікації 1, 3, 4, 6, до другого – 2, 5, 7, 8, 9, 10 (див. табл. 1.8). Представлені рейтингові публікації відносяться до періоду 2000-2010 рр., тобто за останні 10 років публікації такого рівня відсутні, що говорить про зниження зацікавленості наукової спільноти до даної проблеми або більш ймовірну зміну вектору досліджень.

Таблиця 1.8 – Десять найбільш цитованих публікацій, присвячених дослідженню інформаційної безпеки в розрізі економічного розвитку країни

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

Джерело: побудовано авторкою на основі бази даних Scopus

Якщо аналізувати десятку публікацій за період 2011-2020 рр., які є менш цитованими, то можна виділити такі напрямки дослідження, як інвестування у

галузь захисту інформації, розвиток сервісів для користувачів мобільних додатків, Інтернету, застосування сучасних технологій для забезпечення безпеки даних в різних сферах бізнесу, тощо. Тобто, дослідження охоплюють й програмну, технічну та економічну сфери у сукупності, тобто є більш мультидисциплінарними.

Для більш чіткого розуміння тенденцій сучасних досліджень обрані публікації бази даних Scopus, які присвячені проблемі інформаційної безпеки в розрізі економічного розвитку країни, було проаналізовано з використанням аналітичної платформи VOSviewer [75]. Даний інструмент дозволяє здійснювати візуалізацію бібліометричних мереж на основі цитувань, співцитувань, бібліографічних зв'язків, авторів, ключових слів, тощо. Так, було побудовано мережеву карту співавторів наукових досліджень, присвячених інформаційній безпеці у контексті предметної галузі – економіка (рисунок 1.23), де представлено авторів, які мають мінімум 1 статтю з даного напряму. Виявилося, що таких науковців – 759 осіб, при чому перетинів у спільних дослідженнях практично не має. Науковців, які представили результати досліджень більше, ніж 2 публікації – 64 особи, 3 публікації – 14 осіб, 4 публікації – 7 осіб, 5 публікацій – 8 осіб. Це говорить про те, що на сьогодні ще не сформовано стійкі дослідницькі групи авторів або наукові школи, які б опрацьовували економічний напрям досліджень інформаційної безпеки. На нашу думку, це обумовлено тим, що дана сфера є доволі молодою, тому розробка економічного аспекту є програмою майбутніх наукових проектів.

Якщо проаналізувати часові періоди, які відповідають проведеним дослідженням, то на рисунку 1.23 можна побачити досить рівномірний розподіл досліджень авторів за роками, хоча за останні 10 років їх кількість дещо зросла, що відповідає градації кольору від синього до жовтого.

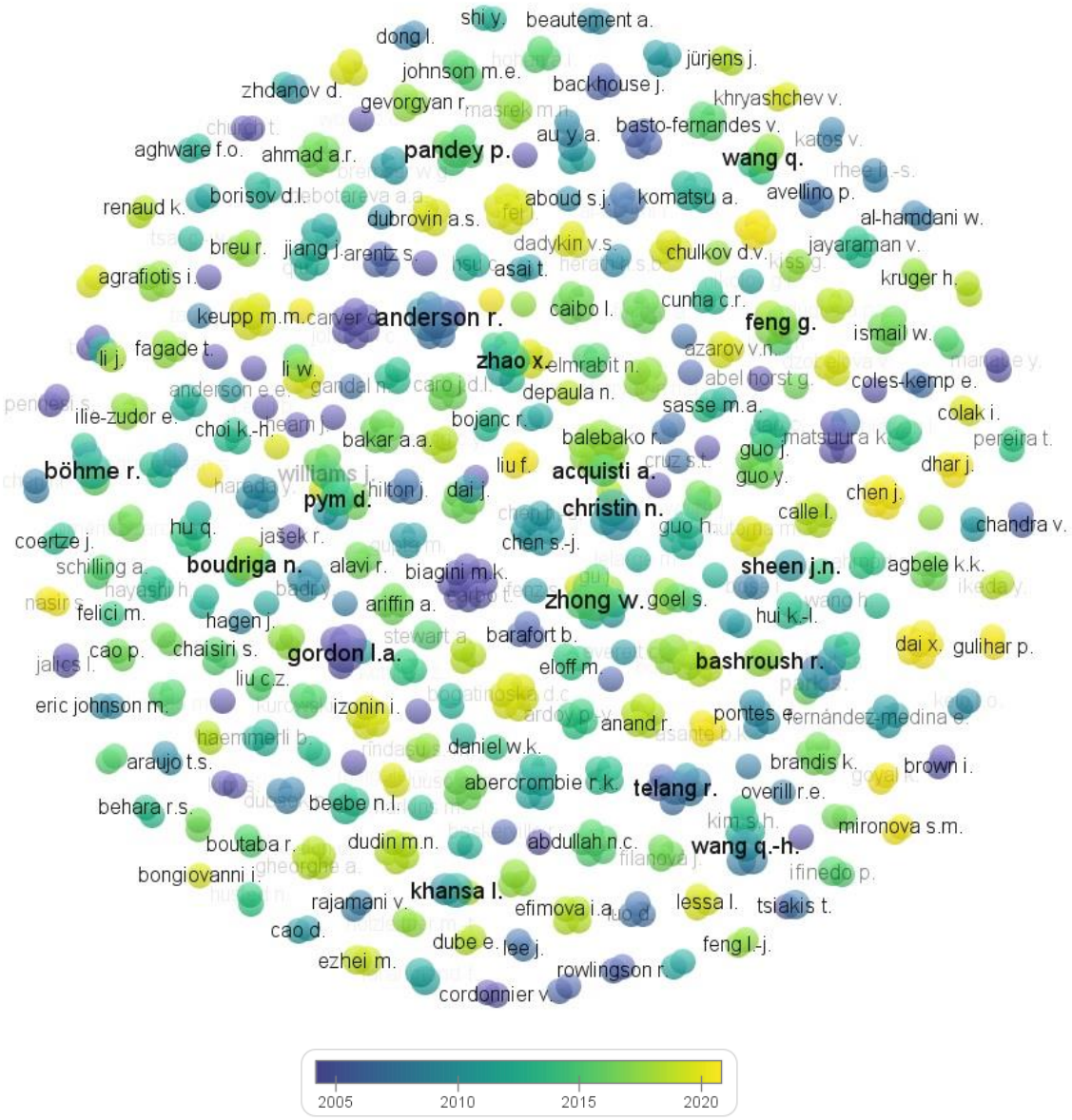


Рисунок 1.23 – Мережева карта співавторів, які проводять дослідження інформаційної безпеки у розрізі економіка

Джерело: побудовано авторкою на основі бази даних Scopus

Що стосується географії авторів публікацій (рисунок 1.24), то тут також можна відмітити відсутність стійких зв’язків між проведеними дослідженнями, які представлені широким колом країн. Так, всього задіяно 68 країн, серед яких основний внесок у вирішені проблеми інформаційної безпеки у економічному контексті належить: США (96 публікацій), Китаю (45), Великобританії (39), Російській Федерації (21), Німеччині (19). Авторам з таких країн як Австрія, Гонконг, Малайзія, Японія, Канада, Південна Корея, Тайвань, Норвегія,

Південна Африка, Індія, Сінгапур, Італія, Туніс, Фінляндія, Австралія, Греція, Румунія, Бразилія, Франція, Португалія, Нігерія, Бельгія, Угорщина, Україна, Чехія, Іспанія, Швейцарія належить від 3 до 9 публікацій. Всім іншим – 1 та 2 наукові праці.

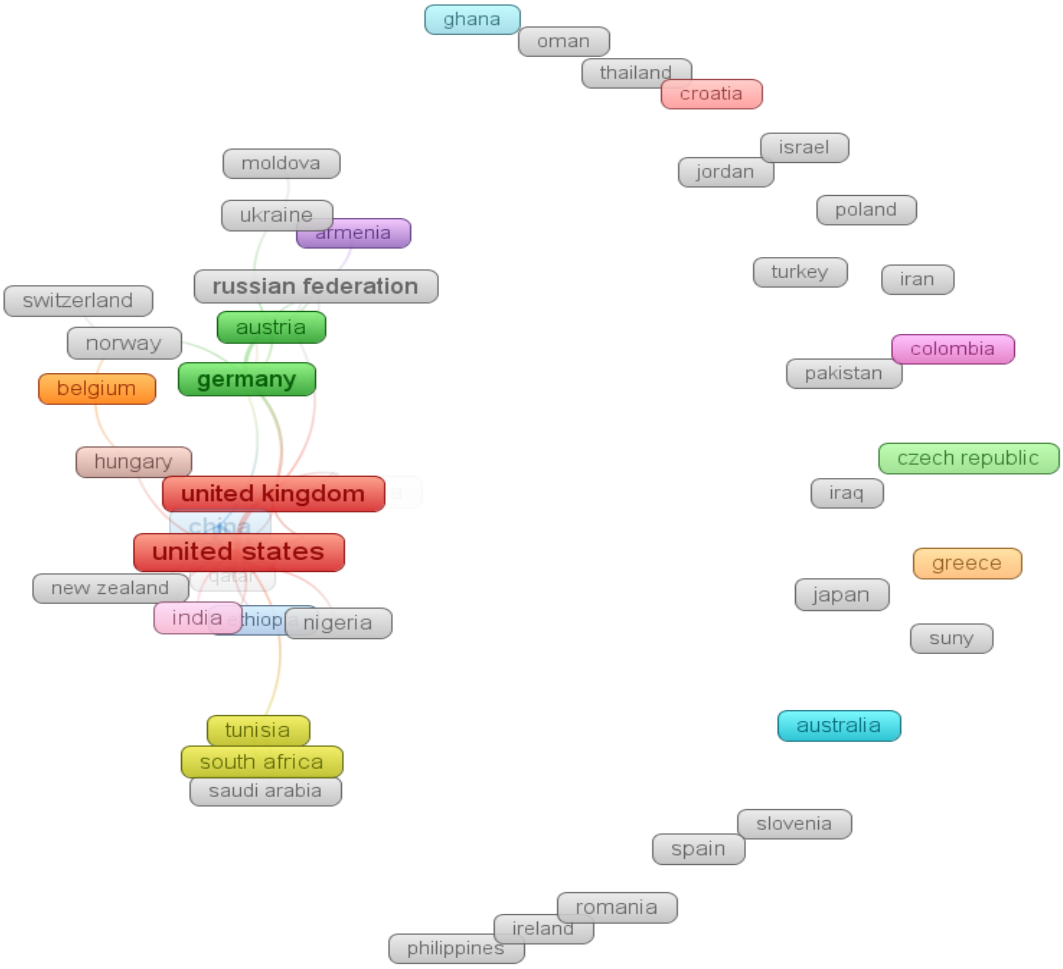


Рисунок 1.24 – Мережева карта країн співавторів, які проводять дослідження інформаційної безпеки у розрізі економіка

Джерело: побудовано авторкою на основі бази даних Scopus

Щоб чітко розуміти, у яких напрямах економічної діяльності, пов’язаних із проблематикою інформаційної безпеки, проводяться дослідження, було побудовано карту бібліографічних досліджень на основі співпадіння ключових слів, присвячених інформаційній безпеці в розрізі її взаємозв’язків із економікою (див. рис. 1.25).

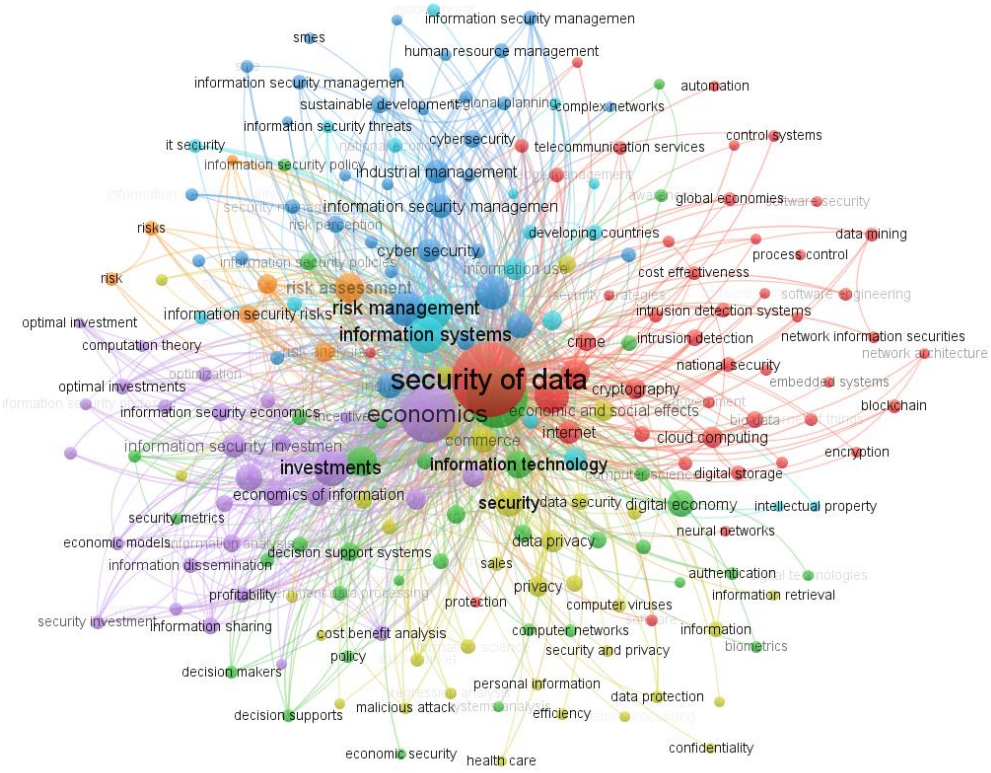


Рисунок 1.25 – Карта наукометричної бібліографії досліджень, присвячених проблемі інформаційної безпеки у контексті предметної галузі – економіка

Джерело: побудовано авторкою на основі бази даних Scopus

На карті 1.25 виділено 7 кластерів існуючих досліджень, які було сформовано на основі ключових слів, зазначених авторами публікацій. Кожен з них надає уяву про напрями, за якими відбуваються дослідження проблеми інформаційної безпеки у розрізі економічного розвитку країни. Деталізуємо кожен із кластерів окремо на наступних рисунках для більш чіткого розуміння проблематики. На рисунку 1.26 представлено найбільший червоний кластер ключових слів, які стосуються сфери захисту даних.

Так, червоний кластер (рисунок 1.26) характеризує основні напрями, пов’язані із створенням, удосконаленням, застосуванням та розвитком сучасних технологій для вирішення проблем інформаційної безпеки. Дослідження даної групи охоплюють: блокчейн та хмарні технології, big data, системи контролю, автоматизації, виявлення вторгнень, прогнозування кібератак, технології криптографії, шифрування, data mining, нейронні мережі.

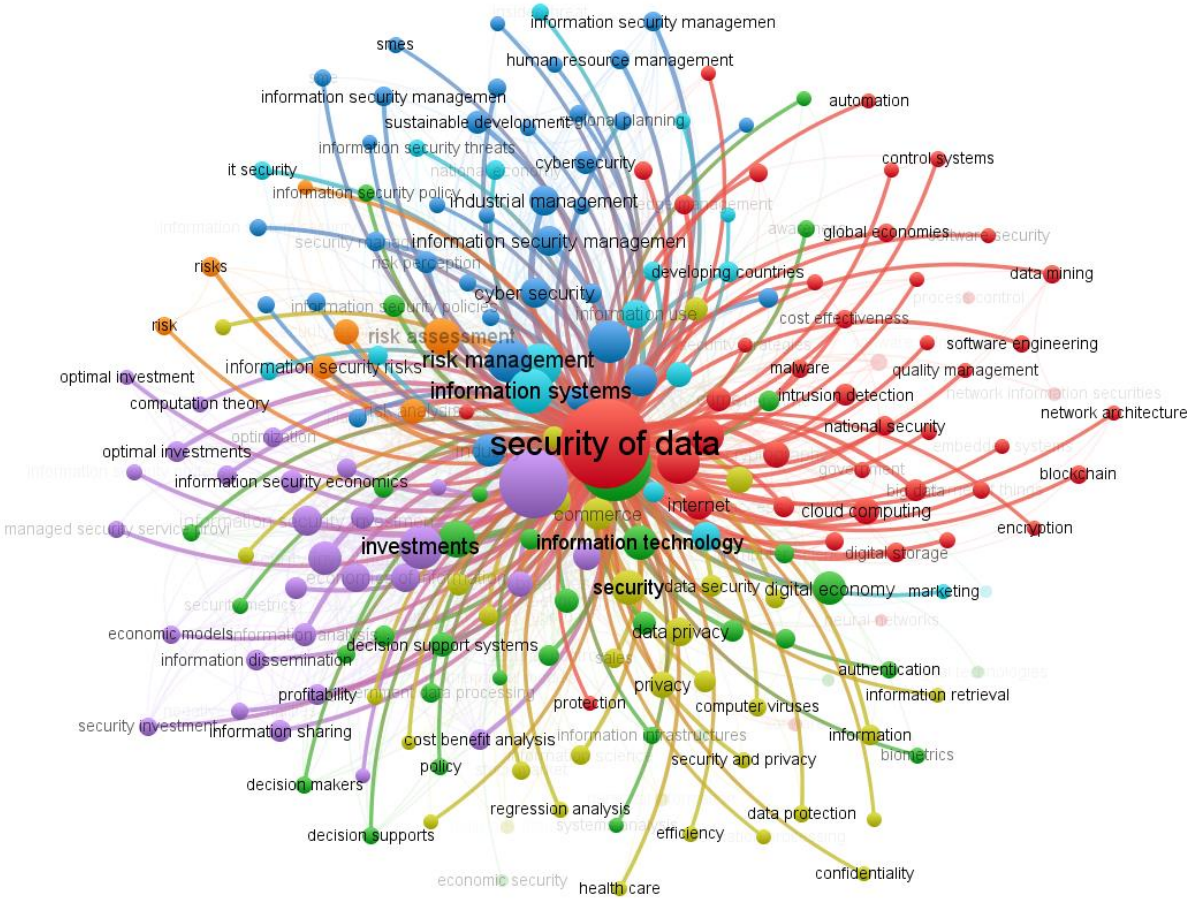


Рисунок 1.26 – Червоний кластер карти наукометричної бібліографії досліджень

Джерело: побудовано авторкою на основі бази даних Scopus

Даний кластер торкається також напряму створення програмного забезпечення та комп’ютерних мереж для забезпечення потреб інформаційної безпеки. Окрім цього визначається також економічна ефективність заходів в сфері безпеки та вплив їх на економіку.

В цій сфері можна відмітити роботу Ван Б., Лі Ю., Чжао С., Чень Х., Цзінь Ю., Дін Ю., яка присвячена дослідженню застосування технології блокчейн для підвищення ефективності обробки транзакцій розподіленої енергії [254]. У праці Покровської Н.Н. запропоновано використовувати алгоритми блокчейнів для розробки багатокритеріальної оцінки активів, щоб вирішити проблему побудови надійної та прозорої системи оподаткування та системи взаємовідносин між економічними агентами [195]. Також недосконалим є процес виявлення різного роду кібер- та інформаційних загроз, тому в рамках цієї

проблеми працюють Рю Ю.У. та Рхі Х.-С., які удосконалили модель виявлення вторгнень з урахуванням потенційно ворожого середовища для фірми та інспекцією співробітників служби безпеки [204].

Окрім технологій червоний кластер охоплює дослідження аспектів національної безпеки для цифрової економіки, де розкриваються питання захисту інформації та контролю в даній сфері. Так, Сонні З. розглядає концепцію національної безпеки країни в умовах зростання її залежності від інформаційних технологій [218]. Кшетрі Н. досліджує імперативи доповіді Комісії США з підвищення національної кібербезпеки "Звіт про забезпечення та зростання цифрової економіки", яку було сформовано у зв'язку із підвищенням рівня кіберзагроз [154]. Перед кожною країною можуть поставати виклики, пов'язані із порушенням національної безпеки та підвищенням ризиків мережевої безпеки, що з огляду подій 21 сторіччя є досить актуальним. Тому в рамках вирішення даної проблеми запропоновано стратегії інформаційної безпеки з точки зору права для країни Китай, які було розроблено Лі Дж. [163].

Зелена група (рисунок 1.27) містить ключові слова, пов'язані із прийняттям рішення в сфері інформаційної безпеки та впровадженням ряду технологічних рішень для аутентифікації користувачів, їх біометрії, підвищення рівня інформаційної культури, попередження вразливостей систем, кіберзлочинів. При цьому дані поняття стосуються також й сфери електронного уряду, цифровізації економіки.

За часту у питаннях, пов'язаних з інформаційною безпекою виникають ситуації, які потребують прийняття зваженого рішення, особливо це стосується обґрунтування інвестицій у безпеку (рисунок 1.27). Вирішення даної проблеми пропонують Таллау Л.Дж., Гупта М., Шарман Р., які застосовують методологію збалансованої системи показників в процесі дослідження питання інформаційної безпеки у IT-відділі одного з університетів США [229]. Для розробки оптимального рішення щодо організації системи безпеки різних фірм деякі автори радять застосовувати економіко-математичні методи та моделі.

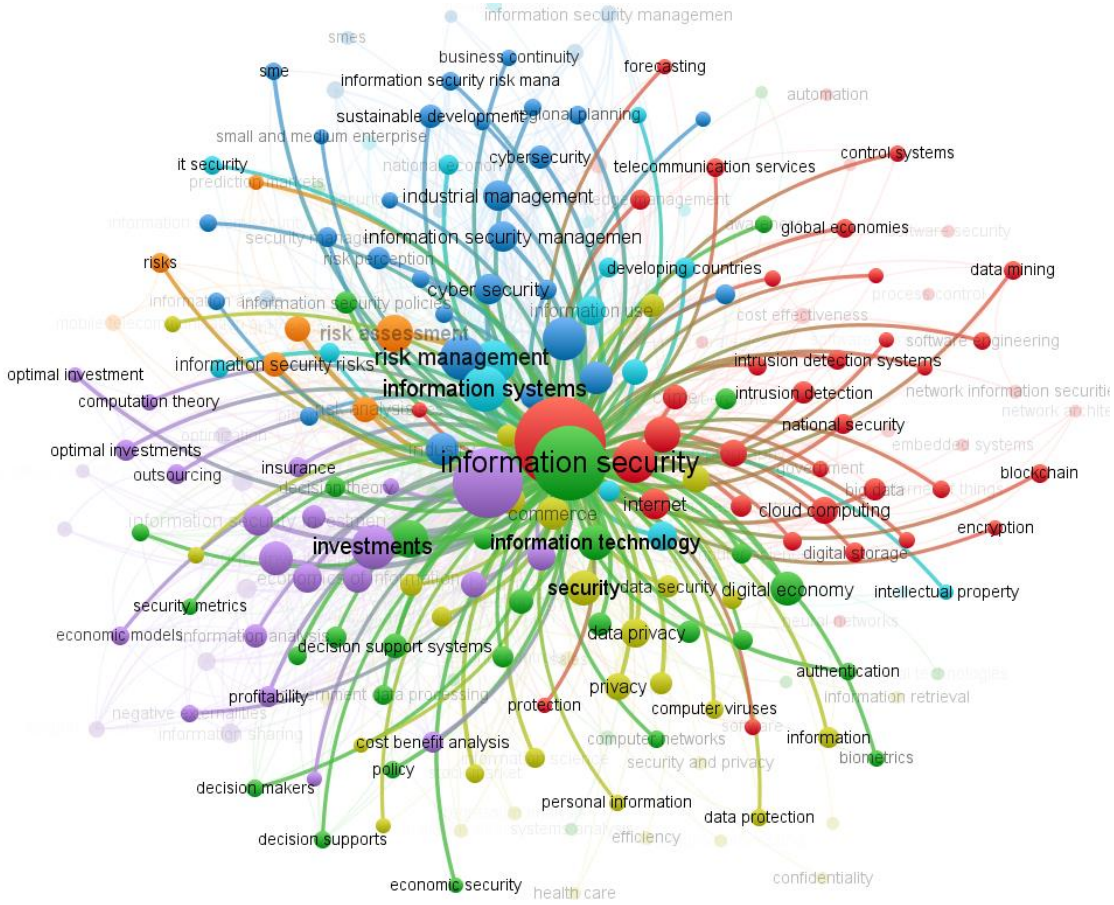


Рисунок 1.27 – Зелений кластер карти наукометричної бібліографії досліджень

Джерело: побудовано авторкою на основі бази даних Scopus

В цьому напрямку Ву Ю., Фен Г., Фунг Р.Й.К. запропонували теорію ігор, яка дозволяє аналізувати заходи безпеки як соціальний планувальник та враховувати взаємодію безпеки із бізнес-середовищем [259]. Для підвищення гнучкості та обчислювальної ефективності рішень щодо оцінки економічної доцільності інвестицій в інформаційну безпеку є можливим використання нечітких економічних моделей, які пропонуються у дослідженні Шин І.Н. [211].

Синій кластер (рисунок 1.28) охоплює напрям інформаційного менеджменту. Тобто тут проводяться дослідження, які стосуються управління людськими ресурсами, ризиками, пов’язаними з попередженнями кіберзагроз, політикою захисту, планування, створення ефективної інфраструктури компанії, тощо.

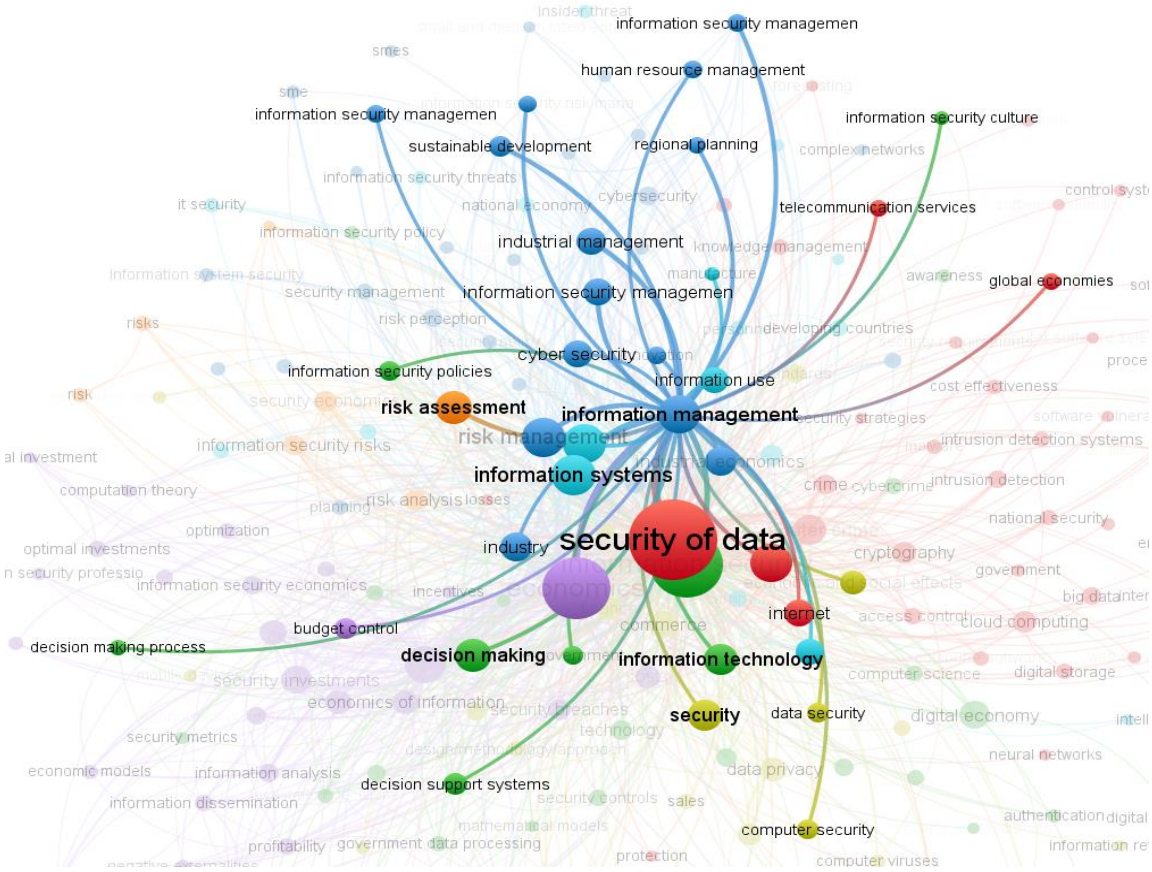


Рисунок 1.28 – Синій кластер карти наукометричної бібліографії досліджень

Джерело: побудовано авторкою на основі бази даних Scopus

В рамках даного кластеру Ключніков А., Мура Л. та Скленар Д. досліджують фактори успіху управління інформаційною безпекою малих та середніх компаній, а саме відповідність управління інформаційною безпекою діловій діяльності компанії, наявність підтримки вищого керівництва, контроль безпеки компанії та обізнаність працівників в питаннях структури організації, серед яких було зроблено акцент на організаційній обізнаності [142]. Сінгх А.Н. та Гупта М.П. підкреслюють важливість для управління інформаційною безпекою таких факторів, як підтримка вищого керівництва, організаційна культура захисту інформації та належна система моніторингу [215]. В якості одного з ефективних заходів управління інформаційною безпекою Бекмуратов Т.Ф., Ганєв А.А., Ботіров Ф.Б. запропонували концепції побудови автоматизованої системи захисту інформації на підприємстві [22].

Жовта група (рисунок 1.29) характеризує специфіку досліджень щодо

питань обробки, відновлення, захисту, забезпечення конфіденційності персональної інформації.

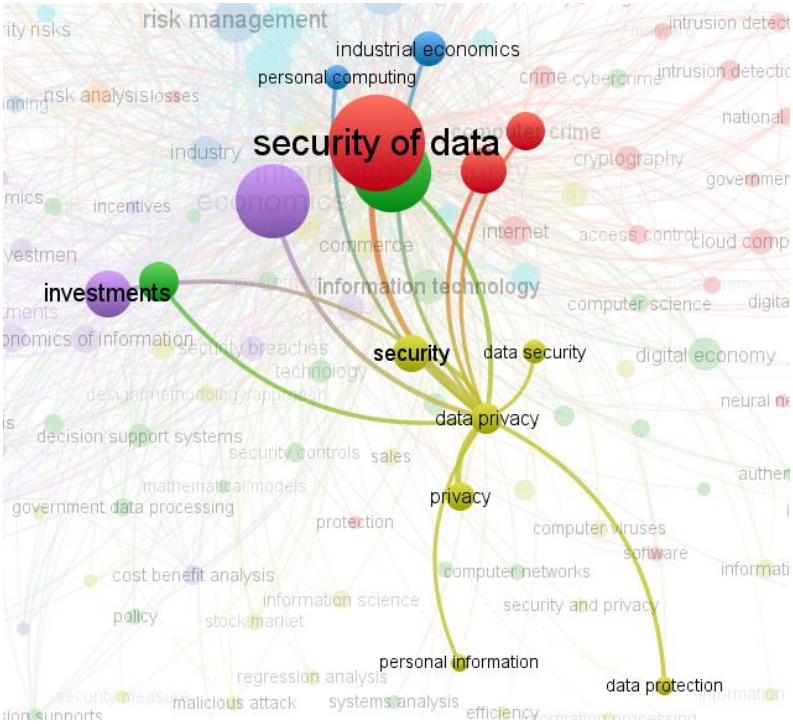


Рисунок 1.29 – Жовтий кластер карти наукометричної бібліографії досліджень

Джерело: побудовано авторкою на основі бази даних Scopus

Дана проблематика розкривається для користувачів мобільних пристроїв, комп'ютерів, платіжних додатків, інтернет-магазинів. Так, Столл М. пропонує розробку цілісної моделі інформаційної безпеки та конфіденційності даних, яка відповідає стандартам Міжнародної організації стандартів, а саме ISO/IEC 27001 [226]. У дослідженні [97] авторами запропоновано модель зрілості захисту персональних даних в організаціях мікрофінансового сектору, засновану на міжнародних стандартах конфіденційності та захисту інформації. Автори Мартінс Н. та Да Вейга А. у науковій праці [174] зробили акцент на тому, що треба розвивати культуру інформаційної безпеки з урахуванням чотирьох механізмів – управління, політики, обізнаності та відповідності, як частин програми інформаційної безпеки, що дозволить мінімізувати ризики поведінки працівників та підвищить ефективність захисту персональних даних та інформації компанії.

Бузковий кластер (рисунок 1.30) містить ключові слова, які стосуються економічних аспектів забезпечення інформаційної безпеки – економіці інформації, економіці інформаційних систем, економіці інформаційного захисту. Тут можна виділити проблеми витрат, пов'язаних із системами захисту даних, побудови ефективних економічних моделей, страхування, інвестування, оптимізації, прибутковості, аутсорсингу, управління в цілому.

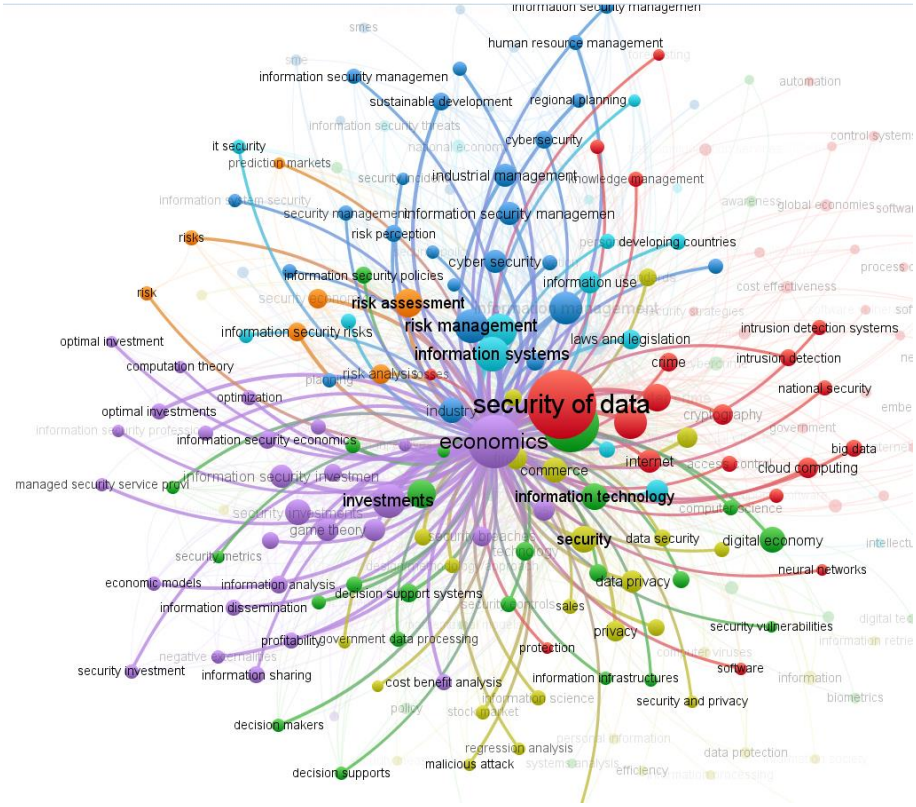


Рисунок 1.30 – Бузковий кластер карти наукометричної бібліографії досліджень

Джерело: побудовано авторкою на основі бази даних Scopus

Так, Андерсон Р. та Мур Т. піднімають питання економіки інформаційної безпеки, в рамках якого відбувається визначення ефективності процесу забезпечення інформацією різних сфер діяльності в умовах порушення її конфіденційності та політики цифрових прав [13]. Беме Р. та Новей Т. приділяють увагу економічним підходам до показників безпеки, при чому вони виділяють дві галузі дослідження – інвестиції та прийняття рішення [31]. Цякіс Т. та Стефанідес Г. також досліджують проблему економічної оцінки системи безпеки [238]. Результати неефективного менеджменту інформаційної

безпеки на рівні держави можуть привести до зниження інвестиційної привабливості будь-якої держави. Як наслідок, це негативно вплине на розвиток економіки країни, що є предметом досліджень Кардхолма Л. [42]. Тому важливо розвивати програми управління інформаційною безпекою, інвестування у які підвищує вартість компаній та формує сприятливий інвестиційний клімат у країні [66]. Гордон Л.А. та Лоєб М.П., працюючи у даному напрямку, запропонували економічну модель, яка дозволяє визначати оптимальну суму інвестування з метою захисту певного набору інформації, що сприяє прогнозуванню втрат компанії від порушення системи безпеки [107].

Бірюзова група (рисунок 1.31) охоплює напрям, пов'язаний із забезпеченням інформаційної безпеки на рівні підприємств та національної економіки через розробку інформаційних систем, стандартів, правових норм. Серед публікацій даного кластеру можна виділити й ті, які присвячені розвитку економіки шляхом розробки стратегій в сфері інформаційної безпеки, що говорить про той факт, що її роль для розвитку суспільства та економіки в цілому є суттєвою.

Так, Топа І. та Карида М. надають рекомендації щодо розробки стандартів для покращення практики управління інформаційною безпекою компанії [236]. Косєвич Е. пропонує приклади стратегій інформаційної безпеки з урахуванням особливостей розвитку країни [150]. Дінцеллі Е. виділяє вплив фактору культурних різниць на інформаційну безпеку та на розробку відповідної стратегії боротьби із інформаційними загрозами [70]. Негативні наслідки в інформаційному середовищі та порушення політичної стабільності країни можуть викликати зовнішні політичні конфлікти, що повинно бути враховано при розробці стратегії розвитку держави, чому приділено увагу у праці Кириленка В.П. та Алексєєва Г.В. [141].

В рамках виникнення внутрішніх конфліктів переслідування свободи слова також може нести загрозу інформаційній безпеці країні, що потребує перегляду правових аспектів з урахуванням забезпечення стратегічної даного напрямку [191].

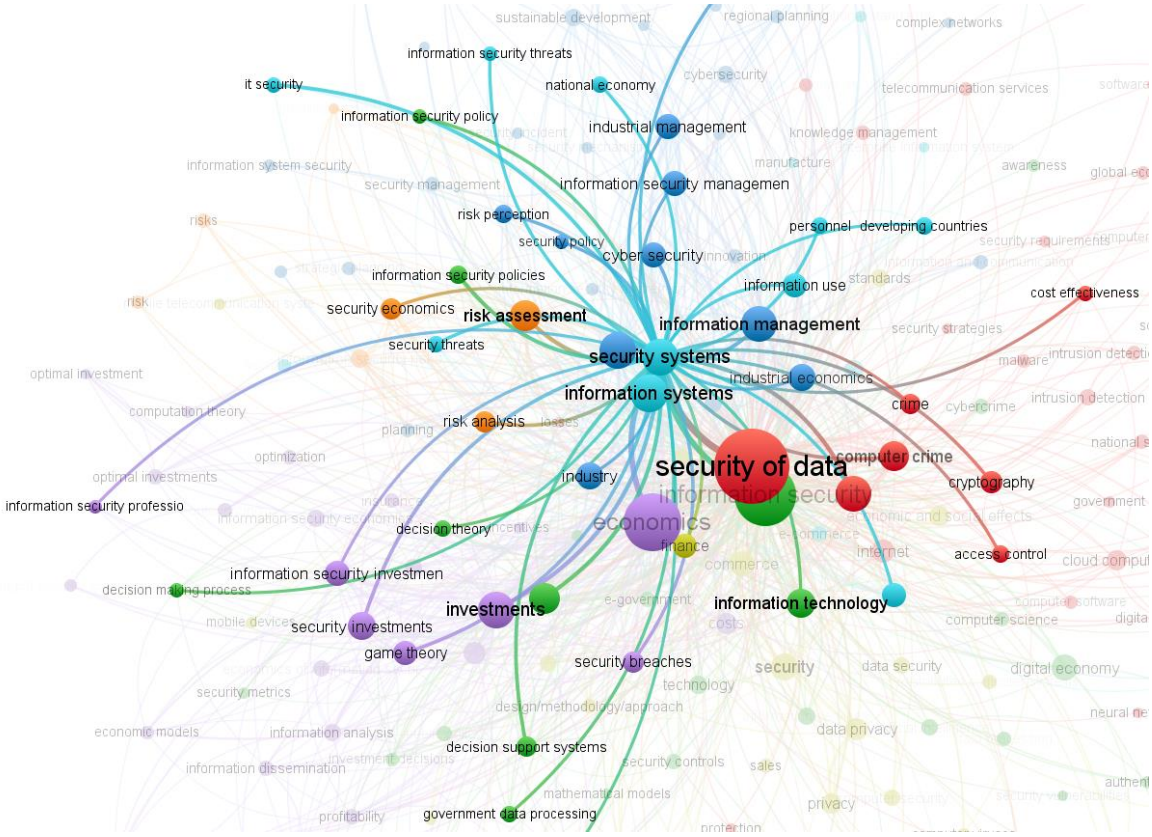


Рисунок 1.31 – Бірюзовий кластер карти наукометричної бібліографії досліджень

Джерело: побудовано авторкою на основі бази даних Scopus

Помаранчевий кластер (рисунок 1.32) характеризує напрям дослідження ризиків інформаційної безпеки, а саме їх передбачення, аналіз, оцінка. Ідентифікація ризиків, що можуть виникати у системі інформаційної безпеки, є однією із ключових проблем у даній сфері, оскільки дозволяє визначати вразливості інформаційних систем економічних агентів та пов’язані із цим фінансові втрати. Тому виникає потреба у розробці різних методологій оцінки, особливо якщо вони враховують якісні та кількісні характеристики, що представлено у дослідженні Мунтеану А. [180]. У наукових працях також розглядаються різні варіанти ідентифікації ризиків з урахуванням загроз, вразливостей, вартостей активів. Так, у цьому контексті запропоновано економічну модель для визначення прийнятного ризику з урахуванням поглинання активів та розрахунком інвестицій у безпеку [132].

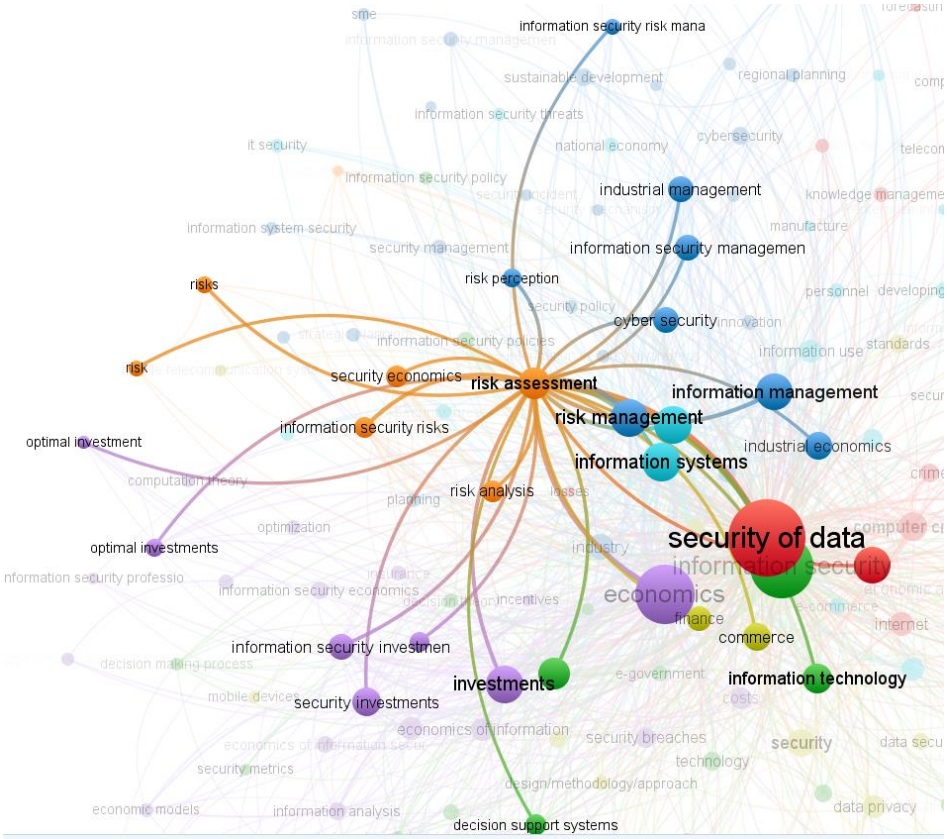


Рисунок 1.32 – Помаранчевий кластер карти наукометричної бібліографії досліджень

Джерело: побудовано авторкою на основі бази даних Scopus

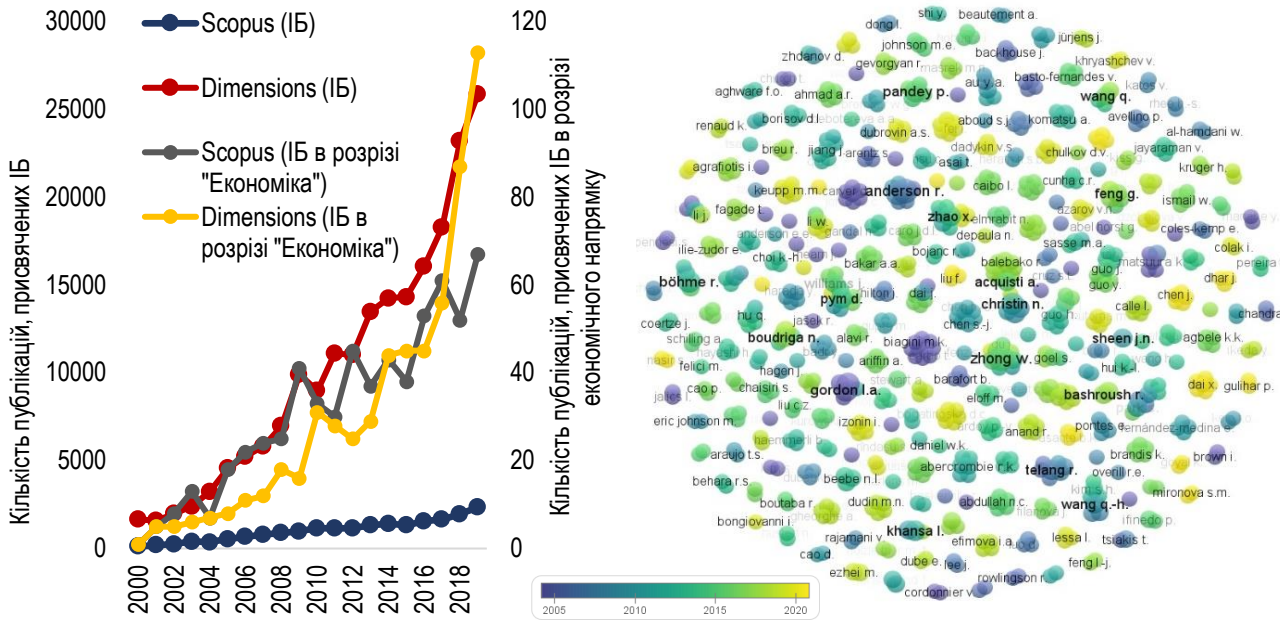
Ши Ю. та Вен К. застосували підхід економічної вартості для оцінки ризиків безпеки, що дозволило визначити різні чинники впливу та їх економічну цінність [212]. На увагу заслуговують спеціальні математичні методи, які використовуються для оцінки ризиків, одним із яких є нечітка логіка. У роботі Коклса М., Філанова Дж., Корчека Ф. розроблено систему нечіткої логіки для оцінки ризиків інформаційної безпеки, яка базується на матричному методі стандарту ISO / IEC 27005 та відповідних нормативних актах Чеської республіки [145].

Таким чином, проблематика, пов’язана із інформаційною безпекою, є досить актуальною у наукових колах, про що свідчить зростання зацікавленістю даної теми протягом останніх 20 років. Це підтверджено збільшенням наукових досліджень у міжнародних виданнях, які індексуються у базі даних Scopus, а також зростанням наукових публікацій у академічних виданнях, інформація про

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

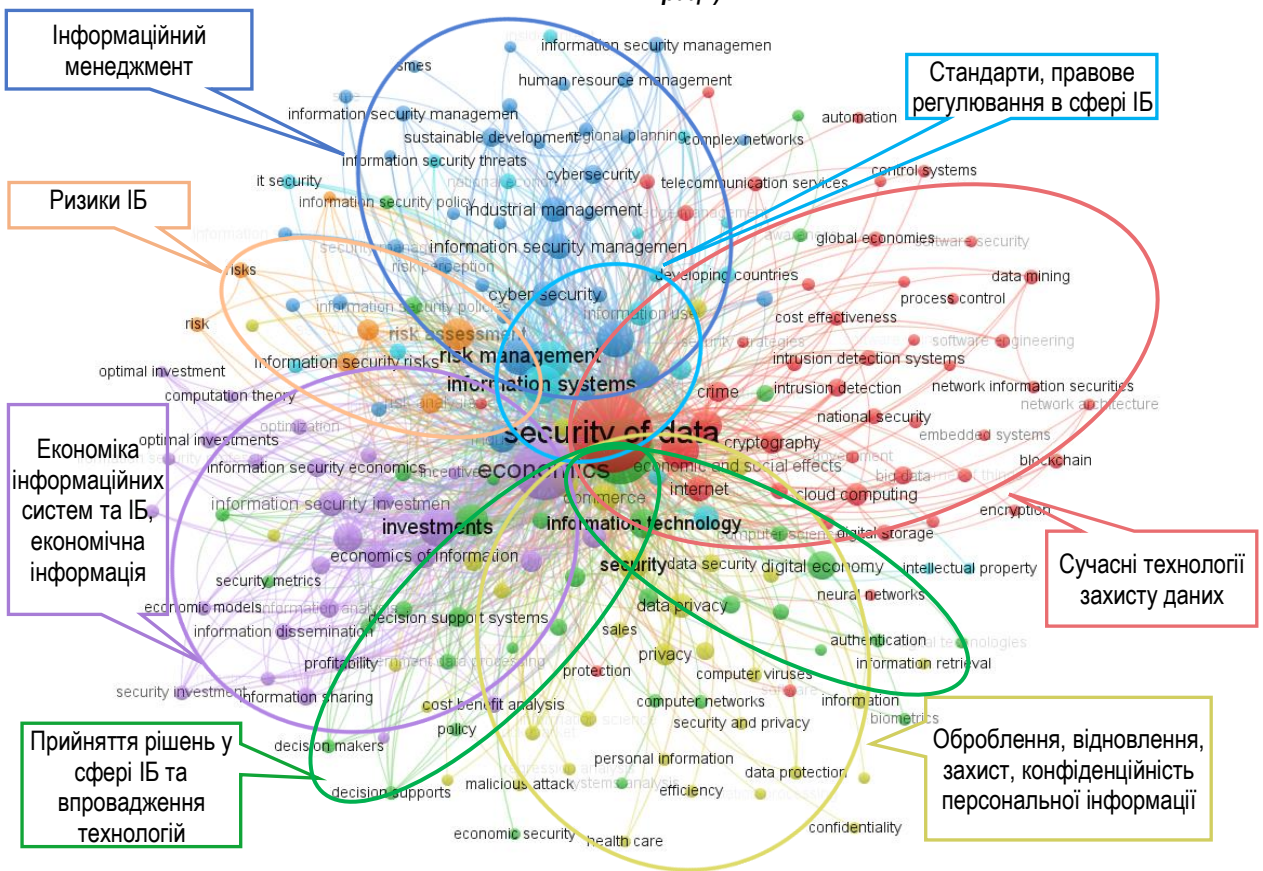
Аналіз журналів, в яких було опубліковано статті, присвячені проблемі інформаційної безпеки в сфері економіки, показав, що з даного напрямку тільки близько 11% статей надруковано у рейтингових журналах, що говорить про здійснення локальних досліджень та отримання результатів, прийнятних для окремих країн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

Узагальнення основних результатів підрозділу 1.3 представимо на рисунку 1.33.



а) динаміка кількості статей у базах даних Scopus і Dimensions із питань ІБ у 2000–2019 рр.

б) мережева карта співавторів, що досліджують ІБ в розрізі предметної галузі "Economics, Econometrics and Finance", побудована на основі бази даних Scopus у 2000–2020 рр. (*діаметр кола – індикатор кількості праць)



в) карта ключових слів у дослідженнях, присвячених проблемі ІБ в розрізі предметної галузі "Economics, Econometrics and Finance" (за базою даних Scopus у 2000–2020 рр.)

Рисунок 1.33 – Результати динамічного (Scopus Citation Overview Tool, Dimensions Tool) та бібліометричного (VOSviewer v. 1.6.10) аналізів досліджень інформаційної безпеки (ІБ) у розрізі предметних галузей економічного напрямку

Висновки до розділу 1

1. У підрозділі 1.1 дисертаційної роботи було досліджено тенденції розвитку національної економіки в умовах її цифровізації. Так, дослідження частки ІТ-галузі в структурі національної економіки за 2010–2019 рр. та побудова поліноміального тренду дозволили спрогнозувати зростання у 2024 р. його обсягу до 38 % від четвертинного сектору та 6 % від ВВП (для порівняння: у 2010 р. ці показники становили 19,15 % та 3,06 % відповідно). Зіставлення частки ІТ-галузі у ВВП України та країн ЄС у 2018 р. (3,90 % та 4,49 % відповідно) засвідчило, що темпи цифровізації української економіки відповідають європейському рівню, що є ознакою наявності потужного інформаційного потенціалу країни.

2. Виходячи з актуальності цифрового варіанту розвитку економіки, було відображено структуру національної економіки, формування якої обумовлено застосуванням системного підходу до визначення систем – хто (суб'єкт), що (об'єкт) та як (інструмент). Це дозволило визначити, що національна економіка країни має складну структуру, яка охоплює таких суб'єктів, як індивіди (нанорівень), сімейні господарства (мінірівень), економічні агенти (мікрорівень), регіони (мезорівень), країна (макрорівень) та світ (мегарівень). Її об'єктами виступають всі сфери, які розподілені за секторами національної економіки. Для забезпечення процесів цифрової трансформації національної економіки визначено ряд інструментів, у якості яких виступають сучасні інформаційні та комп'ютерні технології.

3. Результати аналізу наукових напрацювань щодо трактування поняття «інформаційна безпека», проведеного у підрозділі 1.2, дозволили виокремити два їх напрями: 1) характеристика інформаційної безпеки через її функціональне навантаження, що звужує її розуміння лише як стану, процесу або сфери діяльності, залишаючи поза увагою системний характер; 2) характеристика інформаційної безпеки через її суб'єктів, що розмежовує дослідження інформаційної безпеки держави, економічних агентів або індивідів, залишаючи

поза увагою багаторівневість та крос-секторність наслідків її порушення. З огляду на виявлені недоліки існуючих підходів запропоновано трактувати інформаційну безпеку як комплексну систему захисту об'єктів (інформація, знання, інформаційні системи), що належать до фінансово-господарської, політичної, військової, технологічної сфер діяльності, від різного роду загроз (несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення) із застосуванням програмних, технічних, методичних, інформаційних і правових засобів, що використовують окремі особи або спеціалізовані підрозділи та фахівці державних органів, економічні агенти. Запропоноване визначення відрізняється від існуючих розумінням інформаційної безпеки як складної багатокомпонентної та динамічної системи, що потребує комплексного дослідження з урахуванням суб'єктно-об'єктної специфіки.

4. Запропонований підхід дозволив уточнити концептуальні засади забезпечення інформаційної безпеки в системі управління національною економікою. Основними детермінантами її архітектоніки є зовнішні та внутрішні загрози, що впливають на порушення цілісності, конфіденційності та доступності інформації, знань і безпосередньо інформаційних систем суб'єктів, у результаті чого виникають деструктивні наслідки для економічного, соціального та політичного розвитку країни. Для їх попередження і виявлення інцидентів на рівні держави, суб'єктів господарювання, фінансових інститутів та індивідуумів повинна бути сформована відповідна організаційно-правова структура, ефективність функціонування якої повинна оцінюватися за обсягами зменшення втрат національної економіки від дій інсайдерів та кібершахраїв, з урахуванням потреби в оптимізації витрат на функціонування системи забезпечення інформаційної безпеки і стабілізації економічного, політичного й соціального вимірів розвитку національної економіки.

5. Проведене дослідження у підрозділі 1.3 трендів наукової зацікавленості питаннями інформаційної безпеки виявило, що починаючи з 1967 р. проблематиці інформаційної безпеки присвячено більше ніж 200 тис. публікацій,

зібраних у базі даних Dimensions, близько 24 тис. праць, проіндексованих базою даних Scopus. Це питання спричиняє зростання цікавості науковців: 97 % статей опубліковано в період 2000–2019 рр., що обумовлено стрімкою цифровізацією економіки та суспільства, а також активізацією кіберзагроз. Водночас лише незначна кількість досліджень (1 % за базою даних Scopus та 0,3 % за базою даних Dimensions) реалізовані в розрізі предметних галузей економічного напрямку. Аналіз мережевої карти співавторів, які досліджують проблематику інформаційної безпеки у контексті економічного розвитку, географії дослідження, виявив відсутність домінування окремих наукових шкіл за останні 10 років.

6. Бібліометричний аналіз ключових слів наукових публікацій, що індексуються наукометричною базою даних Scopus та присвячені проблематиці інформаційної безпеки як драйвера розвитку національної економіки, засвідчив наявність семи векторів досліджень. Домінуючим напрямом є створення, вдосконалення, використання та розвиток сучасних технологій для вирішення проблем захисту інформації. Наступними векторами (за зменшенням кількості відповідних публікацій) є такі: 1) економіка інформаційних систем, інформаційного захисту та інформації; 2) забезпечення конфіденційності персональної інформації; 3) прийняття рішень у сфері інформаційної безпеки; 4) ризики інформаційної безпеки; 5) правове забезпечення інформаційної безпеки; 6) інформаційний менеджмент. Одержані результати дозволили окреслити пріоритетні для науки та практики завдання, пов’язані з формуванням системи інформаційної безпеки як драйвера розвитку національної економіки.

Основні положення першого розділу дисертаційної роботи опубліковано авторкою в роботах [381, 384, 397, 398].

РОЗДІЛ 2 МЕТОДОЛОГІЯ ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ ТА ЕФЕКТИВНОСТІ СИСТЕМИ ЇЇ ЗАБЕЗПЕЧЕННЯ

2.1 Визначення складу індикаторів інформаційної безпеки національної економіки

Виходячи з отриманого визначення інформаційної безпеки та доведення фактів, що відбувається трансформація суспільства паралельно із розвитком інформаційних технологій та дослідження даної проблематики у різних сферах діяльності людини, можна висунути гіпотезу щодо існування обопільно обумовлених взаємовпливів між системою інформаційної безпеки та національною економікою. З цією метою оберемо індикатори, які використовуються для вимірювання рівня інформаційної безпеки та розвитку національної економіки, та проведемо відповідні розрахунки щодо доведення або відхилення поставленої гіпотези.

На першому кроці визначимо показники, які використовуються для визначення рівня інформаційної безпеки країни. У вітчизняній літературі відсутні посилання щодо застосування конкретних індексів для вирішення даної проблеми. Але зарубіжні вчені приділяють увагу даному питанню. Так, в рамках підвищення ефективності управління інформаційною безпекою Берк В., Осені Т., Джолфай А., Гондаль І. пропонують використовувати індекси кібербезпеки для її виміру у сфері охорони здоров’я [39]. Юніс М.М. та Кунг К.С. для цієї мети розробили комплексний індекс кібербезбеки з урахуванням багатьох факторів [267]. Джазрі Х., Закарія О., Чикогора Е. у своїй роботі акцентують увагу на створенні індексу оздоровлення кібербезпеки [134]. Попова Л., Коростелкіна І., Дедкова Є., Коростелкін М. використовують показники її розвитку в умовах цифровізації економіки [198].

Оскільки інформаційна безпека є системним поняттям і включає різні аспекти, то на практиці з метою підвищення ефективності її управління на

макроекономічному рівні застосовується ряд індикаторів, які характеризують тільки окремі її складові. Серед них можна виділити «Глобальний індекс кібербезпеки» (The Global Cybersecurity Index – GCI), «Національний індекс кібербезпеки» (The National Cyber Security Index – NCSI), «Індекс розвитку інформаційних та комунікаційних технологій» (ICT Development Index – ICTDI), «Індекс мережевої готовності» (Networked Readiness Index – NRI), «Рівень цифрового розвитку» (Digital Development Level – DDL). Дані індикатори характеризують рівень інформаційної безпеки у напрямках технологічного, інформаційного, організаційного забезпечення, тому, на нашу думку, їх застосування для вимірювання рівня інформаційної безпеки є виправданим.

«Глобальний індекс кібербезпеки» (далі GCI) вимірює рівень кібербезпеки для країн-членів Міжнародного союзу електрозв'язку та оцінюється за п'ятьма напрямами – технічні заходи, юридичні заходи, організаційні заходи, розбудова потенціалу, співпраця [102]. Даний показник є продуктом діяльності міжнародних організацій, які сприяють підвищенню ефективності міжнародного співробітництва та обміну знаннями на глобальному рівні. Його основна мета – це визначення слабких сторін країни щодо кібербезпеки та покращення можливостей для неї шляхом розробки стратегії кібербезпеки та відповідних стандартів.

Використовуючи значення «Глобального індексу кібербезпеки» за 2018 рік для 159 країн світу, побудуємо із використанням програми «MS Excel» карту, яка дозволить зробити візуальний аналіз географії країн та дозволить оцінити, для яких з них характерний високий рівень безпеки, а для яких – низький (рисунок 2.1).

На рисунку 2.1 представлено тільки ті країни, для яких існують емпіричні дані. Візуальний аналіз показує, що високий рівень кібербезпеки характерний для таких країн, як США (93), Великобританія (93), Франція (92), Естонія (91), Литва (91), Сінгапур (90), Іспанія (90), Канада (89), Австралія (89), Люксембург (89), Малайзія (89), Нідерланди (89), Норвегія (89), Японія (88), Маврикій (88), Саудівська Аравія (88), Південна Корея (87), Оман (87), ряд країн ЄС та Китай.

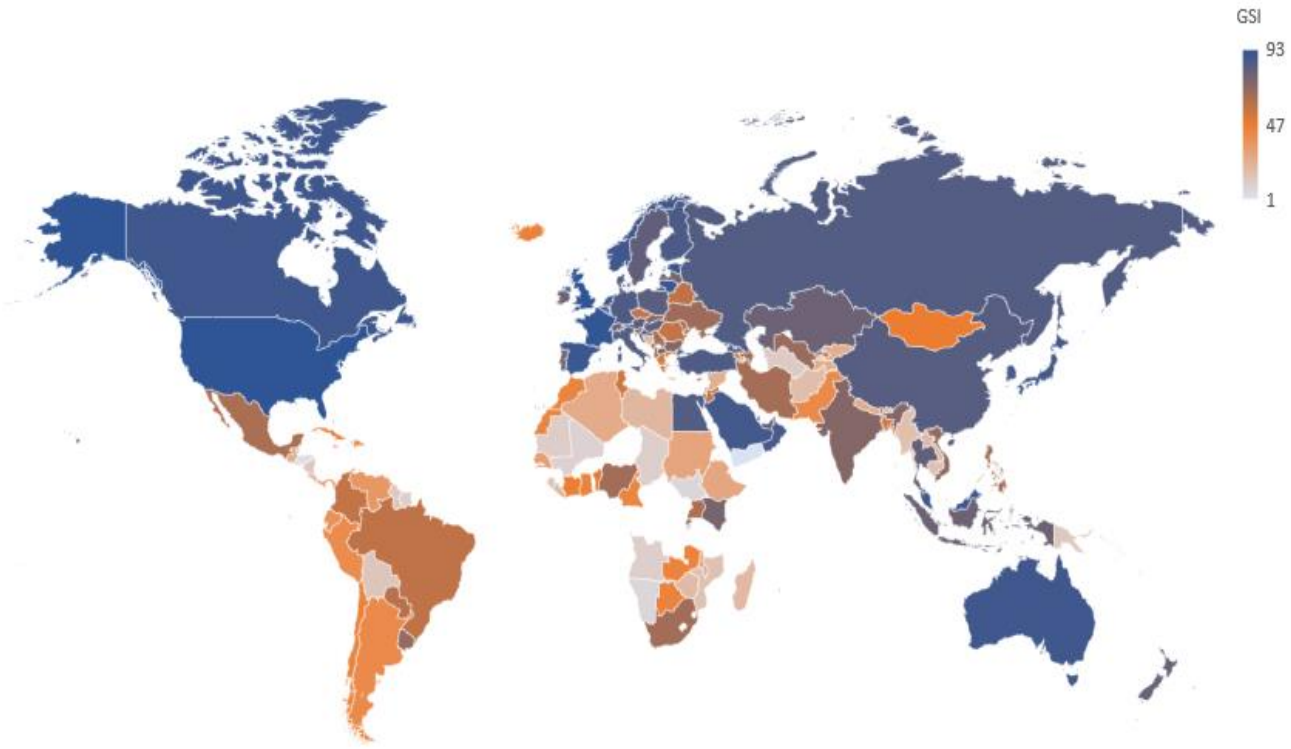


Рисунок 2.1 – Карта рейтингування країн за «Глобальним індексом кібербезпеки» за 2018 рік

Джерело: побудовано авторкою на основі [86]

Для більшості країн Африки, деяких країн Південно-Східної Азії, пострадянських країн, Гватемали, Гондурасу, Панами, Нікарагуа, Гайани, Болівії, Суринама GSI є дуже низьким. Для більшості країн Південної Америки, ряду країн Східної Європи, України, Індії, Монголії, Мексики та інших даний індекс відповідає середньому значенню (47) та вище. Тобто можна зробити попередній висновок, що є певна залежність між рівнем розвитку економіки країни та рівнем її кібербезпеки, оскільки високі значення GSI відповідають країнам, для яких характерний високий рівень економічного розвитку. З іншого боку, найменш розвинені країни із низькими показниками економічного розвитку мають й низький рівень кібербезпеки.

«Національний індекс кібербезпеки» (далі NCSI), розроблений Академією електронного врядування, визначає рівень готовності країни протидіяти кіберзагрозам та керувати кіберінцидентами. Результати його визначення застосовують у якості інформації для формування джерел нарощування

національного потенціалу у галузі кібербезпеки. На відмінність від GSI, NCSI враховує особливості системи кіберзахисту із врахуванням національних аспектів. Для його розрахунку використовується 46 індикаторів, об'єднаних за 12 напрямками, а саме: розробка політики та стратегії в галузі кібербезпеки; аналіз та інформація щодо кіберзагроз; організація освіти та професійного розвитку у галузі кібербезпеки; оцінка внеску у глобальну кібербезпеку; рівень захисту цифрових послуг: відповідальність, стандарти, органи; організація захисту основних послуг; електронна ідентифікація та послуги довіри; захист персональних даних; реагування на кіберінциденти; кіберрегулювання кризи; боротьба з кіберзлочинністю; військові кібероперації [185].

Використовуючи емпіричні значення NCSI за 2018 рік для 159 країн світу, побудовано карту для візуального аналізу та оцінки країн, для яких характерний високий чи низький рівень безпеки (рисунок 2.2).

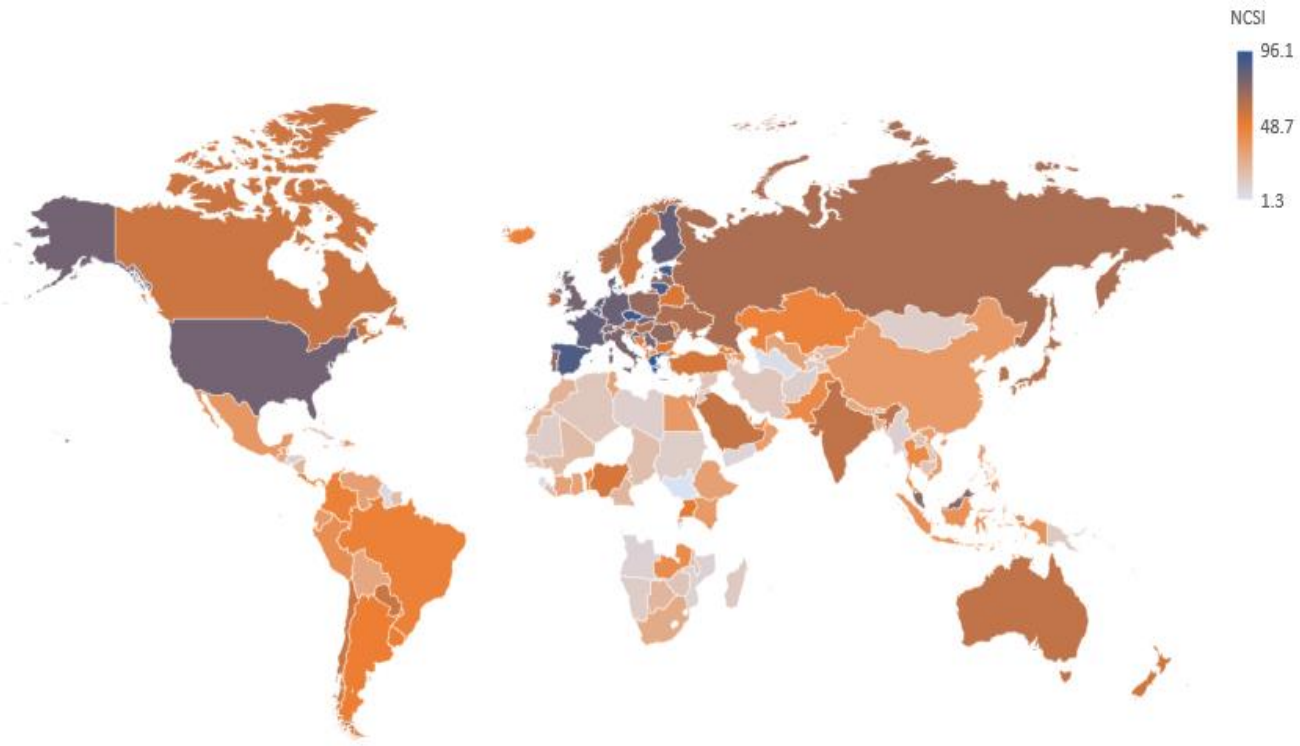


Рисунок 2.2 – Карта рейтингування країн за «Національним індексом кібербезпеки» за 2018 рік

Джерело: побудовано авторкою на основі [86]

Аналізуючи дані, представлені на рисунку 2.2, можна сказати, що країни, які відносяться до розвинутих, а саме США, Канада, Австралія, країни Європи, та інші, мають високі значення національного індексу кібербезпеки. Хоча, якщо порівнювати країни, що розвиваються, наприклад, Україна, яка має індекс, рівний 64, та розвинуту країну Австралію з індексом 60, то можна дійти висновку, що рівень протидії кіберзагрозам в Україні вищий. Також цей показник для України є вищим у порівнянні з такими розвинутими країнами, як Канада (57), Швеція (57), Норвегія (62), Японія (62). Це також характерно й для Малайзії, Росії, Індії та ряду інших країн, що розвиваються, тобто за рівнем протидії кіберзагрозам вони випереджають ряд розвинутих країн. Можна виділити й Нігерію, показник якої дорівнює 55, тобто за рівнем національної кібербезпеки дана країна наздоганяє Канаду та Швецію. Що стосується країн, які є найменш розвинутими (Тувалу, Південний Судан, Соломонові острови, Конго, Бурунді, Туркменістан, Домініка, Кірібаті, Самоа, Беліз та ряд інших), то вони мають доволі низькі значення NCSI. Тобто візуальний аналіз дозволяє зробити висновок, що в основному країни, які є розвинутими мають дійсно найбільші значення показника національного рівня кібербезпеки, що говорить про її високий рівень в цілому. Хоча частина країн, які вважаються тими, що розвиваються, також мають досить високі значення.

Якщо порівнювати рейтинги країн за «Глобальним» та «Національним індексами кібербезпеки», то можна побачити, що за GCI більшість країн світу мають рейтинги вище середнього значення, а за NCSI переважна більшість мають усереднені значення. Тобто це свідчить про те, що є проблеми, пов’язані із спроможністю долати різного роду кіберзагрози, хоча в цілому загальний стан системи національної кібербезпеки відповідає рівню економічного розвитку країни. Можна попередньо прийняти нашу гіпотезу щодо існування впливу рівня розвитку країн на рівень інформаційної безпеки країни.

«Індекс розвитку інформаційних та комунікаційних технологій» (далі ICT DI) характеризує рівень розвитку інформаційних та комунікаційних технологій (далі ІКТ) в країні. Його основними цілями є вимірювання: рівня та

еволюції у часі ІКТ в країнах; ступеня прогресу у їх розвитку; відмінностей між різними країнами з точки зору їх розвитку ІКТ; потенціалу подальшого їх розвитку [234]. Він розраховується, як інтегральний показник, на основі 11 показників, які згруповані в свою чергу за трьома субіндексами: доступ, використання та навички. Використовуючи емпіричні значення ICT DI за 2018 рік для 159 країн світу, побудовано карту для їх візуального аналізу та оцінки (рисунок 2.3).

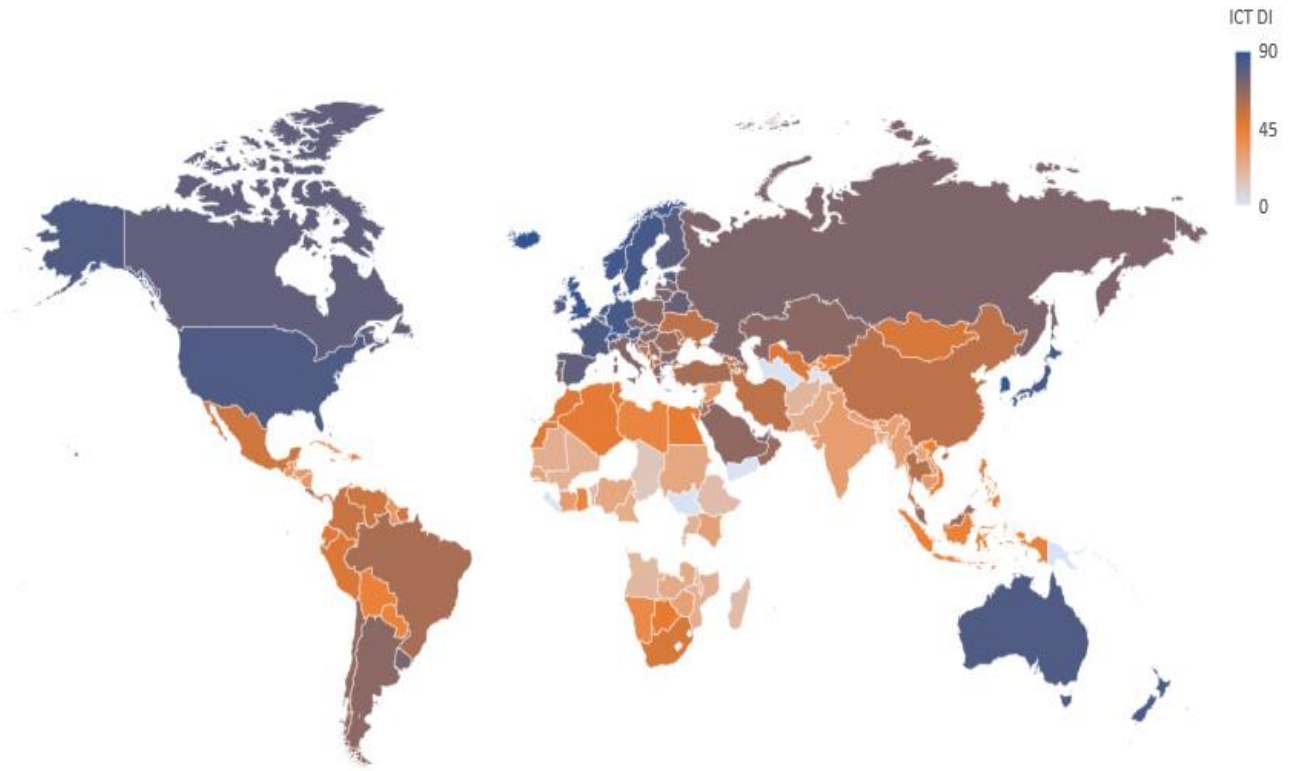


Рисунок 2.3 – Карта рейтингування країн за «Індексом розвитку інформаційних та комунікаційних технологій» за 2018 рік

Джерело: побудовано авторкою на основі [86]

Аналізуючи дані рисунку 2.3, можна підтвердити попередні висновки, що країни, які є розвинутими, мають високі значення NCSI (Ісландія – 90, Південна Корея – 89, Данія – 87; Швейцарія – 87, Великобританія – 87, Люксембург – 85, Нідерланди – 85, Норвегія – 85, Німеччина – 84, Японія – 84, Швеція – 84, Нова Зеландія – 83, Австралія – 82, Франція – 82, США – 82 та інші), найменш розвинутим країнам відповідають низькі (Бурунді – 15, Чад – 13, Конго – 16,

Ефіопія – 17, Гаїті – 17, Мадагаскар – 17, Малаві – 17, Танзанія – 18, Ангола – 19, Бенін – 19, Афганістан – 20, Соломонові острови – 21, Уганда – 22, Руанда – 22, Малі – 22, Кірібаті –22). Україна знаходиться на 75 місці із значенням 56, на рівні Китаю та Ірану, що відповідає середньому рівню розвитку інформаційних та комунікаційних технологій. Хоча спостерігається зміна у країнах лідерах та аутсайдерах у порівнянні із рейтингами за NCSI та GCI, але тенденція щодо відповідності рівня економічного розвитку країни до відповідного показника інформаційної безпеки зберігається.

«Індекс мережевої готовності» (далі NRI) вимірює ступінь технологічної готовності країни для застосування новітніх інформаційно-комунікаційних технологій в різних сферах. Його використання дозволяє провести комплексну оцінку багатофакторного впливу ІКТ на розвиток суспільства та окремих країн. Його розрахунок відбувається за чотирма напрямами – технологія, люди, управління та вплив, що поділяються на 12 субнапрямів, яким відповідають 62 індикатори [79, с. 22]. Використовуючи його фактичні значення за 2018 рік, побудовано карту для аналізу та оцінки (рисунок 2.4).

Аналізуючи дані NRI (рисунок 2.4), можна побачити, що високій рівень технологічної готовності характерний для наступних країн: Фінляндія (86), Сінгапур (86), Нідерланди (83), Норвегія (83), Швеція (83), Швейцарія (83), США (83), Люксембург (81), Великобританія (81), Канада (80), Данія (80), Німеччина (80), Японія (80), Південна Корея (80) та інші. Країни із низьким значенням – це: Чад, Бурунді, Мавританія, Гаїті, Мадагаскар, М’янма, Малаві, Нікарагуа, Ліберія, Танзанія, Малі, Бенін та інші. Україна знаходиться на 61-му місці із значенням показника 60, на рівні із такими країнами, як Китай, Йорданія, Тайланд, Південна Африка, що відповідає вище середнього рівню технологічної готовності. Не дивлячись на зміни рейтингів країн, можна підтвердити висновок, що є зв'язок між рівнем розвитку економіки країни та значенням її NRI.

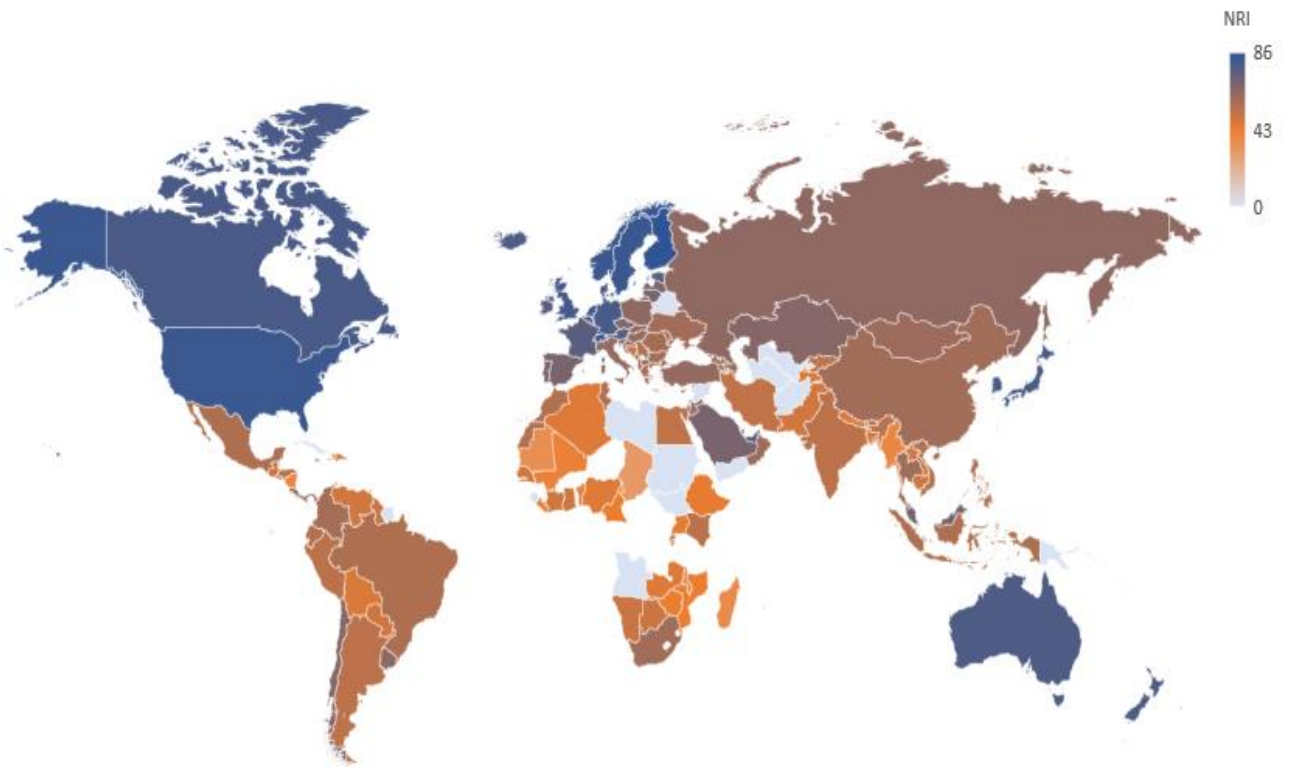


Рисунок 2.4 – Карта рейтингування країн за «Індексом мережевої готовності» за 2018 р.

Джерело: побудовано авторкою на основі [86]

«Рівень цифрового розвитку» (DDL) характеризує рівень цифровізації країни та визначається, як середній відсоток, який країна отримала від максимального значення «Індексу розвитку ІКТ» та «Індексу мережевої готовності». Порівняння країн за DDL та NCSI дозволяє визначити, наскільки ступінь цифровізації країни відповідає рівню її кібербезпеки, що сприяє формуванню рекомендацій щодо коректування програми кібербезпеки. Використовуючи фактичні значення DDL за 2018 рік, побудуємо карту, щоб провести візуальний аналіз (рисунок 2.5).

Результати, відображені на карті 2.5, свідчать, що: розвинуті країни мають високий рівень цифрового розвитку; більшість країн, що розвивається, – середній та вище середнього; найменш розвинуті країни – низький. Тобто тенденції відповідності рівня інформаційної безпеки рівню економічного розвитку зберігаються й в цьому випадку.

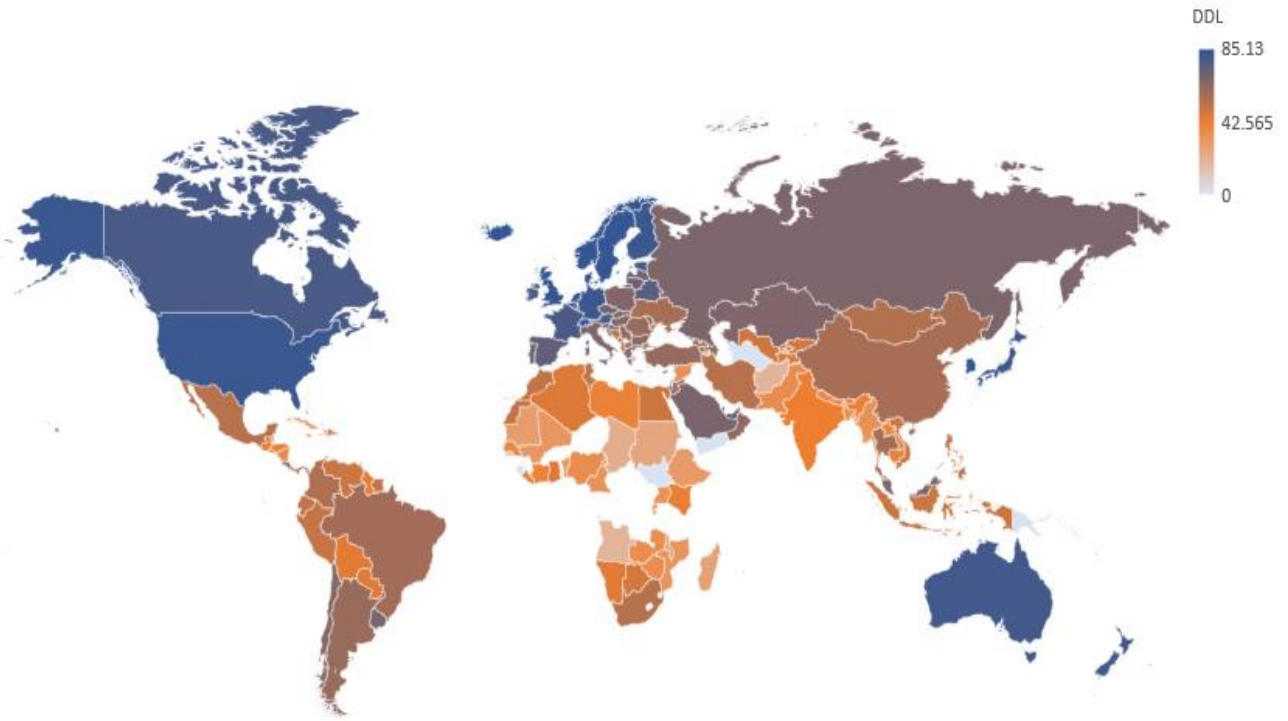


Рисунок 2.5 – Карта рейтингування країн за «Рівнем цифрового розвитку» за 2018 р.

Джерело: побудовано авторкою на основі [86]

Значення проаналізованих п’яти індикаторів для України показують, що в даному питанні нею зроблено потужні кроки на державному рівні. Це може свідчити про наявність потенційних можливостей для країни щодо розвитку різних складових її інформаційної безпеки, які виступатимуть стимулюючим драйвером й для національної економіки та національної безпеки в цілому.

Групу п’яти індикаторів, що вимірюють інформаційну безпеку, пропонуємо назвати індикаторами цифрової спроможності і кібербезпеки країни та використаємо для підтвердження або відхилення висунутої гіпотези.

На другому етапі після проведеного візуального аналізу оберемо показники, які характеризують рівень розвитку національної економіки. Вибір відбувався шляхом застосування методів наукового пізнання – аналізу, синтезу та дедукції, до переліку показників світового розвитку, представлених на сайті Світового банку [257]. В процесі відбору враховувалися ті аспекти розвитку національної економіки, які б могли безпосередньо залежати від рівня

інформаційної безпеки, тобто економічні, соціальні, політичні, технологічні та інші. Таким чином, базу дослідження сформували 37 показників для 159 країн світу за 2018 рік, оскільки саме для цього часового інтервалу та саме для цієї кількості країн зібрані повні дані (див. табл. 2.1).

Таблиця 2.1 – Індикатори розвитку національної економіки

№	Назва індикатора англійською мовою	Назва індикатора українською мовою	Група*
1	GDP per capita (current US$)	ВВП на душу населення (у поточних доларах США)	ЕР
2	General government expenditure (% of GDP)	Загальнодержавні витрати на кінцеве споживання (% від ВВП)	ЕР
3	Portfolio Investment, net (BoP, current US$)	Чисті портфельні інвестиції (платіжний баланс, у поточних доларах США)	ФР
4	Unemployment, total (% of total labor force)	Загальний рівень безробіття (% від загальної робочої сили)	СР
5	Life expectancy	Ймовірна тривалість життя	СР
6	Total reserves (includes gold, current US$)	Загальні резерви (включаючи золото, у поточних доларах США)	ФР
7	Current account balance (BoP, current US$)	Сальдо поточного рахунку (платіжний баланс, у поточних доларах США)	ЗЕД
8	Wage and salaried workers, total (% of total employment)	Оплачувані та наймані працівники (% від загальної кількості зайнятих)	СР
9	GINI index	Індекс GINI	СР
10	Control of Corruption: Estimate	Оцінка контролю корупції	ІС
11	Government Effectiveness: Estimate	Оцінка ефективності уряду	ІС
12	Political Stability and Absence of Violence/Terrorism: Estimate	Оцінка політичної стабільності та відсутності насильства / тероризму	ІС
13	Regulatory Quality: Estimate	Оцінка якості регуляторів	ІС
14	Rule of Law: Estimate	Оцінка верховенства права	ІС
15	Exports of goods and services (% of GDP)	Експорт товарів та послуг (% від ВВП)	ЗЕД
16	External debt stocks, total (DOD, current US$)	Запаси зовнішньої заборгованості, загальна (погашена та непогашена заборгованість, у поточних доларах США)	ЗЕД
17	Foreign direct investment, net inflows (BoP, current US$)	Чистий приплив прямих іноземних інвестицій (платіжний баланс, у поточних доларах США)	ФР
18	GDP (current US$)	ВВП (поточні долари США)	ЕР
19	GDP growth (annual %)	Приріст ВВП (річний у %)	ЕР
20	GNI per capita, PPP (current international $)	ВНД на душу населення, за паритетом купівельної здатності (у поточних міжнародних доларах)	ЕР

Продовження таблиці 2.1

№	Назва індикатора англійською мовою	Назва індикатора українською мовою	Група*
21	GNI, PPP (current international $)	ВНД, за паритетом купівельної здатності (у поточних міжнародних доларах)	ЕР
22	Gross capital formation (% of GDP)	Валовий капітал (% від ВВП)	ЕР
23	Imports of goods and services (% of GDP)	Імпорт товарів та послуг (% від ВВП)	ЗЕД
24	Industry (including construction), value added (% of GDP)	Промисловість, включаючи будівництво, додана вартість (% від ВВП)	ЕР
25	Inflation, GDP deflator (annual %)	Інфляція, дефлятор ВВП (річний у %)	ФР
26	Mobile cellular subscriptions (per 100 people)	Кількість підписок на послуги мобільного зв'язку (на 100 осіб)	ІА
27	Revenue, excluding grants (% of GDP)	Дохід, без урахування грантів (% від ВВП)	ЕР
28	Statistical Capacity score (Overall average)	Оцінка потужності статистичної системи країни	ЯІІ
29	Tax revenue (% of GDP)	Податкові надходження (% від ВВП)	ФР
30	Individuals using the Internet (% of population)	Кількість осіб, які користуються Інтернетом (% від населення країни)	ІА
31	Secure Internet servers (per 1 million people)	Кількість захищених Інтернет-серверів (на 1 мільйон людей)	ЯІІ
32	Charges for the use of intellectual property, payments (BoP, current US$)	Плата за використання інтелектуальної власності, платежі (BoP, поточні долари США)	ІА
33	Charges for the use of intellectual property, receipts (BoP, current US$)	Збори за використання інтелектуальної власності, квитанції (BoP, поточні долари США)	ІА
34	High-technology exports (% of manufactured exports)	Високотехнологічний експорт (% від промислового експорту)	ІА
35	Patent applications, nonresidents	Патентні заявки, нерезиденти	ІА
36	Patent applications, residents	Патентні заявки, резиденти	ІА
37	Scientific and technical journal articles	Статті науково-технічних журналів	ІА

*ІС – інституційна спроможність; ЕР – економічний розвиток; СР – соціальний розвиток; ФР – фінансовий розвиток; ЗЕД – зовнішньоекономічна діяльність; ІА – інноваційна активність; ЯІІ – якість інформаційної інфраструктури.

На третьому кроці для подальшого доведення гіпотези проведемо канонічний аналіз, який дозволить математично її прийняти або відхилити. Даний інструмент дозволяє досліджувати лінійні залежності між двома множинами змінних та виявляти зв’язки між ними, що сприяє подальшій оцінці ступеня впливу однієї множини на іншу та обґрунтуванню її статистичної

значущості [Халафян, с. 185]. Загальну ідею аналізу зобразимо у вигляді наступних рівнянь (2.1):

$$Y = a_1 y_1 + a_2 y_2 + \cdots + a_n y_n, \qquad (2.1)$$
$$X = b_1 x_1 + b_2 x_2 + \cdots + b_m x_m,$$

де $y_1, y_2, \ldots, y_n$ – множина змінних, які відображають *n (5)* показників групи цифрової спроможності і кібербезпеки;

$x_1, x_2, \ldots, x_m$ – множина змінних, які відображають *m (37)* показників, що характеризують розвиток національної економіки країни;

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

$a_1, a_2, \ldots, a_n$; $b_1, b_2, \ldots, b_m$ - вагові коефіцієнти, які розраховуються, виходячи з максимальної корельованості обох множин.

Розрахунки проводилися із використанням модуля канонічного аналізу у аналітичному пакеті “STATISTICA” [223], в результаті чого отримано підсумки, представлені на рисунку 2.6.

З рисунку 2.6 можна побачити, що значення канонічної кореляції R ≈ 0,9752, тобто між множиною відібраних факторів розвитку національної економіки та індексами цифрової спроможності і кібербезпеки існує сильний кореляційний зв'язок. Як результат, збільшення впливу факторів розвитку національної економіки викликає підвищення рівня інформаційної безпеки країни та, навпаки, посилення рівня безпеки позитивно впливає на розвиток країни. Значимість коефіцієнта кореляції підтверджує високе значення критерію Пірсона ($\text{Chi}^2 = 643{,}92$) (перевищує табличне значення 154,5377), рівень значущості якого не перевищує 0,05 (p = 0,0000). Також можна побачити, що значення надмірності для лівої множини, яка відповідає індикаторам цифрової спроможності і кібербезпеки, дорівнює 82,4650%, тобто змінні правої множини, які відповідають обраним індикаторам розвитку країни, на 82,4650% пояснюють мінливість показників інформаційної безпеки, що є досить високим показником.

N=159	Canonical Analysis Summary Canonical R: .97517 Chi²(185)=643.92 p=0.0000 **Left Set**	Right Set
No. of variables	5	37
Variance extracted	100.000%	34.6054%
Total redundancy	82.4650%	26.5405%
Variables: 1	Global Cybersecurity Index	GDP per capita
2	ICT Development Index	General government expenditure
3	Networked Readiness Index	Life expectancy
4	National Cyber Security Index	Wage and salaried workers
5	Digital Development Level	Control of Corruption
6		Government Effectiveness
7		Regulatory Quality
8		Rule of Law
9		GNI per capita, PPP
10		Mobile cellular subscriptions
11		Revenue, excluding grants
12		Individuals using the Internet
13		Portfolio investment
14		Unemployment
15		Total reserves
16		Current account balance
17		GINI index
18		Political Stability and Absence of Violence/Terrorism
19		Exports of goods and services
20		External debt stocks, total
21		Foreign direct investment, net inflows
22		GDP
23		GDP growth
24		GNI, PPP
25		Gross capital formation
26		Imports of goods and services
27		Industry (including construction)
28		Inflation, GDP deflator
29		Statistical Capacity score
30		Tax revenue
31		Secure Internet servers
32		Charges for the use of intellectual property, payments
33		Charges for the use of intellectual property, receipts
34		High-technology exports
35		Patent applications, nonresidents
36		Patent applications, residents
37		Scientific and technical journal articles

Рисунок 2.6 – Підсумки канонічного аналізу (складено авторкою)

В свою чергу, фактори безпеки на 26,5405% пояснюють мінливість факторів розвитку національної економіки країни, тобто на 26,5405% розвиток країни залежить також від рівня захищеності інформаційного та кібернетичного простору держави. Дане значення відповідає слабкому рівню лінійного

кореляційного зв’язку, але у випадку такої специфічної сфери, як інформаційна безпека, можна вважати, що існує взаємовплив між обома групами індикаторів, хоча він є нерівноцінним.

Отримані результати свідчать також про те, що можливо не всі показники розвитку національної економіки країни здійснюють вплив на інформаційну безпеку та навпаки. Тобто є індикатори, які впливають у більшій мірі, ніж інші. Тому проведемо дослідження стосовно рівня впливу окремих груп індикаторів, які було виділено в таблиці 2.1, на групу індикаторів цифрової спроможності національної економіки та кібербезпеки, та навпаки. Для цього знову проведемо канонічний аналіз для кожної групи показників у аналітичному пакеті “STATISTICA”.

Результати для групи економічного розвитку та цифрової спроможності національної економіки і кібербезпеки представлені на рисунку 2.7.

N=159	Canonical Analysis Summary (Kanonich_analyse.sta) Canonical R: .86156 Chi²(45)=270.67 p=0.0000 **Left Set**	Right Set
No. of variables	5	9
Variance extracted	100.000%	68.3363%
Total redundancy	60.9996%	26.4918%
Variables: 1	Global Cybersecurity Index	GDP per capita
2	ICT Development Index	General government expenditure
3	Networked Readiness Index	GDP
4	National Cyber Security Index	GDP growth
5	Digital Development Level	GNI per capita, PPP
6		GNI, PPP
7		Gross capital formation
8		Industry (including construction)
9		Revenue, excluding grants

Рисунок 2.7 – Підсумки канонічного аналізу для групи індикаторів економічного розвитку та цифрової спроможності національної економіки і кібербезпеки (складено авторкою)

З рисунку 2.7 можна побачити, що нове значення канонічної кореляції R ≈ 0,8616, тобто між множиною відібраних факторів економічного розвитку та цифрової спроможності національної економіки і кібербезпеки існує високий

кореляційний зв'язок. Хоча воно нижче за попередній результат (рисунок 2.6), але цю різницю можна пояснити за рахунок зменшення кількості факторів для аналізу. Значимість нового значення коефіцієнту кореляції підтверджується високим значенням критерію Пірсона ($Chi^2 = 270{,}67$) (перевищує табличне значення 30,6123), рівень значущості якого не перевищує 0,05 (p = 0,0000). Значення надмірності для лівої множини, яка відповідає індикаторам цифрової спроможності, дорівнює 60,9996%, тобто індикатори економічного розвитку країни на 60,9996% пояснюють мінливість показників інформаційної безпеки, що вказує на помітний зв'язок. Фактори цифрової спроможності на 26,4918% пояснюють мінливість відібраних індикаторів економічного розвитку, тобто на 26,4918% він залежить від рівня інформаційної безпеки. Отриманий результат корелює із тим, який було отримано для всіх 37 показників, а його значення вказує на слабкий зв'язок.

Проаналізуємо взаємовпливи індикаторів групи інституційної спроможності та цифрової спроможності національної економіки і кібербезпеки (рисунок 2.8).

	Canonical Analysis Summary (Kanonich_analyse.sta) Canonical R: .90520 Chi²(25)=322.15 p=0.0000	
N=159	**Left Set**	Right Set
No. of variables	5	5
Variance extracted	100.000%	100.000%
Total redundancy	67.8652%	59.8153%
Variables: 1	Global Cybersecurity Index	Control of Corruption
2	ICT Development Index	Government Effectiveness
3	Networked Readiness Index	Regulatory Quality
4	National Cyber Security Index	Rule of Law
5	Digital Development Level	Political Stability and Absence of Violence/Terrorism

Рисунок 2.8 – Підсумки канонічного аналізу для групи інституційної спроможності та цифрової спроможності національної економіки і кібербезпеки (складено авторкою)

Значення канонічної кореляції R ≈ 0,9052 (рисунок 2.8), що вказує на дуже високий зв'язок між множиною факторів інституційної спроможності та

цифрової спроможності національної економіки і кібербезпеки. Його значимість підтверджується високим значенням критерію Пірсона ($Chi^2 = 322,15$) (перевищує табличне значення 14,6114), рівень значущості якого не перевищує 0,05 (p = 0,0000). Виявлено, що індикатори інституційної спроможності країни на 67,8652% пояснюють 100% мінливості показників інформаційної безпеки, що вказує на помітний зв'язок. Індикатори цифрової спроможності на 59,8153% пояснюють 100% мінливості індикаторів інституційної спроможності, що також вказує на помітний зв'язок.

Підсумки канонічного аналізу для інших груп представлені на рисунках А.1 – А.5 у додатку А. Отримані результати свідчать, що найбільший взаємний вплив між показниками розвитку національної економіки та інформаційної безпеки відбувається між групами інституційної спроможності та цифрової спроможності національної економіки і кібербезпеки. Це можна пояснити тим, що саме індикатори інституційного розвитку є важливим напрямом регулювання з боку державних органів питань, пов’язаних із національною безпекою в цілому та інформаційною безпекою зокрема. Тому для подальшого дослідження оберемо саме ці дві групи індикаторів.

Далі необхідно визначити вагові коефіцієнти для кожної групи показників, щоб визначити ті, значення яких є критично важливим для подальшого розвитку національної економіки. Для цього оберемо ті канонічні корені, які є статистично значущими. Результат даної процедури представлений на рисунку 2.9.

Root Removed	Chi-Square Tests with Successive Roots Removed					
	Canonicl R	Canonicl R-sqr.	Chi-sqr.	df	p	Lambda Prime
0	0.905205	0.819396	322.1541	25	0.000000	0.120937
1	0.493304	0.243349	61.1582	16	0.000000	0.669625
2	0.307298	0.094432	18.6332	9	0.028532	0.884985
3	0.150662	0.022699	3.5062	4	0.476948	0.977271
4	0.005547	0.000031	0.0047	1	0.945386	0.999969

Рисунок 2.9 – Оцінка статистичної значущості канонічних коренів (складено авторкою)

З рисунку 2.9 визначаємо, що Chi-квадрат у першому рядку, який відповідає аналізу без видалення коренів, є статистично значущим ($p < 0,05$), тому хоча б один канонічний корень є також статистично значущим. При видаленні першого найбільш значущого кореня (другий рядок таблиці на рисунку 2.9) отримали, що інші корені, які залишилися, є також значущими. Процедуру повторюємо доти, доки $p > 0,05$. В результаті отримали три статистично значущих кореня, тобто доцільно розглядати три пари канонічних змінних. Але для отримання достовірних оцінок навантажень канонічних факторів для трьох пар канонічних змінних необхідно мати вибірку, яка буде перевищувати в 40-60 раз кількість початкових даних [369, с. 190], тому приймаємо рішення, що будемо розглядати тільки перший найбільш значущий корень. Для підтвердження своїх висновків визначимо факторну структуру та надмірність (рисунки 2.10-2.11).

Root Variable	Factor Structure, left set				
	Root 1	Root 2	Root 3	Root 4	Root 5
Global Cybersecurity Index	0.873416	-0.346104	-0.311306	0.038100	0.137821
ICT Development Index	0.928860	0.321630	-0.034100	0.140694	-0.113202
Networked Readiness Index	0.827951	-0.355652	0.243930	-0.312957	-0.174830
Digital Development Level	0.952405	0.295333	0.028724	-0.053828	0.044498
National Cyber Security Index	0.862370	-0.255396	0.219263	0.326653	0.190557

Рисунок 2.10 – Факторна структура для показників цифрової спроможності і кібербезпеки (складено авторкою)

Root Variable	Factor Structure, right set				
	Root 1	Root 2	Root 3	Root 4	Root 5
Control of Corruption: Estimate	0.777627	0.525191	0.006145	0.235554	0.252879
Government Effectiveness: Estimate	0.947564	0.283585	-0.070543	0.129188	-0.005981
Political Stability and Absence of Violence/Terrorism: Estimate	0.522121	0.714587	0.062270	0.300382	-0.350214
Regulatory Quality: Estimate	0.927218	0.197926	0.275896	0.154750	0.032046
Rule of Law: Estimate	0.832194	0.333729	0.041054	0.432115	0.087572

Рисунок 2.11 – Факторна структура для показників інституційної спроможності країни (складено авторкою)

Найбільші факторні навантаження (наближені до 1) мають показники, що відповідають першому кореню, як для лівої, так й для правої множини, що

підтверджує правильність вибору тільки одного кореня. Оскільки факторні навантаження представляють собою кореляції між показниками множини, то показники цифрової спроможності і кібербезпеки демонструють сильний (0,70-0,89) та дуже сильний (вище 0,90) кореляційний зв'язок. Що стосується факторів групи інституційної спроможності, то між ними зустрічаються ті, які демонструють значний (0,50-0,69), сильний (0,70-0,89) та дуже сильний (вище 0,90) зв'язок. Виходячи із отриманих результатів, можна зробити висновок, що між канонічними змінними та змінними із заданої множини існує досить тісний лінійний зв'язок, що є підтвердженням гіпотези щодо існування обопільного впливу між показниками інституційної та цифрової спроможності і кібербезпеки для національної економіки.

Проаналізуємо частки та надмірності дисперсії (рисунки 2.12 - 2.13).

Root Factor	Variance Extracted (Proportions), left set	
	Variance extractd	Reddncy.
Root 1	0.792379	0.649273
Root 2	0.100434	0.024440
Root 3	0.041295	0.003900
Root 4	0.045758	0.001039
Root 5	0.020133	0.000001

Рисунок 2.12 – Дисперсія та надмірність для показників цифрової спроможності і кібербезпеки (складено авторкою)

Root Variable	Variance Extracted (Proportions), right set	
	Variance extractd	Reddncy.
Root 1	0.665494	0.545303
Root 2	0.203486	0.049518
Root 3	0.017339	0.001637
Root 4	0.074615	0.001694
Root 5	0.039066	0.000001

Рисунок 2.13 – Дисперсія та надмірність для показників інституційної спроможності країни (складено авторкою)

У випадку аналізу показників цифрової спроможності і кібербезпеки 100% дисперсії будуть пояснювати усі вилучені корені (рисунок 2.12), у випадку факторів інституційної спроможності країни також 100% (рисунок 2.13). Перший канонічний корень вилучає 79,2379% дисперсії із показників цифрової спроможності та 66,5494% дисперсії з факторів інституційної спроможності країни, тобто пояснює 79,2379% та 66,5494% зміни рівня інформаційної безпеки та рівня інституційної спроможності. Інші корені, хоча не будуть прийматися до уваги, пояснюють приблизно від 2 до 20% змін, що є недостатнім для подальшого обґрунтування. З огляду на надмірність, 64,9273% факторів інституційної спроможності пояснюють зміни показників лівої множини, тобто складових інформаційної безпеки (рисунок 2.12). 54,5303% факторів цифрової спроможності і кібербезпеки пояснюють зміни, що пов’язані із розвитком країни. Як результат, фактори інституційної спроможності національної економіки країни є більш інформативними для передбачення рівня розвитку національної системи інформаційної безпеки країни.

Для подальшого аналізу визначимо канонічні ваги, які є коефіцієнтами регресійних рівнянь, де канонічні змінні є відповідними відкликами, що дозволить оцінити внесок кожного фактору у множину аналізованих показників (рисунки 2.14-2.15).

Значення канонічних вагів дозволяє визначити внесок кожного показника у формування значень канонічних змінних, для чого використовується їх абсолютне значення. У структуру показників цифрової спроможності і кібербезпеки вноситимуть найбільший вклад (рисунок 2.14): рівень цифрового розвитку (0,3120), індекс розвитку інформаційних та комунікаційних технологій (0,2654), глобальний індекс кібербезпеки (0,2300), індекс мережевої готовності (0,2012). Найменший вклад здійснюватиме національний індекс кібербезпеки (0,1031). Тобто, вищий рівень розвитку інформаційно-комунікаційних та цифрових технологій впливає на підвищення рівня інформаційної безпеки у країні, що сприятиме також й зростанню рівня національної економіки в умовах її цифровізації.

Variable	Canonical Weights, left set				
	Root 1	Root 2	Root 3	Root 4	Root 5
Global Cybersecurity Index	0.229990	-0.655737	-1.71076	-0.16591	0.33319
ICT Development Index	0.265376	0.123005	-0.74285	1.99580	-3.60254
Networked Readiness Index	0.201227	-0.649078	0.63293	-0.71868	-1.27691
Digital Development Level	0.311982	1.381337	0.62972	-2.22520	3.52931
National Cyber Security Index	0.103073	-0.370735	1.22966	1.16586	0.87101

Рисунок 2.14 – Канонічні ваги для показників цифрової спроможності і кібербезпеки (складено авторкою)

Variable	Canonical Weights, right set				
	Root 1	Root 2	Root 3	Root 4	Root 5
Control of Corruption: Estimate	-0.358167	1.89317	0.28845	-1.26490	2.29527
Government Effectiveness: Estimate	1.216174	-0.61319	-2.74266	-1.38274	-1.11168
Political Stability and Absence of Violence/Terrorism: Estimate	-0.273221	0.99237	0.36340	-0.03151	-1.20029
Regulatory Quality: Estimate	0.398635	-0.20492	2.92997	-0.87671	-0.05481
Rule of Law: Estimate	-0.121186	-1.46513	-0.63917	3.75298	-0.06483

Рисунок 2.15 – Канонічні ваги для показників інституційної спроможності країни (складено авторкою)

Що стосується факторів інституційної спроможності, то найбільший вклад втілюватиме оцінка ефективності уряду (1,2162) (рисунок 2.15). Це свідчить, що існує висока залежність між урядовими рішеннями та наслідками в економіці, тобто вони здійснюють максимальний вплив й на інформаційну безпеку країни. У порівнянні із значенням вкладу даного показника, найменший внесок здійснюють: оцінка якості регуляторів (0,3986), оцінка контролю корупції (-0,3582), оцінка політичної стабільності та відсутності насилля та тероризму (-0,2732), оцінка верховенства права (-0,1212). Серед отриманих результатів ряд показників мають від'ємне значення. Якщо вага має знак «+», то із збільшенням фактору значення кореня збільшується, якщо «–», навпаки, значення кореня зменшується. Наприклад, якщо рівень контролю корупції цифрового розвитку країни буде збільшуватися, то це буде зменшувати внесок даного вкладу у значення кореня. У випадку із отриманими розрахунками можна сказати, що

обернений вплив компенсується можливо вищим навантаженням за рахунок інших індикаторів інституційного розвитку національної економіки.

На наступному кроці побудуємо діаграму розсіювання канонічних значень для першої пари канонічних коренів (рисунок 2.16), в якій горизонтальна вісь – це складові інформаційної безпеки, а вертикальна – показники розвитку національної економіки країни.

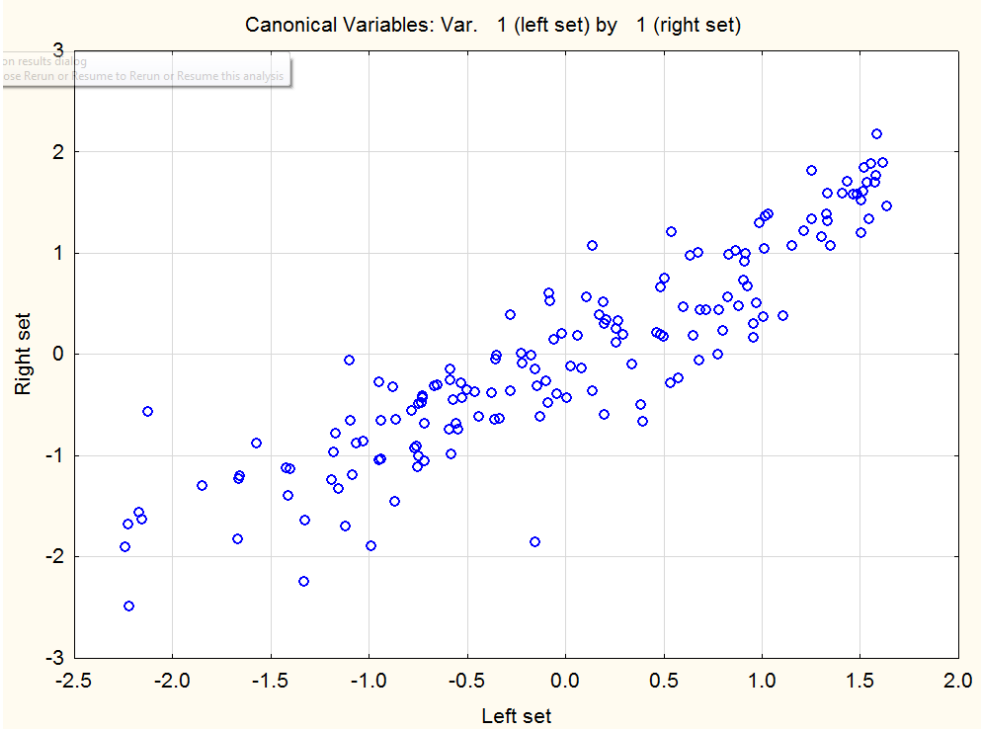


Рисунок 2.16 – Діаграма розсіювання канонічних значень (складено авторкою)

На діаграмі 2.16 можна побачити, що скупчення спостережень є характерним для лінійної залежності, при цьому графік не містить значних викидів, окрім двох, що можливо обумовлено різними темпами розвитку інформаційної безпеки та інституційної спроможності для деяких країн. В цілому, отримані значення діаграми 2.16 свідчать про те, що між індексами інституційної та цифрової спроможності національної економіки є досить тісний зв'язок, який говорить про те, що рівень інформаційної безпеки залежить від рівня розвитку країни, при цьому рівень безпеки може також впливати й на розвиток національної економіки.

Розраховані значення канонічних вагів дозволили визначити рівняння регресії (2.2) для канонічних змінних лівого та правого множин:

$$Y\ (1\ \text{корень}) = \ 0{,}3120\ y_1 + \ 0{,}2654\ y_2 + 0{,}2300\ y_3 + \\ + 0{,}2012\ y_4 + \ 0{,}1031\ y_5,$$

$$X\ (1\ \text{корень}) = \ 1{,}2162\ x_1 + \ 0{,}3986\ x_2 - 0{,}3582\ x_3 - \\ -0{,}2732\ x_4 - 0{,}1212\ x_5 \tag{2.2}$$

При потребі у визначенні для кожної країни значення канонічних змінних необхідно підставити в отриманні рівняння (2.2) значення факторів інституційної спроможності та цифрової спроможності і кібербезпеки. Це дозволить знайти зважену суму факторів з урахуванням впливу множин один на одну. Числові результати представлені у таблицях А.1 – А.2 додатку А, а географія їх розподілу – на рисунках 2.17 та 2.18.

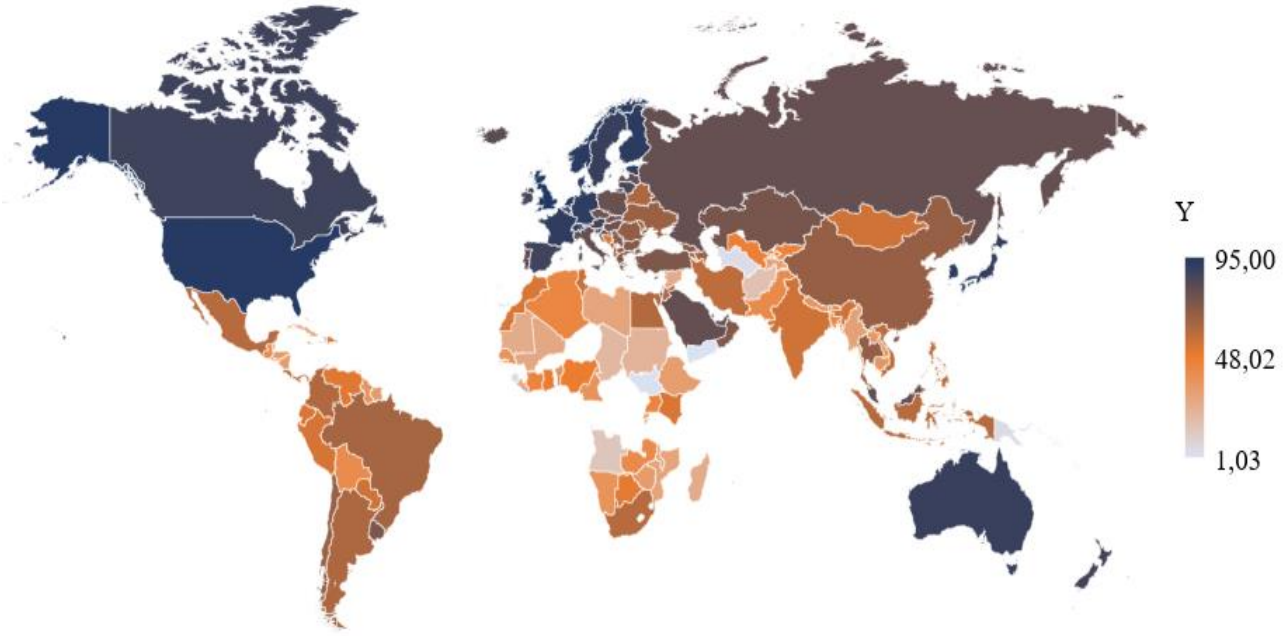


Рисунок 2.17 – Географія розподілу канонічної змінної, яка відповідає індикаторам цифрової спроможності і кібербезпеки (складено авторкою)

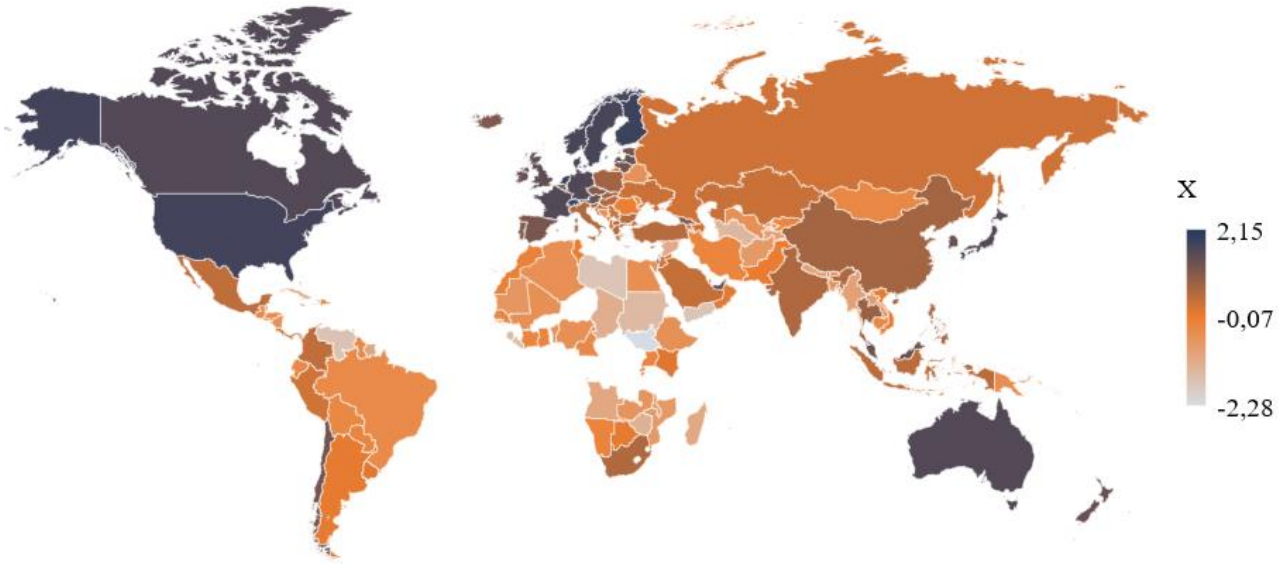


Рисунок 2.18 – Географія розподілу канонічної змінної, яка відповідає індикаторам інституційної спроможності країни (складено авторкою)

Аналізуючи отримані результати канонічного кореня для показників цифрової спроможності та кібербезпеки (рисунок 2.17), можна зробити висновок, що США, Канада, Австралія та ряд європейських країн з високим рівнем добробуту мають найвище зважене сумарне значення групи показників цифрової спроможності та кібербезпеки, що характеризує їх, як країни із високим потенціалом інформаційної безпеки. Найнижчий рівень відповідає країнам із низьким рівнем добробуту. Україна серед усіх країн має рівень вище середнього, оскільки значення її канонічного кореня дорівнює 66,7997, що свідчить про достатні можливості для формування інформаційної безпеки як драйверу розвитку її національної економіки. Аналіз результатів канонічної змінної, що відповідає зваженому сумарному значенню групи показників інституційної спроможності (рисунок 2.18) також підтверджує висновки щодо відповідності рівня добробуту країн значенням їх інституційної спроможності, хоча в даному випадку кількість країн із нижче середнім результатом є дещо більшою, що говорить про критичність даного аспекту розвитку країн. Для України зважене значення є також вище середнього (0,3062), що на тлі від'ємних значень показників інституційної спроможності свідчить про їх сумарне зростання саме під впливом цифрового розвитку та рівня кібербезпеки. Це

підтверджує існування взаємного впливу між інформаційною безпекою та розвитком національної економіки, що дозволяє говорити про її можливості, як драйверу.

Узагальнення найбільш важливих результатів канонічного аналізу представимо у вигляді рисунку 2.19.

Виходячи з результатів проведеного дослідження, можна прийняти гіпотезу щодо існування взаємної обумовленості системи інформаційної безпеки та рівня розвитку національної економіки країни. Дану гіпотезу було підтверджено візуальним аналізом карти країн світу, розподілених за п’ятьма індексами інформаційної безпеки. Даний аналіз підтвердив, що країни, які відносяться до розвинутих, мають найвищі значення. Найменш розвинуті країни мають найнижчі значення індексів. Оскільки обрані показники характеризують окремі аспекти інформаційної безпеки країни, то було прийнято рішення об’єднати їх у групу цифрової спроможності та кібербезпеки країни.

В результаті проведеного канонічного аналізу було визначено, що приблизно 67,87% множини показників цифрової спроможності та кібербезпеки пояснюються факторами розвитку національної економіки. Оскільки вони оцінюють спроможність країни протистояти різним кіберзагрозам, то у країн із високим економічним потенціалом збільшуються можливості їм протидіяти, а також зростає фінансова спроможність для організації додаткових заходів, залучення більш сучасних технологій, кваліфікованих фахівців. Але з іншого боку, саме у таких країнах підвищується ризик кібератак, інформаційного тероризму та кібершахрайства.

Також було визначено, що 59,82% множини факторів інституційної спроможності країни пояснюється за рахунок складових інформаційної безпеки. Тобто підвищення її рівня в цілому сприятиме розвитку країни в частині соціального, економічного та політичного розвитку. Чим вище рівень захищеності персональних даних, тим вище довіра населення до держави та різних інститутів. Якщо це фінансові дані людини, тим вище надійність банківської системи та менше втрати від кібершахраїв.

а) оцінювання взаємного впливу груп індикаторів розвитку НЕ та групи індикаторів ЦСіКБ

Група індикаторів розвитку НЕ (R; Chi^2; p-value)	Значення показника TR	
	вплив групи відповідних індикаторів розвитку НЕ на групу показників ЦСіКБ, %	вплив групи показників ЦСіКБ на групу відповідних індикаторів розвитку НЕ, %
ІС (0,91; 322,15; <0,05)	67,87 (помітний)	59,82 (помітний)
ЕР (0,86; 270,67; <0,05)	61,00 (помітний)	26,49 (слабкий)
СР (0,79; 164,33; <0,05)	47,47 (помірний)	23,81 (слабкий)
ФР (0,60; 87,69; <0,05)	27,15 (слабкий)	10,59 (слабкий)
ЗЕД (0,58; 91,89; <0,05)	25,36 (слабкий)	15,43 (слабкий)
ІА (0,94; 387,04; <0,05)	67,80 (помітний)	24,72 (слабкий)
ЯІІ (0,51; 53,29; <0,05)	18,10 (слабкий)	18,41 (слабкий)

б) канонічні ваги для показників із найбільш впливових груп індикаторів (ІС та ЦСіКБ)

Показник групи ЦСіКБ	Канонічні ваги	Показник групи ІС	Канонічні ваги
ІР ІКТ	0,27	ОКК	–0,36
ІМГ	0,20	ОЕУ*	1,22
ГІК	0,23	ОЯР	0,40
НІК**	0,10	ОВП**	–0,12
РЦР*	0,31	ПС	–0,27

* Найбільш вагомий індикатор.

** Найменш вагомий індикатор.

ЦСіКБ – цифрова спроможність національної економіки (НЕ) та кібербезпека; ІС – інституційна спроможність; ЕР – економічний розвиток; СР – соціальний розвиток; ФР – фінансовий розвиток; ЗЕД – зовнішньо–економічна діяльність; ІА – інноваційна активність; ЯІІ – якість інформаційної інфраструктури; R – канонічний коефіцієнт кореляції (для ФР, ЗЕД, ЯІІ – помітний зв'язок; ЕР, СР – високий; ІС, ІА – дуже високий); Chi^2 – критерій хі-квадрат (усі значення більші за табличні, тому R – статистично значущий) ; p-value – p-рівень значущості (усі значення менші за 0,05 – критерій хі-квадрат є статистично значущим); TR – значення показника "Total Redundancy", яке в канонічному аналізі є характеристикою міри впливу однієї групи показників на іншу; ІР ІКТ – індекс розвитку інформаційних та комунікаційних технологій; ІМГ – індекс мережевої готовності; ГІК – глобальний індекс кібербезпеки; НІК – національний індекс кібербезпеки; РЦР – рівень цифрового розвитку; ОКК – оцінювання контролю корупції; ОЕУ – оцінювання ефективності уряду; ОЯР – оцінювання якості регуляторів; ОВП – оцінювання верховенства права; ПС – політична стабільність і відсутність насилля / тероризму

Рисунок 2.19 – Результати канонічного аналізу для обґрунтування складу індикаторів рівня інформаційної безпеки країни (складено авторкою)

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

2.2 Інтегральне оцінювання інформаційної безпеки національної економіки

Визначений взаємний вплив між показниками інституційної та цифрової спроможності і кібербезпеки, який є статистично значущий та помітний, дозволяє розробити інтегральний індекс інформаційної безпеки національної економіки. Він буде використовуватися в якості показника, який узагальнює, з одного боку, характеристики, властиві системі інформаційної безпеки країни щодо її можливостей попереджувати загрози та динамічно розвиватися у цифровому просторі, та, з іншого боку, характеристики, що уособлюють інституційний розвиток національної економіки країни, який забезпечує її регулювання на державному рівні. Оскільки їх взаємно обумовлений вплив було доведено у підрозділі 2.1, тому вкрай важливо враховувати обидва напрями в процесі розрахунку інтегрального рівня.

Так, базою вхідних даних інтегрального показника інформаційної безпеки національної економіки слугуватимуть індикатори групи цифрової спроможності та кібербезпеки, тобто глобальний індекс кібербезпеки, національний індекс кібербезпеки, рівень розвитку інформаційно-комунікаційних технологій країни, рівень технологічної готовності країни та рівень її цифрового розвитку [86]. Їх застосування дозволить оцінити систему управління інформаційною безпекою держави з боку програмного, технічного та інформаційного її забезпечення, а також рівня протидії зовнішнім та внутрішнім кіберзагрозам.

Для формування показників другої групи було обрано індикатори інституційної спроможності з бази даних Світового банку [257], а саме: оцінювання ефективності уряду, оцінювання якості регуляторів, оцінювання верховенства права, оцінювання контролю корупції, оцінювання політичної стабільності та відсутності насилля і тероризму.

Інформацію було обрано для 159 країн світу за 2018 рік. Кількість країн та період обумовлені наявністю та повнотою даних по кожному з обраних показників у базі даних Світового банку та e-GovernanceAcademyFoundation.

Розрахунок інтегрального індексу інформаційної безпеки національної економіки пропонується здійснювати за наступною методикою.

1 етап. Нормалізація масиву вхідних даних з метою співставлення різних за вимірами показників та їх інтеграції. Методів нормалізації існує чимало, але для першого етапу обрано нелінійну нормалізацію, яка більш ефективно згладжує різні за знаками та значеннями дані, що є характерним для сформованого набору. Цей процес відбуватиметься за формулою (2.3):

$$Z_{ij} = \left(1 + e^{\frac{\overline{y_j} - y_{ij}}{\sigma(y)}}\right)^{-1}, \tag{2.3}$$

де Z_{ij} – нормалізоване значення j-ї складової інтегрального індексу інформаційної безпеки національної економіки в розрізі i-ї країни;

$\overline{y_j}$ – середнє значення *j*-ї складової інтегрального індексу інформаційної безпеки національної економіки в межах досліджуваного переліку країн;

y_{ij} – фактичне значення *j*-ї складової інтегрального індексу інформаційної безпеки національної економіки в розрізі *i*-ї країни;

$\sigma(y_j)$ – середнє квадратичне відхилення *j*-ї складової інтегрального індексу інформаційної безпеки національної економіки в межах досліджуваного переліку країн.

2 етап. Дослідження впливу показників цифрової спроможності та кібербезпеки на кожен з обраних показників інституційної спроможності країни з метою визначення частини варіації інтегрального індексу інформаційної безпеки національної економіки. Для його визначення пропонується на цьому етапі застосувати канонічний аналіз, який краще, ніж регресійний, дозволить визначити значення варіації між множинами змінних для оцінки ступеня впливу однієї множини на іншу.

3 етап. Побудова інтегрального індексу інформаційної безпеки національної економіки на основі використання функції Харрінгтона-Менчера, яка на відміну від інших методів дозволяє вимірювати ефективність будь-якої системи [112, 175].

Крок 3.1. Трансформація нормалізованих значень показників статистичної бази дослідження до безрозмірної шкали бажаності Харрінгтона за допомогою формули (2.4):

$$d_{ij} = \exp(-\exp(-Z_{ij})), \quad (2.4)$$

де Z_{ij} – нормалізоване значення *j*-го показника індексу інформаційної безпеки національної економіки в розрізі *i*-ї країни;

d_{ij} - проміжне значення *j*-го показника індексу інформаційної безпеки національної економіки в розрізі *i*-ї країни, приведене до безрозмірної шкали бажаності Харрінгтона.

Крок 3.2. Проведення візуалізації залежності d_{ij} від фактичних значень в розрізі кожного вхідного показника з метою подальшого вибору типу кривої перетворення Харрінгтона-Менчера.

Крок 3.3. Формалізація перетворення Харрінгтона-Менчера в межах обраного на попередньому кроці залежності $\mathrm{d_{ij}}$ від фактичних значень в розрізі кожного вхідного показника. Тобто на основі отриманих на кроці 3.2 графіків можна отримати криві 6 типів (2.5) – (2.10).

Крива першого типу– S-подібна, зростаюча, симетрична крива, що визначається за формулою (2.5):

$$d_{ij}{}^{*} = \exp\left(-\exp\left(-\left(9\left(\frac{Z_{ij} - \min\limits_{i} Z_{ij}}{\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}}\right)^{1.927} - 2\right)\right)\right), \quad (2.5)$$

де $d_{ij}{}^{*}$ – проміжне значення *j*-го показника індексу інформаційної безпеки національної економіки в розрізі *i*-ої країни, приведене до безрозмірної шкали бажаності Харрінгтона-Менчера;

$\min\limits_{i} Z_{ij}$ – мінімальне значення нормалізованого *j*-го показника інформаційної безпеки національної економіки в розрізі *i*-ї країни;

$\max\limits_{i} Z_{ij}$ – максимальне значення нормалізованого *j*-го показника інформаційної безпеки національної економіки в розрізі *i*-ї країни.

Крива другого типу – S-подібна, зростаюча, асиметрична крива зі швидким початковим ростом, що визначається за формулою (2.6):

$$d_{ij}{}^{*} = \exp\left(-\exp\left(-\left(9\left(\frac{Z_{ij} - \min\limits_{i} Z_{ij}}{\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}}\right)^{k_{II}} - 2\right)\right)\right)$$

$$k_{II} = \frac{\ln\left(2 - lnln\dfrac{1}{d_{ij}{}^{II}}\right)}{\ln\left(y_{ij}^{II} - \min\limits_{i} Z_{ij}\right) - \ln\left(\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}\right)} \quad (2.6)$$

де $d_{ij}{}^{II}, y_{ij}^{II}$ – будь-яка співставна пара в межах однієї країни в межах одного показника.

Крива третього типу – S-подібна, зростаюча, асиметрична крива з повільним початковим ростом, що визначається за формулою (2.7):

$$d_{ij}{}^{*} = 1 - \exp\left(-\exp\left(-\left(9\left(\frac{\max\limits_i Z_{ij} - Z_{ij}}{\max\limits_i Z_{ij} - \min\limits_i Z_{ij}}\right)^{k_{III}} - 2\right)\right)\right)$$

$$k_{III} = \frac{\ln\left(2 - lnln\dfrac{1}{1 - d_{ij}{}^{III}}\right) - ln9}{\ln\left(\max\limits_i Z_{ij} - y_{ij}^{III}\right) - \ln\left(\max\limits_i Z_{ij} - \min\limits_i Z_{ij}\right)} \tag{2.7}$$

де $d_{ij}{}^{III}, y_{ij}^{III}$ – будь-яка співставна пара в межах однієї країни в межах одного показника.

Крива четвертого типу – S-подібна, спадаюча, симетрична крива, що визначається за формулою (2.8):

$$d_{ij}{}^{*} = \exp\left(-\exp\left(-\left(9\left(\frac{\max\limits_i Z_{ij} - Z_{ij}}{\max\limits_i Z_{ij} - \min\limits_i Z_{ij}}\right)^{1.927} - 2\right)\right)\right) \tag{2.8}$$

Крива п’ятого типу – S-подібна, спадаюча, асиметрична крива зі швидким початковим спадом, що визначається за формулою (2.9):

$$d_{ij}{}^{*} = 1 - \exp\left(-\exp\left(-\left(9\left(\frac{\max\limits_i Z_{ij} - Z_{ij}}{\max\limits_i Z_{ij} - \min\limits_i Z_{ij}}\right)^{k_V} - 2\right)\right)\right)$$

$$k_V = \frac{\ln\left(2 - lnln\dfrac{1}{1 - d_{ij}{}^{V}}\right) - ln9}{\ln\left(y_{ij}^{V} - \min\limits_i Z_{ij}\right) - \ln\left(\max\limits_i Z_{ij} - \min\limits_i Z_{ij}\right)} \tag{2.9}$$

де $d_{ij}{}^{V}, y_{ij}^{V}$ – будь-яка співставна пара в межах однієї країни в межах одного показника.

Крива шостого типу – S-подібна, спадаюча, асиметрична крива зі повільним початковим спадом, що визначається за формулою (2.10):

$$d_{ij}{}^{*} = \exp\left(-\exp\left(-\left(9\left(\frac{\max\limits_{i} Z_{ij} - Z_{ij}}{\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}}\right)^{k_{VI}} - 2\right)\right)\right)$$

$$k_{VI} = \frac{\ln\left(2 - lnln\dfrac{1}{1 - d_{ij}{}^{VI}}\right) - ln9}{\ln\left(y_{ij}^{VI} - \min\limits_{i} Z_{ij}\right) - \ln\left(\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}\right)} \tag{2.10}$$

де $d_{ij}{}^{VI}, y_{ij}^{VI}$ – будь-яка співставна пара в межах однієї країни в межах одного показника.

Крок 3.4. Обчислення інтегрального індексу інформаційної безпеки національної економіки на основі використання функції Харрінгтона-Менчера, як середньої геометричної похідних величин від індикаторів цифрової спроможності національної економіки і кібербезпеки та індикаторів інституційної спроможності:

$$IIBNE_i = \sqrt[n+m]{\prod_{j=1}^{n}\left(d_{ij}^{*}\right)^{\frac{w_j}{100}} \cdot \prod_{j=n+1}^{m} d_{ij}^{*}}, \tag{2.11}$$

де $IIBNE_i$ – інтегральний індекс інформаційної безпеки національної економіки для *i*-ї країни;

n – кількість показників групи інституційної спроможності країни;

m – кількість показників групи цифрової спроможності і кібербезпеки;

w_j – ступінь варіації індексу інформаційної безпеки національної економіки під впливом j-го вхідного показника інституційної спроможності країни (визначається на 2-му етапі);

d_{ij}^* - проміжне значення j-го показника індексу інформаційної безпеки національної економіки в розрізі i-ї країни, приведене до безрозмірної шкали бажаності Харрінгтона-Менчера.

4 етап. Здійснення візуалізації результатів розрахунків та проведення якісної інтерпретації індексу інформаційної безпеки національної економіки. Для цього використовуються наступні оцінки інтерпретації, представлені у таблиці 2.2.

Таблиця 2.2 – Кількісна та якісна інтерпретація інтегрального індексу інформаційної безпеки національної економіки

Якісна інтерпретація	Кількісна оцінка
Дуже добре	1,00 – 0,80
Добре	0,80 – 0,63
Задовільно	0,63 – 0,37
Погано	0,37 – 0,20
Дуже погано	0,20 – 0,00

Послідовно для обраних емпіричних даних було реалізовано запропонований підхід до визначення інтегрального показника, який дозволить оцінити рівень інформаційної безпеки національної економіки країни. Так, на першому етапі, застосовуючи формулу (2.3), після проведення нормалізації за допомогою програми «MS Excel» отримано нормалізовані дані для показників інституційної та цифрової спроможності. Результати розрахунків представлені в таблиці Б.1 додатку Б.

На другому етапі з використанням аналітичного пакету «STATISTICA» проведено канонічний аналіз взаємозалежності кожного з показників інституційної спроможності. Результати систематизовано у таблиці 2.3.

Таблиця 2.3 – Результати канонічного аналізу для індикаторів інституційної спроможності

Назва індикатору	Повна надмірність	Канонічний R	Chi^2	p
Оцінка контролю корупції	56,3878	0,7509	128,21	0,0000
Оцінка ефективності уряду	75,6136	0,8696	218,02	0,0000
Оцінка якості регуляторних органів	72,1726	0,8495	197,63	0,0000
Оцінка верховенства права	59,8971	0,7739	141,17	0,0000
Оцінка політичної стабільності та відсутності насилля / тероризму	35,0056	0,5917	66,57	0,0000

Дані стовпчика “Канонічний R” таблиці 2.3 свідчать, що між показниками безпеки та факторами розвитку існує сильний зв'язок, причому для більшості факторів ($R \geq 0,7$), а для “Оцінка політичної стабільності та відсутності насилля / тероризму” зв'язок є значним, оскільки $0,7 > R \geq 0,5$. Його статистичну значимість підтверджує високе значення критерію Пірсона (стовпчик “Chi^2”), рівень значущості якого не перевищує 0,05 ($p = 0,0000$). У стовпчику “Повна надмірність” представлено значення надмірності для факторів опосередкованого впливу, які пояснюються мінливістю показників цифрової спроможності і кібербезпеки. Наприклад, показник “Оцінка ефективності уряду” на 75,6136% пояснюється змінами показників цифрової спроможності і кібербезпеки, тобто їх варіація призводить до зміни ефективності уряду на 75,6136%. Оскільки фактори інституційного розвитку здійснюють вплив на рівень інформаційної безпеки країни опосередковано, то отримані значення мінливості дозволять використати їх у якості вагів впливу даних показників при розрахунку інтегрального показника інформаційної безпеки.

На кроці 3.1 проведено трансформацію нормалізованих значень показників статистичної бази дослідження до безрозмірної шкали бажаності Харрінгтона за допомогою формули (2.4). Результати отриманих даних представлені в таблицях Б.1-Б.2 додатку Б.

На кроці 3.2 для кожної складової інтегрального індексу інформаційної безпеки національної економіки побудовано графік, аналіз форми якого дозволив визначити тип кривої. В результаті отримано 10 графіків, залежності на

яких ідентифіковано тільки за двома типами кривих. Так, крива другого типу характерна для індексу мережевої готовності країни та національного індексу кібербезпеки. Приклад отриманого результату для індексу мережевої готовності країни представлений на рисунку 2.20. Для всіх інших показників було ідентифіковано криву першого типу, приклад якої наведено для оцінки контролю корупції на рисунку 2.21. Для інших показників графіки представлені на рисунках Б.1-Б.8 у додатку Б.

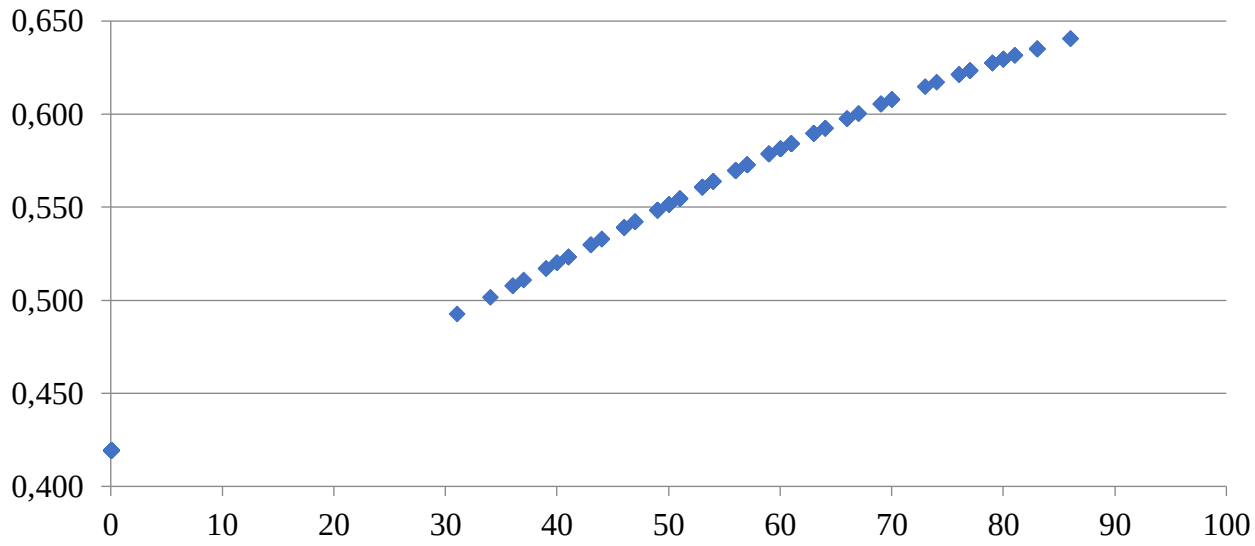


Рисунок 2.20 – Графік кривої другого типу для індикаторі «Індекс мережевої готовності» (складено авторкою)

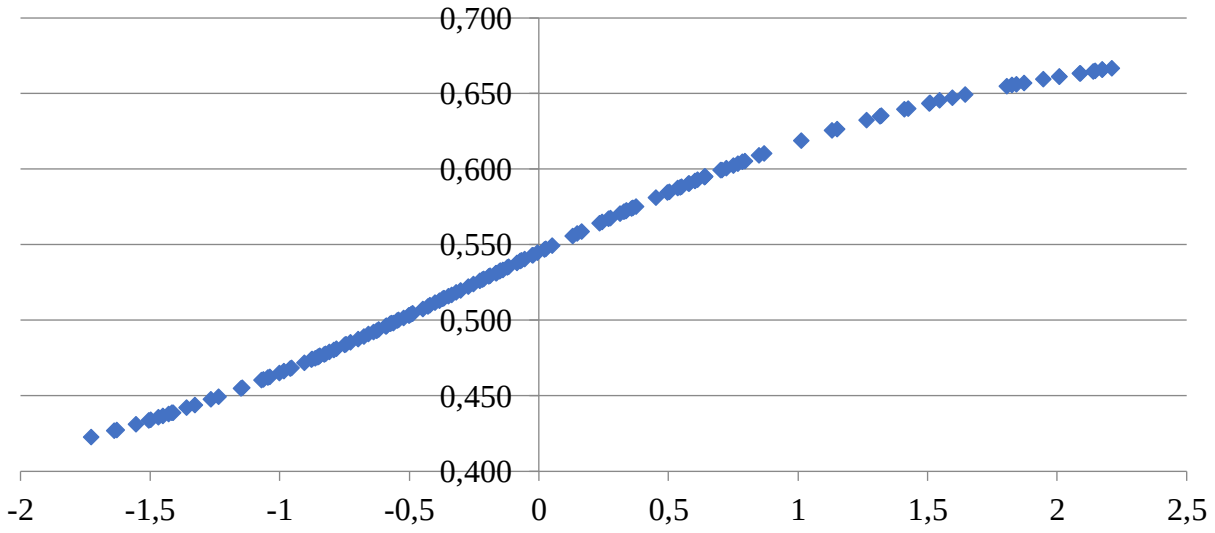


Рисунок 2.21 – Графік кривої першого типу для індикатора «Оцінка контролю корупції» (складено авторкою)

Вибір типу кривої дозволив провести подальшу трансформацію функції Харрінтона-Менчера, яка використовується для визначення інтегрального індексу інформаційної безпеки національної економіки.

За результатами попереднього кроку для показників з кривою першого типу було обрано формулу (2.5) для розрахунку d_{ij}^{*}, а для показників з кривою другого типу – формулу (2.6). Було проведено відповідні розрахунки у «MS Excel», результати яких наведено у таблиці Б.3 додатку Б.

В процесі розрахунку перетворень Харрінгтона-Менчера для кривої другого типу необхідно було визначити ${d_{ij}}^{II}, y_{ij}^{II}$ за формулою (2.6). З цією метою необхідно було узяти дані для співставної країни. Обрано країни, які мають середнє значення відповідного показника, оскільки це дозволило скоротити розрив між країнами із самими високими показниками розвитку та безпеки, та самими низькими. На основі зроблених перетворень розраховано інтегральний індекс інформаційної безпеки національної економіки за формулою (2.11) (див. таблиця Б.3 додатку Б), за результатами чого побудовано карту розподілу країн за отриманим інтегральним індексом інформаційної безпеки (рисунок 2.22).

Як результат, було отримано п’ять груп країн, рівень інституційної спроможності та інформаційної безпеки яких ідентифікується за їх можливістю державного забезпечення інформаційної безпеки національної економіки. Так, до країн, рівень протидії загрозам яких є “дуже добре”, попали 49 країн: Західної, Північної та Південної Європи, США, Канада, Австралія, Японія, Нова Зеландія, Малайзія, Саудівська Аравія, Ізраїль, тощо (рисунок 2.22). Тобто дану групу сформували країни, які в більшості відносяться до розвинутих, мають потужну економіку, високий науково-технічний потенціал та застосовують стратегічні підходи до управління системою інформаційної безпеки на рівні країни. Вони мають найвищі можливості у порівнянні з іншими країнами протистояти кіберзагрозам, інформаційному тероризму, які призводять до зниження стану захищеності національних інтересів країни та особистісних інтересів суспільства. Тому вони мають більші переваги у порівнянні з іншими щодо

швидкості реагування у випадку дестабілізації рівня інформаційної безпеки та мають ресурси на відновлення, що не гальмуватиме їх подальший розвиток.

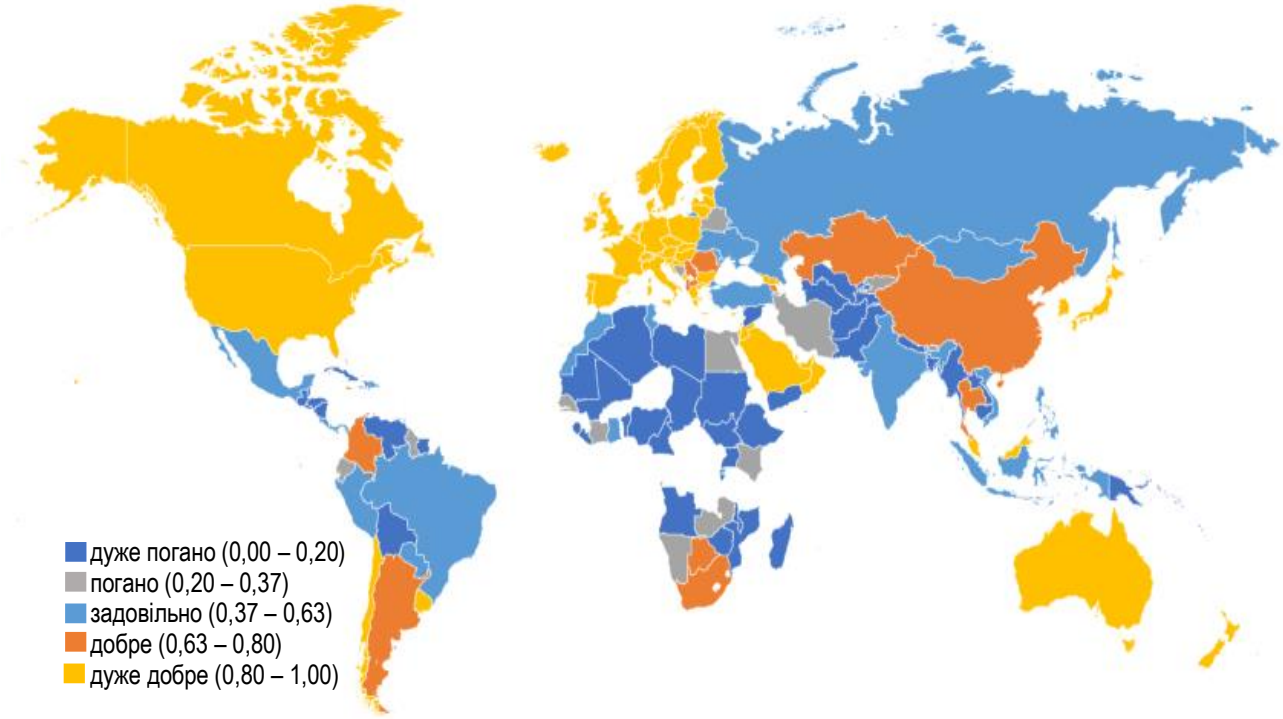


Рисунок 2.22 – Карта розподілу країн за інтегральним індексом інформаційної безпеки національної економіки (складено авторкою)

За результатами розрахунків 14 країн було віднесено до групи, яка має якісну оцінку “добре”. Її сформували ряд нових індустріальних країн – Бразилія, Китай, Таїланд, та ряд країн, які розвиваються, - Албанія, Аргентина, Вірменія, Казахстан, Румунія, Сербія та інші. Реальні показники цифрової спроможності та кібербезпеки цих країн для більшості країн перевищують середні значення по всій генеральній сукупності. Але найбільш характерним для цієї групи є значні відхилення для показників контролю корупції та верховенства права. Тобто країнам цієї групи необхідно змінити підходи до державного регулювання національною системою інформаційної безпеки країни, а саме удосконалити стандарти кібербезпеки, посилити правову відповідальність за кіберінциденти, впровадити стандарти захисту персональних даних користувачів Інтернету та мобільного зв’язку, переформатувати інститути, які відповідають за

інформаційну безпеку в країні. Все це можливо тільки за рахунок удосконалення напрямів державного регулювання національною економікою в частині подолання корупції та внесення відповідних змін до нормативно-правових документів.

Країни, які було віднесено до групи з оцінкою “задовільно”, – це 24 країни, які відносяться до країн, що розвиваються: Азербайджан, Бразилія, Молдова Монголія, Марокко, Перу, Російська Федерація, Туніс, Україна, тощо. Для цієї групи характерно, що рівень розвитку інформаційно-комунікаційних технологій є нижчим за середній рівень, інші показники інформаційної безпеки переважно його перевищують. Що стосується показників інституційної спроможності, то для даної групи їх значення є критичними та для більшості країн є нижчими за середнє значення за вибіркою. Тобто у випадках виникнення ситуацій, пов’язаних із кібертероризмом, країни групи “задовільно” є технічно підготовленими, хоча в цілому рівень їх інформаційно-технологічного розвитку дещо відстає. Але низький рівень забезпечення державного регулювання інформаційної безпеки є тим бар’єром, який впливає на її розвиток та на розвиток економіки країни в цілому. На відміну від попередньої групи країнам групи “задовільно” слід приділити увагу розробленню комплексу стратегічних заходів, які сприятимуть розвитку цифрових та комп’ютерних технологій для сфери інформаційної безпеки. Вони можуть включати й програми щодо підвищення підготовки фахівців в сфері кібербезпеки, внесення змін до політики безпеки, норм законодавства, впровадження технологій з метою прийняття рішення та попередження корупції в різних сферах, створення планів щодо управління кіберкризами, зміни підходів щодо захисту особистих даних, цифрових та комп’ютерних послуг, тощо. Дуже важливо створювати умови, пов’язані не тільки з організацією перерахованих заходів, але й з можливістю створювати перспективні плани з урахуванням останніх досягнень четвертої промислової революції, координувати проекти та стартапи в сфері ІТ на рівні держави, контролювати ефективність даних заходів. Але передусім даним країнам необхідно зосередитися на заходах державного регулювання інформаційної

безпеки, а саме впровадити: зміни до нормативно-правових документів у сфері інформаційної безпеки та захисту інформації, особливо в частині кримінальної відповідальності за кіберзлочини; заходи щодо протидії корупції та зниження рівня насилля та тероризму (особливо це актуально для таких країн, як Україна, Мексика, Бразилія, Азербайджан, тощо); заходи щодо створення спеціальних підрозділів щодо реагування на кіберзлочини.

До групи з оцінкою “погано” увійшли 18 країн – Барбадос, Білорусія, Бутан, Єгипет, Еквадор, Іран, Кенія, Киргизстан, Намібія, Замбія та інші, а до групи “дуже погано” – 54 країни: Афганістан, Камерун, Камбоджа, Лівія, Мозамбік, Нікарагуа, Нігерія, Судан, Таджикистан, Туркменістан, тощо. Для країн цих груп характерні низькі або дуже низькі показники інституційної та цифрової спроможності та кібербезпеки. Відповідно, ризик існування загрози інформаційної безпеки національної економіки для цих країн є критичним або значно критичним, тобто вони є більш вразливими, а їх наявні економічні ресурси не достатні для подолання наслідків кіберкризи, інформаційного тероризму або інформаційної війни. З іншого боку, ризик того, що вони опиняться у якості об’єктів кібертерористів, є невеликий у порівнянні з країнами групи “дуже добре”, “добре” та “задовільно”. Можна припустити, що підвищення рівня соціального та економічного розвитку таких країн значно впливатиме на заходи щодо підсилення рівня інформаційної безпеки країни. Саме тому, завдання розвитку всіх сфер діяльності країни повинно стати однією із головних стратегій для покращення стану інформаційної безпеки.

Результати оцінки рівня інформаційної безпеки національної економіки на основі запропонованого індексу можна вважати адекватними, оскільки отримані групи країн містять країни, близькі за рівнем добробуту та економічного розвитку, що було продемонстровано в процесі аналізу підсумків. Також у групах відсутні поєднання кардинально протилежних за ступенем розвитку та рівнем інформаційної безпеки країн.

Запропонована оцінка рівня інформаційної безпеки національної економіки країни враховує не тільки окремі сфери, такі як рівень кібербезпеки,

розвитку інформаційних технологій, ступінь цифровізації та інформатизації, але й рівень державного регулювання з позиції забезпечення економічної безпеки. Розрахунки індексу дозволили сформувати п’ять груп країн та провести їх якісну ідентифікацію та візуалізацію у вигляді карти країн, розподілених за групами. Групу “дуже добре” сформували в більшості випадків потужні в економічному плані країни з високим рівнем інформаційної безпеки. Рівень їх протидії загрозам є найвищим, що свідчить також про значні можливості даних країн долати наслідки інформаційних війн та загроз. До групи “добре” увійшли нові індустріальні країни та ті, що розвиваються. Їх рівень інформаційної безпеки національної економіки говорить про те, що цим країнам слід приділити увагу окремим показникам її розвитку та сприяти вирішенню ряду проблем, пов’язаних із стандартизацією, правовими аспектами, організацією інститутів з питань інформаційної безпеки, тощо. Країни, які розвиваються, але мають посередні показники економічного розвитку та рівень інформаційної безпеки сформували групу “задовільно”, куди увійшла й Україна. Їх рівень інформаційної безпеки свідчить про те, що наслідки інформаційних загроз будуть відчутними для економіки, соціальної та політичної сфер, але завдяки критичним аспектам державного регулювання. Тому цим країнам слід переформатувати не тільки стратегію управління, але й розробити програми для залучення інвестицій у розвиток та застосування сучасних програмних та технологічних рішень у сферу інформаційної безпеки. Країни із низькими показниками соціо-економічного розвитку та низьким рівнем безпеки, а також країни, які є найменш розвинутими, ідентифіковано як “погано” та “дуже погано”. В першу чергу цим країнам слід вирішувати завдання щодо покращення рівня економічного розвитку, що стимулюватиме також підвищення рівня ефективності системи інформаційної безпеки національної економіки.

Отримані результати можна використовувати для подальших прогнозів щодо можливостей країни забезпечувати інформаційну безпеку як драйвер розвитку національної економіки. Значення індексу сприятимуть розробці не тільки стратегії управління інформаційної безпеки, але можуть бути враховані

при формуванні стратегічних планів розвитку країни. Запропоновану методологію в узагальненому вигляді представлено на рисунку 2.23.

Етап 1: 1) формування бази даних для розрахунку інтегрального показника: 5 індикаторів цифрової спроможності НЕ та кібербезпеки (ЦСіКБ): індекс розвитку інформаційних і комунікаційних технологій (ІР ІКТ); індекс мережевої готовності (ІМГ); глобальний індекс кібербезпеки (ГІК); національний індекс кібербезпеки (НІК); рівень цифрового розвитку (РЦР); 5 індикаторів інституційної спроможності (ІС): оцінювання контролю корупції (ОКК); оцінювання ефективності уряду (ОЕУ); оцінювання якості регуляторів (ОЯР); оцінювання верховенства права (ОВП); політична стабільність і відсутність насилля / тероризму (ПС); 2) здійснення нормалізації даних із використанням нелінійної нормалізації.

Етап 2: 1) трансформація нормалізованих значень показників до безрозмірної шкали бажаності Харрінгтона; 2) вибір типу кривої перетворення Харрінгтона – Менчера та його формалізація залежно від отриманого типу кривої.

За кривою 1-го типу:
ОКК, ОЕУ, ОЯР, ОВП, ПС, ІР ІКТ, ГІК, РЦР

$$d_{ij}^{\ *} = \exp\left(-\exp\left(-\left(9\left(\frac{z_{ij}-\min\limits_i z_{ij}}{\max\limits_i z_{ij}-\min\limits_i z_{ij}}\right)^{1.927}-2\right)\right)\right),$$

де $d_{ij}^{\ *}$ – проміжне значення *j*-го показника для *i*-ї країни; $\min\limits_i Z_{ij}$ та $\max\limits_i Z_{ij}$ – відповідно мінімальне та максимальне значення нормалізованого *j*-го показника, приведеного до безрозмірної шкали бажаності Харрінгтона – Менчера, для *i*-ї країни (Z_{ij})

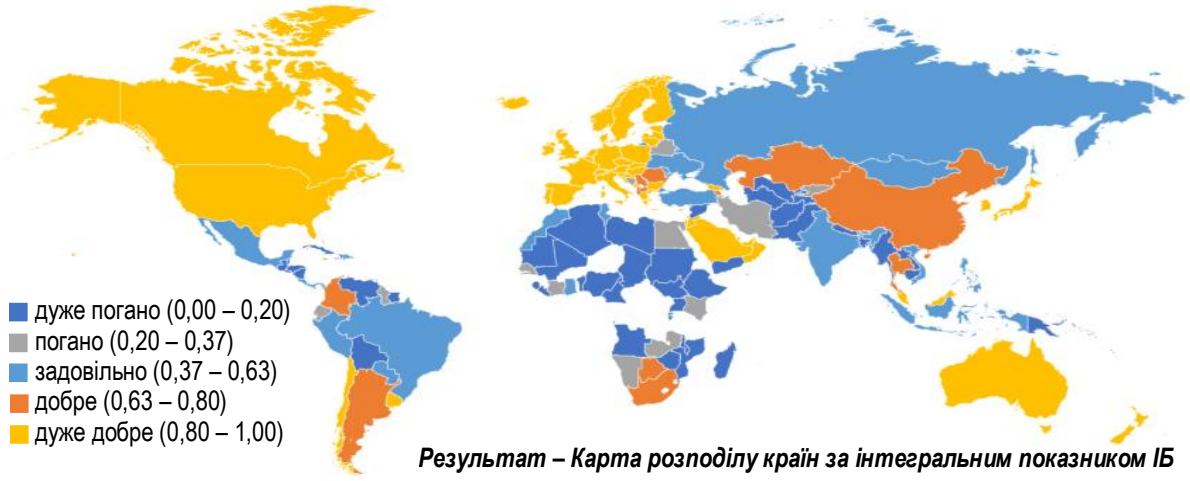
За кривою 2-го типу:
НІК, ІМГ

$$d_{ij}^{\ *} = \exp\left(-\exp\left(-\left(9\left(\frac{z_{ij}-\min\limits_i z_{ij}}{\max\limits_i z_{ij}-\min\limits_i z_{ij}}\right)^{k_{II}}-2\right)\right)\right),$$

де $k_{II} = \frac{\ln\left(2-ln ln\frac{1}{d_{ij}^{\ II}}\right)}{\ln\left(y_{ij}^{II}-\min\limits_i Z_{ij}\right)-\ln\left(\max\limits_i Z_{ij}-\min\limits_i Z_{ij}\right)}$; $d_{ij}^{\ II}, y_{ij}^{II}$ – будь-яка зіставна пара *j*-го показника для *i*-ї країни

Етап 3: обчислення інтегрального індексу ІБ країни.

$IIBNE_i = \sqrt[n+m]{\prod_{j=1}^{n}\left(d_{ij}^{*}\right)^{\frac{w_j}{100}} \cdot \prod_{j=n+1}^{m} d_{ij}^{*}}$, де $IIBNE_i$ – інтегральний індекс ІБ НЕ для *i*-ї країни; *n* – кількість індикаторів ІБ НЕ країни; *m* – кількість показників ЦСіКБ; w_j – ступінь варіації індексу ІБ НЕ під впливом *j*-го вхідного показника розвитку країни, визначених із результатів канонічного аналізу



Результат – Карта розподілу країн за інтегральним показником ІБ

Рисунок 2.23 – Методологія формування та результати оцінювання інтегрального індексу інформаційної безпеки (ІБ) національної економіки (НЕ) (складено авторкою)

2.3 Оцінювання ефективності системи забезпечення інформаційної безпеки національної економіки

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

В залежності від мети аналізу у науковій літературі та на практиці застосовують різні підходи. Традиційним вважається класична модель Дюпона «Рентабельність капіталу», яка передбачає використання двох груп показників: перша – для порівняння результатів діяльності з витратами; друга – для визначення ефективності використання окремих видів ресурсів [343, с. 454]. Для розрізнення рентабельних процесів від нерентабельних використовується процесно-орієнтований аналіз рентабельності (Activity - Based Profitability Analysis, ABPA), який було запропоновано М. Мейером та В. Маршалом [326]. Для комплексної оцінки суб’єктів господарювання, як правило, використовуються фінансові та нефінансові показники, які дозволяють збалансовано підійти до визначення ефективності діяльності. Такий підхід має назву «Управління результатами» (Performance Management) та був розроблений Р. Капланом та Д. Нортоном [337]. Для оцінки об’єктів з позиції потенційної можливості здійснення інвестицій традиційно застосовують методику аналізу, засновану на аналізі грошових потоків, яка передбачає розрахунок чистого

грошового потоку (NCF -net cash flow), внутрішньої норми прибутковості (IRR – Internal Rate Of Return), модифікованої внутрішньої норми прибутковості (MIRR – Modified Internal Rate Of Return), індексу рентабельності (PI – profitability index), методу повернення на вкладені інвестиції (ROI – Return On Investment), чистої поточної вартості (NPV – Net Present Value) [275].

Основними недоліками перелічених методів є те, що їх використання доцільно для аналізу ефективності господарської діяльності та передбачає розрахунок різних коефіцієнтів, за результатами яких робиться висновок. У випадку оцінювання ефективності системи забезпечення інформаційної безпеки національної економіки доцільно використання саме математичних методів, які дозволяють проводити оцінювання параметрів відносно значень, які є найкращими у групі аналізованих об’єктів. Саме тому для проведення дослідження було використано DEA-метод (Data Envelopment Analysis), який було запропоновано А. Чарнсом, В. Купером та Е. Родесом у 1978 році [355]. Цей інструмент не залежить від мети аналізу та використовується у багатьох галузях для оцінки ефективності складних систем, що відбувається шляхом рішення оптимізаційної задачі лінійного програмування. Її мета – це визначення ефективності системи на основі співвідношення її виходів та входів, при цьому необхідно врахувати максимальний вихід ресурсів при заданому рівні входів, або мінімальний рівень ресурсів при заданому рівні виходів.

Для проведення дослідження було обрано вхідні дані, які було відібрано у підрозділах 2.1 та 2.2 на основі канонічного аналізу та розрахунку інтегрального показника інформаційної безпеки національної економіки, а саме: глобальний індекс кібербезпеки, національний індекс кібербезпеки, індекс розвитку інформаційно-комунікаційних технологій, індекс мережевої готовності країни, рівень цифрового розвитку, оцінка ефективності уряду, оцінка верховенства права, оцінка контролю корупції, оцінка якості регуляторів, політична стабільність і відсутність насилля / тероризму. Дані показники сформували базу вхідних даних для 159 країн світу за 2018 рік. У якості вихідного параметру, який є індикатором узагальненого рівня ефективності, виступатиме запропонований у

підрозділі 2.2 інтегральний індекс інформаційної безпеки національної економіки.

Для того, щоб дані можна було піддавати подальшому аналізу, необхідно було провести їх нормалізацію, оскільки кожен з відібраних показників має різні виміри та значення. З цією метою у підрозділі 2.2 було проведено нормалізацію вхідних даних на основі нелінійної нормалізації за формулою (2.3).

Оскільки DEA-метод є ефективним для даних, які мають близькі характеристики, то доцільно додатково провести кластерний аналіз, який дозволить сформувати кластери країн з урахуванням не тільки кінцевого інтегрального значення, а й з урахуванням всіх його складових. З цією метою використаємо аналітичну платформу «Deductor Academic» [345], яка є потужним програмним інструментом для здійснення математичного моделювання та просунутої аналітики, а саме реалізації інструментів Data Mining.

Перед початком здійснення кластерного аналізу необхідно здійснити перевірку вхідних даних на якість, виявлення викидів, дублікатів та протиріч. В результаті аналізу якості даних було виявлено викиди за індикатором оцінки політичної стабільності і відсутності насилля / тероризму, що свідчить про необхідність коректування даних за цим показником. В цілому отриманий показник якості для всіх змінних знаходиться у межах від 0,8299 до 0,9771, що говорить о високій якості початкового набору даних. Перевірка даних на наявність дублікатів та протиріч виявила, що вони відсутні у наборі даних. В результаті проведених перевірок було здійснено коректування тільки даних індикатора політична стабільність і відсутність насилля / тероризму, для чого було обрано метод обмеження для критичних значень викидів.

Після підготовки даних проведено аналіз рівня інформаційної безпеки національної економіки країн, що здійснювалося із використанням самоорганізованих карт Кохонена. Карти Кохонена представляють собою вид нейронної мережі з некерованим навчанням, яка проектує дані з багатовимірного простору у двовимірний. Даний інструментарій було розроблено фінським вченим Теуво Кохоненом у 1982 році [144].

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

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

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

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

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

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

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

7) при порівнянні результатів автоматичного визначення кількості кластерів та ручного визначення врешті-решт було обрано автоматичне визначення з рівнем значущості 0,05%. Кількість кластерів при ручному режимі виставлялося рівним 5, бо саме стільки кластерів було отримано при ручній перевірці з використанням методу k-means. Але результати автоматичного визначення виявилися кращими.

Після виконання процедур алгоритму побудови карт Кохонена отримано 7 кластерів та для кожного з відібраних показників побудовано карту. Результати представлені на рисунку 2.24.

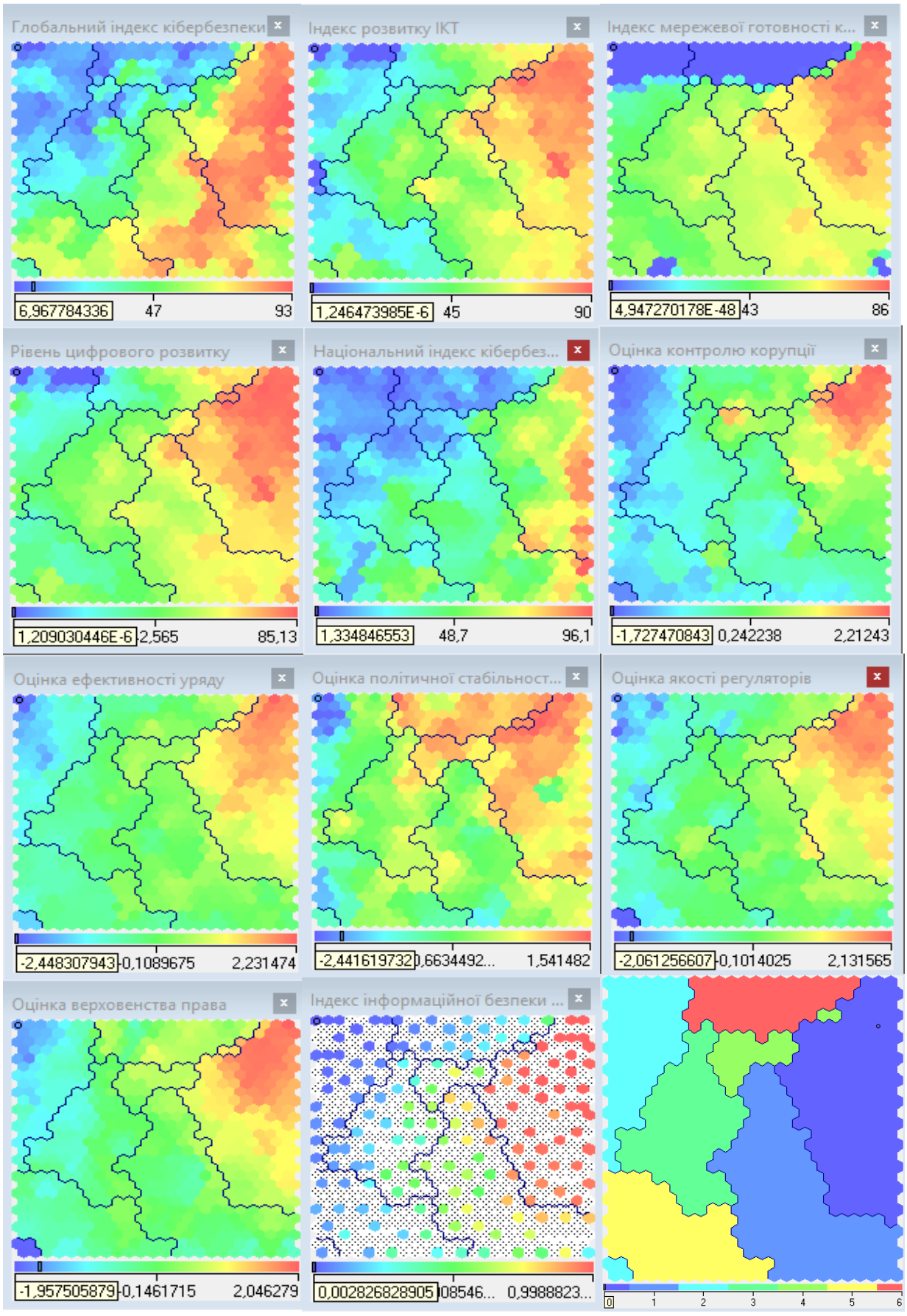


Рисунок 2.24 – Карти Кохонена для індексу інформаційної безпеки та його складових (складено авторкою)

Також було виведено зв’язки кластерів (рисунок В.1 додатку В) та діаграма розсіювання кластерів (рисунок В.2 додатку В), яка показала високий рівень концентрації змодельованих значень у межах статистичної значущості. Кінцевий результат матриць помилок квантування, щільності попадання та відстаней, які характеризують якість результатів кластерного аналізу, представлено на рисунку 2.25. В процесі аналізу даних карт, було виявлено тільки 1 країну, помилка квантування для яких перевищує 10%, що є дуже високим показником якості кластеризації.

а) Матриця помилок квантування

б) Матриця щільності попадання

в) Матриця відстаней

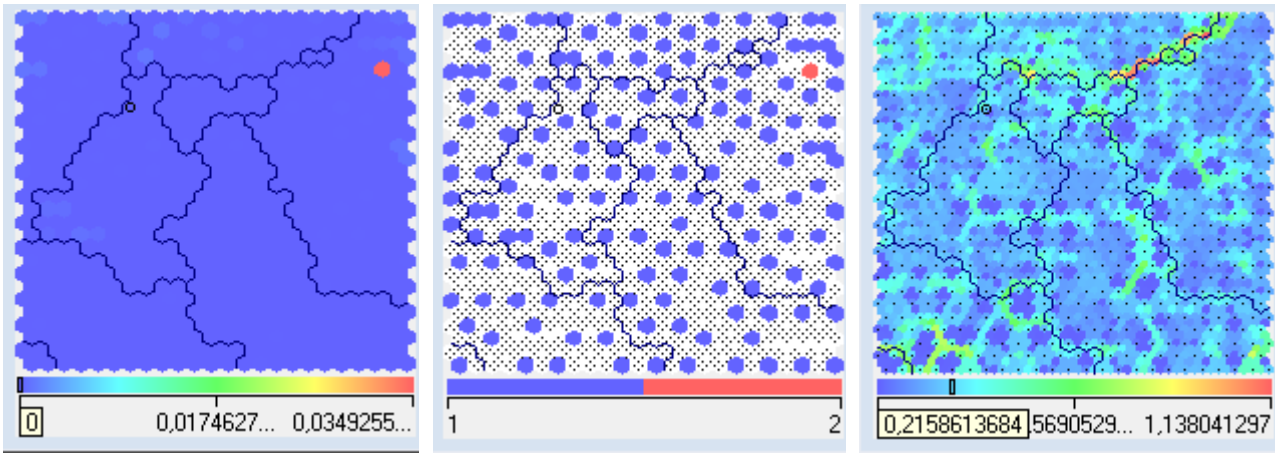


Рисунок 2.25 – Матриці помилок квантування, щільності попадання, відстаней (складено авторкою)

Так, до 0-го кластеру увійшли 42 країни: Австралія, Австрія, Бельгія, Великобританія, Данія, Естонія, Ізраїль, Ісландія, Ірландія, Канада, Люксембург, Нідерланди, Німеччина, Нова Зеландія, Норвегія, Сінгапур, США, Фінляндія, Франція, Швеція, Швейцарія та інші. Даний кластер сформували розвинуті країни з потужним економічним потенціалом та високим рівнем інформаційної безпеки (див. рис. 2.24 та табл. 2.4). Тобто, за умови виникнення різного роду загроз інформаційній безпеці вони зможуть з найменшими втратами подолати наслідки інформаційної кризи. Для країн цього кластеру характерний високий рівень безпеки, який свідчить про те, що для її забезпечення застосовуються

сучасні комп'ютерні технології та програмні засоби, які дозволяють швидко попереджати загрози. Також високий рівень їх економічного розвитку сприятиме формуванню потужного економічного потенціалу для забезпечення національної інформаційної безпеки.

Таблиця 2.4 – Середні значення показників у відповідності із профілем кластера

Назва індикатору інтегрального індексу інформаційної безпеки	Середні значення індикаторів, що відповідають певному кластеру (в дужках зазначено кількість країн у кластері)						
	0 (42)	1 (31)	2 (24)	3 (21)	4 (6)	5 (17)	6 (18)
Індекс розвитку інформаційно-комунікаційних технологій	77,74	60,29	17,88	40,57	47,33	29,71	45,33
Індекс мережевої готовності країни	74,29	58,16	21,5	51,62	55,23	45,24	0,00
Глобальний індекс кібербезпеки	80,26	67,52	15,04	27,14	26,33	58,06	18,00
Національний індекс кібербезпеки	68,58	45,79	12,07	25,05	24,03	36,67	12,19
Рівень цифрового розвитку	75,95	60,41	24,67	46,03	51,47	38,93	45,37
Оцінка контролю корупції	1,21	-0,28	-1,20	-0,59	0,64	-0,67	0,38
Оцінка ефективності уряду	1,28	0,05	-1,35	-0,41	0,36	-0,52	-0,04
Оцінка якості регуляторів	1,30	0,07	-1,24	-0,34	0,11	-0,57	-0,18
Оцінка верховенства права	1,26	-0,18	-1,30	-0,54	0,28	-0,54	0,28
Політична стабільність і відсутність насилля / тероризму	0,77	-0,34	-1,29	-0,16	0,73	-0,90	0,82

Кластер 1 сформувала 31 країна: Албанія, Аргентина, Вірменія, Азербайджан, Білорусь, Бразилія, Китай, Колумбія, Грузія, Греція, Казахстан, Молдова, Російська Федерація, Україна та інші. Частину країн даного кластеру представляють колишні республіки Радянського Союзу, а також ті, які пережили своє становлення через минулі військові події. На даний момент їх усіх можна віднести до групи країн, що розвиваються, але на сьогодні вони мають ряд проблем в економічній, соціальній та політичній сфері. Це також підтверджується низькими значеннями їх показників інституційної спроможності у порівнянні із країнами 0-го кластеру (див. рис. 2.24 та табл. 2.4). Отримані значення показників їх інформаційної безпеки свідчать про середній

рівень, хоча для розвитку сфери безпеки є потреба у залученні коштів для забезпечення змін не тільки на рівні стратегії інформаційної безпеки, але й на рівні її окремих складових – рівня технологічного розвитку, впровадження нових комп'ютерних програм, зміни стандартів, реформування законодавства, тощо.

До 2-го кластеру увійшли 24 країни, які відносяться до групи найменш розвинутих країн, що характеризуються дуже низькими показниками розвитку економіки, соціальної та політичної сфери, а також інституційної спроможності та кібербезпеки (див. рис. 2.24 та табл. 2.4). Більшість країн даного кластеру – це країни Африки та Близького Сходу, де тривають озброєні конфлікти. Для таких країн першочерговим є подолання конфліктів у суспільстві та розвиток економіки. Для підвищення рівня їх інформаційної безпеки їм необхідно долучатися до програм та стартапів, які сприятимуть припливу інвестицій та зміни програмно-технічної інфраструктури на мікро-рівні, а потім й на рівні держави.

До 3-го кластеру увійшла 21 країна: Алжир, Болівія, Камбоджа, Домініканська республіка, Еквадор, Гана, Гватемала, Гондурас, Киргизстан, Непал, Панама, Перу, Сенегал, Тринідад і Тобаго та інші. Даний кластер сформували країни, які розвиваються, але мають низькі показники розвитку та низький рівень інформаційної безпеки (див. рис. 2.24 та табл. 2.4). Головними проблемами цього кластеру є передусім вирішення питань, пов'язаних із економічним розвитком, але ці країни мають відповідний потенціал для розвитку й інформаційної безпеки. Про це свідчить їх достатній рівень розвитку інформаційних технологій, цифровізації різних сфер та технологічної готовності.

4-й кластер сформували тільки 6 країн: Бутан, Ботсвана, Коста Рика, Ямайка, Намібія та Сейшели. Характерними особливостями для них є позитивні значення групи показників інституційної спроможності та досить різні варіанти розвитку складових інформаційної безпеки (див. рис. 2.24 та табл. 2.4), а саме: індекс мережевої готовності країни та рівень цифрового розвитку мають середні значення, інші показники є досить низькими. Для даної групи є характерним те, що країни мають потенціал для регулювання інформаційної безпеки

національної економіки, але система кібербезпеки має ряд суттєвих проблем, які за умови підтримки уряду можуть бути вирішеними.

До 5-го кластеру увійшли 17 країн: Бангладеш, Бенін, Камерун, Єгипет, Ефіопія, Індія, Іран, Кенія, Нігерія, Пакистан та інші. Тобто сюди включено ті країни, які мають значення показників інституційної спроможності нижчими, ніж для 3-го кластеру, та показниками цифрової спроможності і кібербезпеки, які є нижче середнього рівня (див. рис. 2.24 та табл. 2.4). Даний кластер сформовано країнами, які мають низькі показники економічного добробуту в цілому та мають проблеми соціального та політичного характеру. Їм досить складно долати інформаційні кризи, оскільки ряд цих країн знаходяться в зоні діючих воєнних конфліктів. Проблемами інформаційної безпеки країн даного кластеру можуть бути ті, які пов'язані із правовими аспектами в даній сфері, рівнем організації освіти, недостатнім рівнем інвестування у новітні інформаційні технології, тощо.

До 6-го кластеру увійшли 18 країн: Багами, Барбадос, Беліз, Бруней, Куба, Домініка, Кірібаті, Самоа, Суринам та інші. Більшість країн даного кластеру є острівними, основний вид забезпечення діяльності яких є туризм. Також для них є характерним відсутність значення індексу мережевої готовності. Даний факт було враховано при побудові початкового набору даних. Їх виключення давало значне зміщення в результатах розрахунків, тому було прийнято рішення врахувати їх у генеральній сукупності. Також для цього кластеру є характерним дуже низькі значення показників кібербезпеки та значення нижче середнього рівня показників цифрової спроможності (див. рис. 2.24 та табл. 2.4). Це свідчить про те, що ці країни знаходяться на стадії свого активного розвитку у напрямку створення ІТ-інфраструктури, оскільки вони мають проблему віддаленості від материків. Але що стосується показників інституційної спроможності, то для них характерним є відсутність насилля та тероризму, помірний рівень боротьби із корупцією, а також позитивне значення оцінки верховенства права. Тобто можна зробити висновок, що головною проблемою даного кластеру є низький рівень технологічної готовності країни до забезпечення надійної системи інформаційної безпеки.

Використання DEA-методу дозволить визначити ефективність рівня системи інформаційної безпеки країни протидіяти загрозам з урахуванням потенціалу країни, а саме можливостей державного регулювання та управління процесів забезпечення інформаційної безпеки. Ефективність буде досягатися тоді, коли рівень протидії загрозам для окремої країни не можливо збільшити, при цьому залишивши рівень розвитку та безпеки країни на тому самому рівні. Також це можливо у випадку, коли зменшення рівня розвитку та безпеки країни призводить до змін рівня протидії інформаційним загрозам. Виходячи з вище сказаного, можна сформувати початкову DEA-модель [355], яку буде використано для проведення оцінки ефективності рівня інформаційної безпеки країни за формулою (2.12):

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

$$\begin{cases} \dfrac{\sum_{p=1}^{z} u_{ps} y_{pj}}{\sum_{i=1}^{m} v_{is} x_i\, j} \le 1, \\ s, j = \overline{1, n}, \\ u_p, v_i \ge 0, \\ y_{p,} x_i \ge 0. \end{cases} \qquad (2.12)$$

де θ – рівень ефективності системи інформаційної безпеки для конкретної країни, визначений як коефіцієнт між зваженою сумою виходів та входів;

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

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

y_p – p-та характеристика умовних виходів, тобто значень індексу інформаційної безпеки національної економіки для кожної країни;

x_i – i-та характеристика умовних входів, тобто значень показників інформаційної безпеки та показників розвитку країни.

Обмеження (2.12) говорять про те, що відношення виходу до входу не може перевищувати 1 для кожної θ. Тому представлену дробову задачу слід перетворити на лінійну, що значно спрощує її подальше використання. Відповідно до цього, розрізняють два типи DEA-моделі – CCR (Charnes A., Cooper W. and Rhodes E.), яку було запропоновано Чарнсом А., Купером У. та Родесом Е. [355] у 1978 році, та BCC (Banker R., Charnes A. and Cooper W.), яку було розроблено на основі CCR-моделі у 1984 році Банкером Р., Чарнсом А. та Купером У. [17]. Кожна з цих моделей (2.13) – (2.16) орієнтована на вхід (ресурси) та вихід (результуючі показники):

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

$$\begin{cases} \sum_{i=1}^{m} v_{is} x_{is} = 1 \\ \sum_{p=1}^{z} u_{ps} y_{pj} - \sum_{i=1}^{m} v_{is} x_{ij} \le 0 \\ u_p, v_i \ge \gamma \end{cases} \tag{2.13}$$

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

$$\begin{cases} \sum_{i=1}^{m} v_{is} x_{is} = 1 \\ \sum_{p=1}^{z} u_{ps} y_{pj} + k_s \le \sum_{i=1}^{m} v_{is} x_{ij} \\ u_p, v_i \ge \gamma \\ k_s - \ unconstrained \end{cases} \tag{2.14}$$

$$\min_{\alpha,\beta,k} \theta_s = \sum_{i=1}^{m} \beta_i x_{is} - k_s \tag{2.15}$$

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

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

$$\begin{cases} \sum_{p=1}^{z} \alpha_p y_{ps} = 1 \\ \sum_{i=1}^{m} \beta_i x_{ij} - \sum_{p=1}^{z} \alpha_p y_{pj} \geq 0 \\ \alpha_p, \beta_i \geq \gamma \end{cases} \quad (2.16)$$

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

Моделі CCR (2.13) та BCC (2.14) є Input-oriented моделями, тобто направлені на оцінку ефективності розподілу показників інституційного розвитку країни та їх інформаційної безпеки, що сприяє виявленню структурної неефективності заданих індексів. Моделі CCR (2.16) та BCC (2.15) є Output-oriented, тобто дозволяють здійснити оцінку ефективності системи інформаційної безпеки країни шляхом визначення максимальних значень індексу інформаційної безпеки національної економіки за умови заданих значень показників інституційної та цифрової спроможності і кібербезпеки.

DEA-аналіз було проведено у аналітичному пакеті “Frontier Analyst”, який дозволяє здійснювати розрахунки за моделями CCR та BCC [92]. Оскільки було використано демо-версію, то для дослідження в кожному кластері країн було обрано 12 представників, для яких проводився Data Envelopment Analysis. Мінімальне значення вагів у програмі було встановлено на основі результатів проведеного методу головних компонент за допомогою аналітичної платформи

“STATISTICA”, що дозволило визначити частки їх значень у загальній сукупності. Так, для глобального індексу кібербезпеки визначено вагу, що дорівнює 8,28%, індексу розвитку ІКТ – 11,05%, індексу мережевої готовності – 7,32%, національного індексу кібербезпеки – 8,79%, рівня цифрового розвитку – 11,42%, оцінювання контролю корупції – 10,52%, оцінювання ефективності уряду – 12,62%, оцінювання політичної стабільності та відсутності тероризму – 6,43%, оцінювання якості регуляторів – 12,12%, оцінювання верховенства права – 11,44%. Максимальне значення вагів було встановлено на рівні 100%.

Так, результати оцінок отриманої ефективності за моделями CCR та BCC для країн 1-го кластеру представлено на рисунках 2.26-2.29. Якщо порівняти результати отриманих моделей (рисунки 2.26-2.29), то можна побачити, що модель CCR є більш обмежувальною ніж BCC. Це пов’язано із тим, що вона базується на постійності віддачі від масштабу, а також дає можливість масштабувати неефективні одиниці вибірки. BCC-модель базується на змінній віддачі від масштабу та дозволяє оцінити технічну ефективність. Така зміна її вхідних параметрів може призводити до непропорційної зміни вихідних, що дозволяє оцінювати більшість об’єктів як ефективні. Саме такий результат й було отримано в даному дослідженні.

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Georgia	100,0%	✓	
Bulgaria	100,0%	✓	
China	97,2%		
Romania	96,8%		
Armenia	95,1%		
Kazakhstan	88,6%		
Brazil	83,5%		
Moldova	78,2%		
Azerbaijan	74,7%		
Russian Federation	67,2%		
Ukraine	63,7%		
Belarus	42,5%		

Рисунок 2.26 – Input-oriented CCR model (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficien	Conditi
Azerbaijan	100,0%	✓	
Armenia	100,0%	✓	
Brazil	100,0%	✓	
Bulgaria	100,0%	✓	
China	100,0%	✓	
Georgia	100,0%	✓	
Belarus	100,0%	✓	
Ukraine	100,0%	✓	
Romania	98,8%		
Moldova	98,1%		
Kazakhstan	94,0%		
Russian Federation	93,9%		

Рисунок 2.27 – Input-oriented BCC model (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Bulgaria	100,0%	✓	
Georgia	100,0%	✓	
China	97,2%		
Romania	96,8%		
Armenia	95,1%		
Kazakhstan	88,6%		
Brazil	83,5%		
Moldova	78,2%		
Azerbaijan	74,7%		
Russian Federation	67,2%		
Ukraine	63,7%		
Belarus	42,5%		

Рисунок 2.28 – Output-oriented CCR model (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficien	Conditi
Ukraine	100,0%	✓	
Armenia	100,0%	✓	
Belarus	100,0%	✓	
Brazil	100,0%	✓	
Bulgaria	100,0%	✓	
China	100,0%	✓	
Georgia	100,0%	✓	
Azerbaijan	100,0%	✓	
Romania	98,4%		
Moldova	92,5%		
Kazakhstan	91,5%		
Russian Federation	80,6%		

Рисунок 2.29 – Output-oriented BCC model (складено авторкою)

Тобто CCR-модель дозволила виділити тільки 2 країни 1-го кластеру (Болгарію та Грузію), які мають ефективність для входів та виходів рівною 100%. Відповідно, за BCC-моделлю було отримано 8 країн з ефективністю входів та виходів 100% – Азербайджан, Вірменія, Бразилія, Болгарія, Китай, Грузія, Білорусь та Україна. А такі країни, як Румунія, Молдова, Казахстан та Російська Федерація, за результатами BCC-моделі не мають змоги досягти 100%-го рівня ефективності системи інформаційної безпеки. За результатами моделі CCR даний перелік країн є більшим. Оскільки BCC-модель завищує результати, то для подальшого дослідження використовуємо тільки результати CCR-моделі. Також виявлено, що оцінки ефективності для Output-oriented та Input-oriented CCR-моделей є однаковими. Це свідчить про той факт, що у разі забезпечення максимального рівня інтегрального показника інформаційної безпеки, змін в ефективності по відношенню до інших країн у кластері не відбудеться. Але це можливо тільки у разі одночасних зрушень для всіх країн кластеру, що на практиці не є реалізованим.

Що стосується країн інших кластерів, то результати розрахунків представлені у додатку Г, а узагальнена оцінка ефективності їх системи інформаційної безпеки – у таблиці 2.5, де містяться розрахунки за Output-oriented та Input-oriented CCR-моделями.

Таблиця 2.5 – Ефективність системи інформаційної безпеки національної економіки країн за Output-oriented та Input-oriented CCR-моделями

Країна	Виходи максимі-зовані, %	Входи мінімі-зовані, %	Країна	Виходи максимі-зовані, %	Входи мінімі-зовані, %
0-й кластер			3-й кластер		
Кіпр	100,0	100,0	Камбоджа	28,3	28,3
Польща	100,0	100,0	Малаві	25,3	25,3
Чехія	94,8	94,8	4-й кластер		
Іспанія	94,6	94,6	Ботсвана	100,0	100,0
Португалія	94,6	94,6	Ямайка	95,0	95,0
Мальта	91,8	91,8	Сейшели	79,5	79,5
США	87,0	87,0	Коста Ріка	72,8	72,8
Німеччина	85,5	85,5	Намібія	54,2	54,2
Нова Зеландія	85,4	85,4	Бутан	53,6	53,6
Фінляндія	83,7	83,7	5-й кластер		

Продовження таблиці 2.5

Країна	Виходи максимізовані, %	Входи мінімізовані, %	Країна	Виходи максимізовані, %	Входи мінімізовані, %
Нідерланди	83,4	83,4	Індія	100,0	100,0
Сінгапур	82,1	82,1	Парагвай	100,0	100,0
2-й кластер			Руанда	100,0	100,0
Венесуела	100,0	100,0	Єгипет	96,8	96,8
Нікарагуа	87,6	87,6	Іран	93,1	93,1
М'янма	84,2	84,2	Кот-д'Івуар	78,0	78,0
Таджикистан	83,9	83,9	Замбія	63,1	63,1
Мавританія	79,6	79,6	Уганда	56,2	56,2
Мозамбік	78,4	78,4	Танзанія	53,8	53,8
Малі	70,5	70,5	Пакистан	45,9	45,9
Мадагаскар	67,9	67,9	Нігерія	40,5	40,5
Зімбабве	59,3	59,3	Ефіопія	32,0	32,0
Гаїті	42,7	42,7	6-й кластер		
Бурунді	37,2	37,2	Бруней	100,0	100,0
Чад	35,1	35,1	Антигуа і Барбуда	75,3	75,3
3-й кластер			Барбадос	64,7	64,7
Монголія	100,0	100,0	Сент-Вінсент і Гренадини	67,1	67,1
Марокко	97,4	97,4	Сент-Кіттс і Невіс	62,7	62,7
Панама	87,9	87,9	Багами	62,7	62,7
Перу	85,6	85,6	Домініка	61,1	61,1
Тринідад і Тобаго	71,8	71,8	Гренада	59,1	59,1
Боснія і Герцеговина	56,7	56,7	Самоа	58,6	58,6
Киргизстан	45,6	45,6	Сент-Люсія	57,8	57,8
Сальвадор	41,9	41,9	Тонга	53,9	53,9
Гватемала	36,8	36,8	Суринам	45,2	45,2
Непал	30,9	30,9	X	X	X

Аналізуючи результати, представлені в таблиці 2.5, можна сказати, що ряд країн досягають ефективності системи інформаційної безпеки в частині її забезпечення для національної економіки. До них відносяться: країни 0-го кластеру – Кіпр, Польща; країни 2-го кластеру – Венесуела; країни 3-го кластеру – Монголія; країни 4-го кластеру – Ботсвана; країни 5-го кластеру – Індія, Парагвай, Руанда; країни 6-го кластеру – Бруней. Результати для інших країн говорять про те, що їм слід приділити увагу тим напрямкам, які сприятимуть підвищенню ефективності, щоб досягти 100%-го значення в рамках кластеру. Це може відбуватися за рахунок того, що ряд вхідних ресурсів

потребують покращення або збільшення ефективності рівня інформаційної безпеки можливо за рахунок формування резервів окремих показників.

Проаналізуємо структурну ефективність вхідних показників для країн першого кластеру, отриману в результаті проведення аналізу за Input-oriented CCR-model (рисунок Г.1 додатку Г). Отримані значення всіх показників є від'ємними, тобто забезпечення поточного рівня інформаційної безпеки національної економіки країн 1-го кластеру відбувається із досягненням ефективності по кожному напряму – інституційної спроможності та цифрової спроможності і кібербезпеки. Слід відмітити, що для даних країн найбільший резерв формується саме за складовими інформаційної безпеки, тобто для них характерним є цифровізація економіки та розвиток IT-технологій, що слід враховувати при розробці стратегії безпеки країни. Україна є представником 1-го кластеру. Ефективність її інформаційної безпеки національної економіки забезпечується лише на рівні 63,7% по відношенню до інших країн кластеру (рисунок 2.26). Це відбувається за рахунок розподілу наступної структурної ефективності (рисунок 2.30).

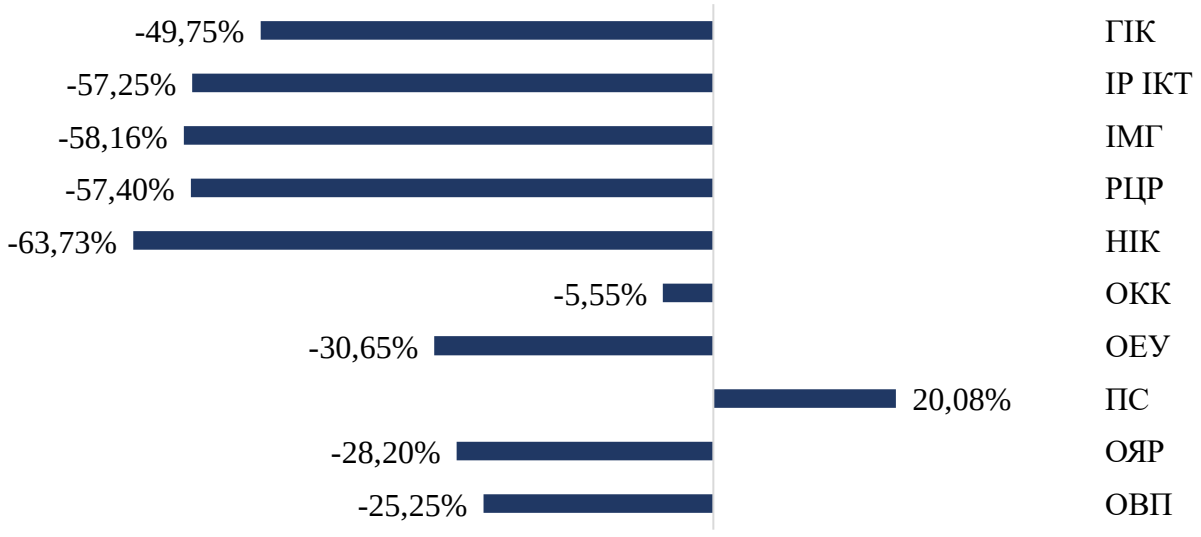


Рисунок 2.30 – Результати ефективності за складовими системи інформаційної безпеки національної економіки України (за Input-oriented CCR-моделлю) (складено авторкою)

На рисунку 2.30 можна побачити, що всі показники, окрім одного, мають достатній резерв (значення показників від'ємні), перерозподіл якого може забезпечити підвищення загального рівня інформаційної безпеки національної економіки. Але такий показник, як оцінка політичної стабільності та відсутності насилля / тероризму (ПС), потребує значного покращання для забезпечення ефективності системи інформаційної безпеки на фактичному рівні, оскільки його значення дорівнює 20,08%. Дана ситуація є цілком логічною в умовах військово-політичного конфлікту на Сході України. Оскільки вплив даного показника є досить вагомим, то першочерговим завданням для забезпечення ефективності інформаційної безпеки повинно бути саме урегулювання даної ситуації, а також створення умов для формування інформаційного простору, вільного від інформаційних атак з боку Російської Федерації.

Проведемо аналіз потенціалу покращання ефективності системи інформаційної безпеки країн першого кластера за умови максимізації інтегрального індексу інформаційної безпеки національної економіки. Результати Output-oriented CCR-model представлено на рисунку Г.2 додатку Г, де можна побачити, що максимальне зростання індексу інформаційної безпеки національної економіки можливе на 21,85%. Це можливо забезпечити за рахунок резервів потенціалу за показниками: глобальний індекс кібербезпеки (-5,59%), індекс розвитку ІКТ (-12,32%), рівень цифрового розвитку (-13,43%) та національний індекс кібербезпеки (-8,52%). Тобто країни першого кластеру мають потенціал цифрової спроможності та кібербезпеки, достатній для забезпечення підвищення рівня інформаційної безпеки національної економіки країни, тобто у даному випадку можна казати, що вони виступають драйвером розвитку.

З іншого боку, для забезпечення максимального рівня можливостей розвитку національної економіки країни повинні бути розроблені ряд заходів, спрямованих на підвищення контролю за корупцією (10,21%), якості регуляторних органів (13,14%), рівня верховенства права (4,63%), політичної стабільності в країні (5,85%), трансформації уряду (3,82%), а також мережевої

готовності країни (0,66%) (рисунок Г.2 додатку Г). Отримані результати свідчать, що країни 1-го кластера є країнами із низьким рівнем державного регулювання, тому для підвищення рівня їх інформаційної безпеки необхідно посилити саме інституційну складову.

Результати структурної ефективності складових максимального рівня інформаційної безпеки України представлені на рисунку 2.31.

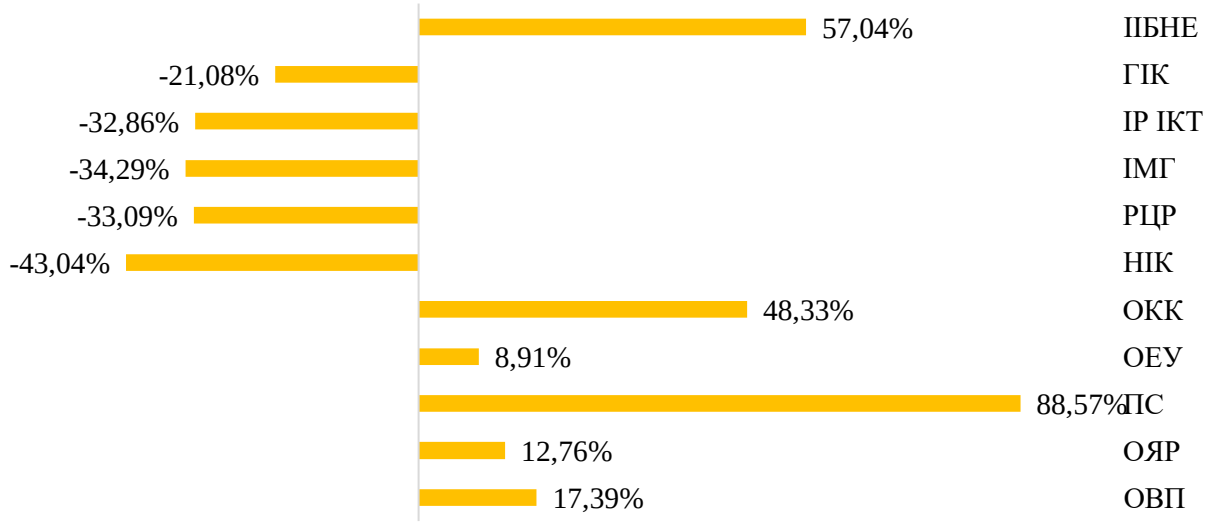


Рисунок 2.31 – Результати ефективності за складовими системи інформаційної безпеки національної економіки України (за Output-oriented CCR-моделлю) (складено авторкою)

На рисунку 2.31 можна побачити, що всі показники групи цифрової спроможності та кібербезпеки для України мають значні резерви для підвищення рівня ефективності її інформаційної безпеки, що говорить про їх можливості як драйверу розвитку країни в цілому та національної економіки зокрема. Що стосується інституційної складової, то ця група потребує значного покращання, особливо в частині регулювання політичної стабільності (88,57%) та заходів боротьби із корупцією (48,33%). Якраз корупція може бути однією із причин витоку інформації, а також одним з інструментів в процесі здійснення інформаційного та кібершпигунства. Відповідно це вимагає розробки спеціальних заходів багаторівневого доступу до інформації, особливо тієї, яка

має підвищений рівень секретності, а також шифрування даних.

Що стосується оцінювання ефективності потенціалу країн інших кластерів, то у таблиці 2.6 представлено зведені результати, отримані на основі Input-oriented CCR-model та розрахунки яких відображені у додатку Г.

Таблиця 2.6 – Порівняння потенціалу покращення ефективності системи інформаційної безпеки країн різних кластерів (Input-oriented CCR-model)

№	Назва показника	Input-oriented CCR-model, у %						
		0	1	2	3	4	5	6
1	Глобальний індекс кібербезпеки	-7,53	-12,25	-0,84	-6,29	0,76	-11,41	2,9
2	Індекс розвитку інформаційних і комунікаційних технологій	-1,02	-16,42	9,87	-10,06	-12,69	-13,22	-10,96
3	Індекс мережевої готовності країн	-8,74	-12,72	-6,83	-10,26	-14,3	-12,78	-13,7
4	Рівень цифрового розвитку країни	-5,89	-16,93	0,83	-9,65	-14,31	-12,54	-10,31
5	Національний індекс кібербезпеки	-25,13	-13,69	-0,87	-15,71	-11,92	-6,77	-5,46
6	Оцінювання контролю корупції	-12,09	-3,2	-14,06	-10,38	-8,56	-10,14	-12,54
7	Оцінювання ефективності уряду	-9,78	-7,23	-14,64	-10,79	-12,37	-7,59	-8,28
8	Політична стабільність і відсутність насилля / тероризму	-7,96	-7,34	-12,38	-5,48	-9,26	-7,42	-12,65
9	Оцінювання якості регуляторів	-8,28	-2,59	-20,07	-11,16	-7,26	-7,74	-10,52
10	Оцінювання верховенства права	-13,59	-7,63	-19,61	-10,22	-8,57	-10,39	-12,68
11	Інтегральний індекс інформаційної безпеки	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Так, для забезпечення фактичного рівня індексу інформаційної безпеки національної економіки, практично всі показники мають значний резерв, що характерно для країн всіх кластерів. Для країн 0-го кластеру є характерним високий рівень національної кібербезпеки (-25,13%) та верховенства права (-13,59%) (див. табл. 2.6), що свідчить про підтримку з боку держави процесів забезпечення безпеки, а також формування власної системи інформаційної

безпеки з урахуванням національних особливостей та рівня економічного, політичного та соціального розвитку.

Для країн 2-го кластеру критичним є значення індексу розвитку інформаційних і комунікаційних технологій (9,87%), тобто для них є властивим низький рівень інформатизації різних сфер життєдіяльності, що свідчить про низькі темпи цифровізації економіки. Але слід відмітити, що для країн даного кластеру є характерним значні резерви інституційної складової, які є найвищими серед інших кластерів. Тобто є можливості впливу на формування процесів інформаційного захисту в державі за рахунок створення передумов для організації ІТ-виробництв, розробки податкових пільг для ІТ-компаній, залучення іноземних інвестицій, формування державних грантових програм для підтримки ІТ-бізнесу в країнах даного кластеру.

Країни 3-го кластеру мають рівномірне формування ресурсного забезпечення інформаційної безпеки національної економіки, але їм слід більше приділити увагу політичній стабільності за рахунок регулювання конфліктів, характерних для більшості країн з цього кластеру. Країни 4-го та 6-го кластерів мають незабезпеченим глобальний показник кібербезпеки (0,76% та 2,9% відповідно) (див. табл. 2.6). Основною проблемою для них є низькі можливості впливу на глобальний рівень кібербезпеки, а саме: забезпечення правових взаємовідносин, формування механізмів технічного забезпечення інформаційної безпеки країни, розробка національних стратегій, метрик, освітніх заходів, забезпечення міжнародної кооперації з питань глобальної кібербезпеки, тощо.

Для країн п’ятого кластеру є характерним превалювання розвитку інформаційних і комунікаційних технологій (-13,22%) (див. табл. 2.6) серед отриманих значень для інших показників. Це свідчить про потенціал та можливості не тільки для розвитку технологій але й для розвитку інших сфер.

Результати аналізу ефективності системи інформаційної безпеки країн різних кластерів з урахуванням визначення максимального рівня індексу протидії інформаційним загрозам, отримані в результаті побудови Output-oriented CCR-model, представлені у таблиці 2.7.

Таблиця 2.7 – Порівняння потенціалу покращення ефективності системи інформаційної безпеки країн різних кластерів (Output-oriented CCR-model)

№	Назва показника	Output-oriented CCR-model, y%						
		0	1	2	3	4	5	6
1	Глобальний індекс кібербезпеки	4,10	-5,59	7,81	11,6	28,43	-2,85	28,16
2	Індекс розвитку інформаційних і комунікаційних технологій	17,51	-12,32	19,11	1,98	-5,44	-8,39	-3,17
3	Індекс мережевої готовності країн	2,16	0,66	1,33	-1,45	-10,21	-9,06	-9,68
4	Рівень цифрового розвитку країни	7,79	-13,43	10,26	2,6	-9,6	-6,56	-1,6
5	Національний індекс кібербезпеки	-29,66	-8,52	7,6	-17,22	-3,83	5,79	8,71
6	Оцінювання контролю корупції	-4,97	10,21	-6,16	-0,82	0,92	-0,17	-6,76
7	Оцінювання ефективності уряду	0,10	3,82	-6,47	-1,77	-5,52	8,64	2,99
8	Політична стабільність і відсутність насилля / тероризму	3,95	5,85	-4,45	12,38	0,55	9,34	-7,17
9	Оцінювання якості регуляторів	2,99	13,14	-12,72	-2,96	6,92	4,54	-1,9
10	Оцінювання верховенства права	-7,20	4,63	-12,27	0,13	1,31	-1,4	-7,27
11	***Інтегральний індекс інформаційної безпеки***	***19,58***	***21,85***	***11,83***	***47,09***	***27,27***	***43,27***	***22,58***

Максимальне зростання індексу інформаційної безпеки національної економіки для країн нульового кластеру можливе на 19,58%, що ймовірно забезпечити за рахунок існуючих резервів національного індексу кібербезпеки (-29,66%), контролю корупції (-4,97%) та верховенства права (-7,20%) (див. табл. 2.7). Відповідно, для стимулювання розвитку інформаційної безпеки національної економіки необхідно впроваджувати заходи із розроблення політики кібербезпеки, впровадження менеджменту кіберкриз, забезпечення аналізу кіберзагроз, розвитку освіти та підвищення кваліфікації у напрямку інформаційної безпеки, розвитку трастових послуг в сфері електронної ідентифікації, тощо. Для країн другого кластеру можливе зростання індексу інформаційної безпеки національної економіки на 11,83%, що можливо повністю за рахунок резервів інституційної спроможності, а саме: контролю корупції (-6,16%), ефективності уряду (-6,47%), політичної стабільності (-4,45%), якості регуляторів (-12,72%) та верховенства права (-12,27%) (див. табл. 2.7). Тобто,

потужний рівень розвитку інформаційної безпеки національної економіки країн 2-го кластеру можливий за рахунок наявних резервів якісного управління державою, що полягає у створенні умов ефективної зайнятості фахівців з питань безпеки, відсутності корупції, здійсненні якісного правового регулювання питань інформаційної безпеки та правової відповідальності за її порушення, тощо.

Індекс інформаційної безпеки національної економіки для країн третього кластеру може зростати на 47,09% (максимальне значення у порівнянні з іншими кластерами) за умови існуючих резервів індексу мережевої готовності країни (-1,45%), національного індексу кібербезпеки (-17,22%), контролю корупції (-0,82%), ефективності уряду (-1,77%), якості регуляторів (-2,96%) (див. табл. 2.7). Тобто країни даної групи, як і країни 0-го кластеру мають достатні резерви кібербезпеки та ефективний уряд, що сприятиме створенню сприятливих умов для розвитку ІТ-галузі. Для країн четвертого кластеру можливе зростання інтегрального рівня інформаційної безпеки національної економіки на 27,27% за рахунок розвитку інформаційних і комунікаційних технологій (-5,44%), мережевої готовності країни (-10,21%), її цифрового розвитку (-9,6%), національної кібербезпеки (-4,18%), індексу мережевої готовності країни (-0,14%), рівня цифрового розвитку (-3,83%), ефективності уряду (-5,52%) (див. табл. 2.7). Для даної групи є характерним саме створення резерву інформаційно-технологічного спрямування, оскільки в даний кластер потрапляють країни, що розвиваються та потребують збільшення інвестиції саме в ІТ-сферу, яку вони розглядають як найбільш пріоритетною галуззю.

Для країн п’ятого кластеру можливе найбільше зростання індексу інформаційної безпеки національної економіки у порівнянні із іншими – на 43,27%. Це може бути обумовлено за рахунок внеску у глобальну кібербезпеку (-2,85%), розвитку інформаційних і комунікаційних технологій (-8,39%), мережевої готовності країни (-9,06%), її цифрового розвитку (-6,56%), контролю корупції (-0,17%), верховенства права (-1,4%) (див. табл. 2.7). Країни даної групи мають достатній інформаційно-технологічний потенціал, який дозволить їм не тільки

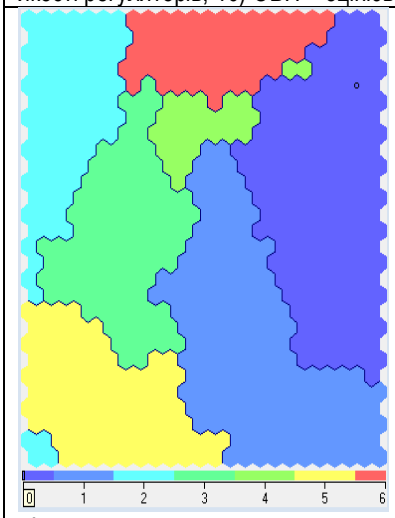
підвищити рівень протидії інформаційним загрозам, але й сприятиме розвитку ІТ-сфери, цифровізації економіки та суспільства, що в подальшому забезпечить й зростання економіки. Існуючий потенціал країн шостого кластеру уможливлює зростання інтегрального рівня інформаційної безпеки на 22,58% за рахунок існуючих резервів контролю корупції (-6,76%), політичної стабільності (-7,17%), якості регуляторів (-1,9%), верховенства права (-7,27%), розвитку інформаційних і комунікаційних технологій (-3,17%), мережевої готовності (-9,68%), цифрового розвитку (-1,6%) (див. табл. 2.7). Тобто країни даної групи мають достатній резерв й інституційних та інформаційно-технологічних ресурсів, що дозволить підвищити ефективність протидії інформаційним загрозам.

Узагальнення ключових позицій запропонованої методології та результатів аналізу ефективності представлено на рисунку 2.32.

Питання підвищення ефективності системи інформаційної безпеки у частині забезпечення протидії загрозам національної економіки є досить актуальним, що пов’язано із зростанням рівня інформатизації, цифровізації та комп’ютеризації суспільства. Застосування Data Envelopment Analysis у даному дисертаційному дослідженні дозволило визначити ефективність системи інформаційної безпеки країн, об’єднаних в кластери з урахуванням рівня їх інституційної спроможності та цифрової спроможності і кібербезпеки.

Використані моделі CCR та BBC надали можливості проаналізувати структурну ефективність показників інституційного розвитку країн та аспектів їх безпеки з урахуванням поточного рівня інтегрального індексу інформаційної безпеки національної економіки. Також дані моделі дозволили оцінити максимальний рівень його зростання за наявного ресурсного потенціалу країни. Модель CCR виявилася більш обмежуючою, ніж BCC, для визначення ефективності, що сприяло формуванню більш критичної оцінки щодо існуючих резервів країн, необхідних для забезпечення протидії інформаційним загрозам. Саме тому вона була використана для проведення аналізу усіх кластерів країн.

Етап 1. Проведення кластерного аналізу: *вхідні показники кластеризації*: 1) ГІК – глобальний індекс кібербезпеки; 2) ІР ІКТ – індекс розвитку інформаційних і комунікаційних технологій; 3) ІМГ – індекс мережевої готовності країн; 4) РЦР – рівень цифрового розвитку країни; 5) НІК – національний індекс кібербезпеки; 6) ОКК – оцінювання контролю корупції; 7) ОЕУ – оцінювання ефективності уряду; 8) ПС – політична стабільність і відсутність насилля / тероризму; 9) ОЯР – оцінювання якості регуляторів; 10) ОВП – оцінювання верховенства права; *вихідні:* 11) ІІБНЕ – індекс ІБ НЕ



а) кластери країн за картами Кохонена

Склад кластерів країн світу за показниками інституційної та цифрової спроможності, а також кібербезпеки

Назва індикатора інтегрального індексу ІБ НЕ	Середні значення індикаторів, що відповідають певному кластеру (у дужках зазначено кількість країн у кластері)						
	0 (42)	1 (31)	2 (24)	3 (21)	4 (6)	5 (17)	6 (18)
ІР ІКТ	77,74	60,29	17,88	40,57	47,33	29,71	45,33
ІМГ	74,29	58,16	21,5	51,62	55,23	45,24	0,00
ГІК	80,26	67,52	15,04	27,14	26,33	58,06	18,00
НІК	68,58	45,79	12,07	25,05	24,03	36,67	12,19
РЦР	75,95	60,41	24,67	46,03	51,47	38,93	45,37
ОКК	1,21	–0,28	–1,20	–0,59	0,64	–0,67	0,38
ОЕУ	1,28	0,05	–1,35	–0,41	0,36	–0,52	–0,04
ОЯР	1,30	0,07	–1,24	–0,34	0,11	–0,57	–0,18
ОВП	1,26	–0,18	–1,30	–0,54	0,28	–0,54	0,28
ПС	0,77	–0,34	–1,29	–0,16	0,73	–0,90	0,82

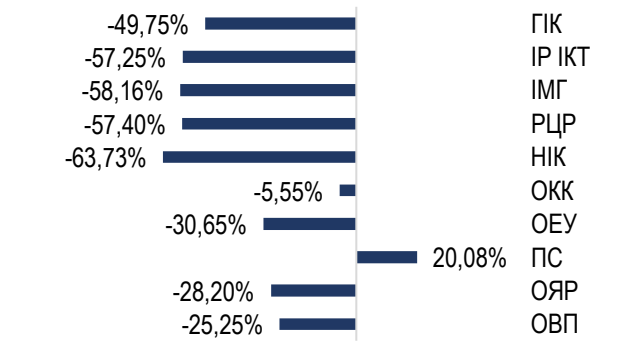
Етап 2. Визначення вагів вхідних показників за методом головних компонентів

Етап 3. Проведення DEA-аналізу та побудова CCR-моделі

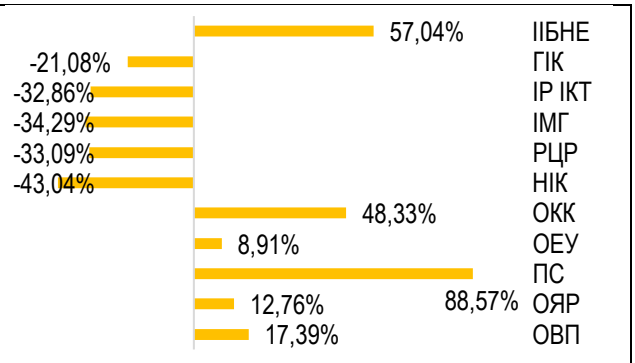
б) результати оцінювання ефективності ІБ НЕ кластерів країн

№*	Input-oriented CCR-model, %							Output-oriented CCR-model, %						
	0	1	2	3	4	5	6	0	1	2	3	4	5	6
1	–7,53	–12,25	–0,84	–6,29	0,76	–11,41	2,9	4,10	–5,59	7,81	11,6	28,43	–2,85	28,16
2	–1,02	–16,42	9,87	–10,06	–12,69	–13,22	–10,96	17,51	–12,32	19,11	1,98	–5,44	–8,39	–3,17
3	–8,74	–12,72	–6,83	–10,26	–14,3	–12,78	–13,7	2,16	0,66	1,33	–1,45	–10,21	–9,06	–9,68
4	–5,89	–16,93	0,83	–9,65	–14,31	–12,54	–10,31	7,79	–13,43	10,26	2,6	–9,6	–6,56	–1,6
5	–25,13	–13,69	–0,87	–15,71	–11,92	–6,77	–5,46	–29,66	–8,52	7,6	–17,22	–3,83	5,79	8,71
6	–12,09	–3,2	–14,06	–10,38	–8,56	–10,14	–12,54	–4,97	10,21	–6,16	–0,82	0,92	–0,17	–6,76
7	–9,78	–7,23	–14,64	–10,79	–12,37	–7,59	–8,28	0,10	3,82	–6,47	–1,77	–5,52	8,64	2,99
8	–7,96	–7,34	–12,38	–5,48	–9,26	–7,42	–12,65	3,95	5,85	–4,45	12,38	0,55	9,34	–7,17
9	–8,28	–2,59	–20,07	–11,16	–7,26	–7,74	–10,52	2,99	13,14	–12,72	–2,96	6,92	4,54	–1,9
10	–13,59	–7,63	–19,61	–10,22	–8,57	–10,39	–12,68	–7,20	4,63	–12,27	0,13	1,31	–1,4	–7,27
11	***0,00***	***0,00***	***0,00***	***0,00***	***0,00***	***0,00***	***0,00***	***19,58***	***21,85***	***11,83***	***47,09***	***27,27***	***43,27***	***22,58***

* № відповідає номерам індексів (див. етап 1); кольором виділені значення індексів, що потребують покращання.



в) результати ефективності системи ІБ НЕ України (Input-oriented CCR-model)



г) результати ефективності системи ІБ НЕ України (Output-oriented CCR-model)

Рисунок 2.32 – Методологія та результати аналізу ефективності системи забезпечення інформаційної безпеки (ІБ) національної економіки (НЕ) (складено авторкою)

В результаті було отримано, що збільшення інтегрального рівня інформаційної безпеки національної економіки можливо в межах від 11,83% до 47,09%. Найбільше зростання є характерним для кластеру, в якому представлені країни з низьким рівнем економічного розвитку. Але вони мають потенціал інституційної спроможності та розвитку ІТ-сфери, достатній для здійснення такого потужного зростання й рівня протидії інформаційним загрозам. Для країн, які займають лідуючі позиції у світі відповідно до їх високого рівня економічного розвитку, а також високого рівня життя та добробуту населення, є можливим підвищення інтегрального рівня інформаційної безпеки на 19,58%, що можливе за рахунок потужного рівня національної кібербезпеки країни.

Аналіз структурної ефективності також дозволив виділити ті слабкі місця, які потребують кардинальних змін. Це стосується необхідності трансформації інформаційно-технологічної складової для країн нульового та другого кластеру. Вони мають передумови для створення комфортних умов залучення ІТ-фахівців, побудови сучасних підприємств з виробництва комп'ютерних технологій, розвитку ІТ-стартапів, тощо. Країнам першого кластеру доцільно підвищувати державні витрати на інформаційну безпеку, а також підсилювати рівень її державного регулювання. Для країн із низьким рівнем економічного розвитку третього та п'ятого кластеру доцільно звернути увагу на забезпечення формування умов припинення воєнних конфліктів та політичної стабілізації. Також їх недостатній рівень соціо-економічного розвитку потребує зростання економіки та підвищення рівня соціальних стандартів, що стимулюватиме й приріст ефективності інформаційної безпеки. Країнам 4-го та 6-го кластерів критично важливо звернути увагу на формування їх внеску у глобальну кібербезпеку, що пов'язано із вирішенням питань їх участі у міжнародному співробітництві з проблем інформаційної безпеки та розвитку міжнародного волонтерства у цій сфері.

Висновки до розділу 2

1. У підрозділі 2.1 дисертаційної роботи для обґрунтування індикаторів, які повинні бути враховані під час інтегрального оцінювання рівня інформаційної безпеки країни, сформовано 8 груп показників: цифрової спроможності національної економіки і кібербезпеки (5), економічного (9), соціального (4) та фінансового (5) розвитку національної економіки, зовнішньо–економічної діяльності (4), інноваційної активності (8), якості інформаційної інфраструктури (2), інституційної спроможності держави (5). Дослідження здійснене на основі даних 159 країн світу за 2018 р. із використанням інструментарію канонічного аналізу в аналітичному пакеті «STATISTICA».

2. Результати розрахунків засвідчили, що найбільш істотний взаємний вплив демонструють група індикаторів інституційної спроможності держави та група показників цифрової спроможності національної економіки і кібербезпеки (відповідні значення показника «Total Redundancy» за результатами канонічного аналізу становлять 67,87 % та 59,82 %). Тому саме ці 10 індикаторів і рекомендовано враховувати під час інтегрального оцінювання рівня інформаційної безпеки країни. Розрахунок канонічних ваг засвідчив, що з цих двох груп індикаторів найбільш вагомими є «Рівень цифрового розвитку» та «Ефективність уряду», що повинно бути враховано під час формування державної політики забезпечення інформаційної безпеки.

3. У підрозділі 2.2 дисертаційної роботи для інтегрального оцінювання рівня інформаційної безпеки національної економіки запропоновано використовувати метод переваг, згідно з яким нормалізовані значення п’яти індикаторів групи цифрової спроможності національної економіки та кібербезпеки, а також п’яти індикаторів групи інституційної спроможності держави трансформуються за допомогою шкали бажаності Харрінгтона (вибір типу кривої перетворення обумовлений характером відмінності фактичних значень відповідних показників від нормалізованих). Одержані значення

узагальнено в межах інтегрального індикатора інформаційної безпеки національної економіки за функцією Харрінгтона – Менчера.

4. Розрахунки на даних 159 країн світу за 2018 р. засвідчили, що найвищий рівень інформаційної безпеки національної економіки мають 49 країн світу (до першої п'ятірки увійшли: Сінгапур (0,9989), Норвегія (0,9987), Люксембург (0,9987), Нідерланди (0,9986), Данія (0,9985)), а найнижчий – 54 (цей рейтинг замикають такі країни, як Афганістан (0,0113), Туркменістан (0,0102), Ємен (0,0062), Південний Судан (0,0028)). Україна потрапила до складу 24 країн, чий рівень інформаційної безпеки національної економіки оцінюють як задовільний. Зокрема, розрив між інтегральними індексами для України та Сінгапуру (країни-лідера) становить 0,6218 од., що значно більшою мірою обумовлене розривами за субіндексами інституційної спроможності країни (у середньому на 145,79 %), ніж за субіндексами цифрової спроможності та кібербезпеки (у середньому на 27,76 %).

5. У підрозділі 2.3 дисертаційної роботи за допомогою системного поєднання методу DEA-аналізу в специфікації CCR із використанням аналітичного пакета «Frontier Analyst» та кластерного аналізу, реалізованого за допомогою побудови карт Кохонена на платформі «Deductor Academic», сформовані 7 кластерів країн, які є найбільш близькими за співвідношенням фактичних рівнів складових інтегрального індексу інформаційної безпеки національної економіки. Україна ввійшла до кластеру № 1 разом із більшістю пострадянських країн, а також Аргентиною, Бразилією, Болгарією, Індонезією, Оманом, Мексикою, Румунією, Туреччиною та ін. Це дослідження дозволило встановити для кожного кластеру країн характерні для них особливості розвитку інформаційної безпеки національної економіки та визначити відповідні напрямки реалізації державної політики щодо збільшення рівнів цифрової та інституційної спроможності національної економіки, а також кібербезпеки.

6. У роботі визначений максимальний рівень інформаційної безпеки, якого може досягти країна за умови наявного потенціалу, а також приховані резерви для його підвищення. Так, зокрема, поточна ефективність системи забезпечення інформаційної безпеки України становить 63,7 % від її максимального значення

в межах кластеру, водночас її підтримання на цьому рівні і в майбутньому потребує підвищення лише однієї з компонент інтегрального індексу інформаційної безпеки національної економіки – індексу політичної стабільності та відсутності насилля / тероризму (на 20,08 %), що є абсолютно логічним в умовах військово-політичного конфлікту на Сході України.

7. Крім того, розрахунки засвідчили, що за умови застосування відповідних регуляторних інтервенцій інтегральний рівень інформаційної безпеки України може збільшитися максимально на 57,04 %. Умовами цього збільшення повинне стати покращання не субіндексів цифрової спроможності та кібербезпеки країни, а показників її інституційної спроможності: контролю корупції – на 48,33 %, ефективності уряду – на 8,91 %, політичної стабільності та відсутності насилля / тероризму – на 88,57 %, якості регуляторів – 12,76 %, верховенства права – 17,39 %, що можливо здійснити за рахунок потенційних резервів показників цифрової спроможності і кібербезпеки. Отже, основні можливості підвищення рівня інформаційної безпеки в Україні перебувають у площині підвищення якості державного регулювання національної економіки.

Основні положення другого розділу дисертаційної роботи опубліковано авторкою в роботах [261, 262, 263, 382, 386, 389, 403].

РОЗДІЛ 3 ПРИЧИННО-НАСЛІДКОВІ ЗВ'ЯЗКИ У ДОСЛІДЖЕННІ ВПЛИВУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РОЗВИТОК НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

3.1 Вплив економічних факторів на формування національних патернів персональної інформаційної безпеки

Важливим аспектом організації інформаційної безпеки у країні є ефективне її забезпечення також й на рівні окремого користувача програмних та технічних засобів, що, як наслідок, може впливати на настрої населення у суспільстві. Наприклад, якщо людина стає об'єктом зламування її акаунту у соціальній мережі або її поштової скриньки, то, як правило, це призводить до негативної реакції користувача по відношенню до компаній-власників мережі, провайдерів, тощо. Масовість та систематичність таких дій може викликати зниження кількості користувачів та, відповідно, зменшення рівня доходів від розміщення онлайн-реклами, продажу контенту, тощо. Якщо відбувається атака на онлайн-банкінг або застосовується соціальна інженерія, в результаті чого здійснюється витік досить важливої інформації, яка стосується фінансових операцій, рахунків, платіжних карт, то це може призвести до незаконного привласнення коштів з особових рахунків клієнтів. Як наслідок, фінансові установи змушені відшкодовувати втрати своїм клієнтам, або в протилежному випадку вони їх втрачають, що призводить до зменшення довіри, появи репутаційних ризиків, зростання збитків. Саме тому виникає потреба у виявленні настроїв населення, які формуються під впливом зростання або зниження рівня їх персональної інформаційної безпеки. З цією метою проведемо аналіз даних, отриманих в результаті моніторингу громадської думки в країнах – членах Європейського Союзу та країнах кандидатах, що здійснювалося в рамках програми Євробарометр. Для цього було використано дані за 2014 та 2019 роки, представлені на порталі відкритих даних Європейського Союзу [220, 221]. Вибір періоду дослідження здійснювався виходячи із того, що 2014 рік – це початок проведення дослідження, 2019 рік – останнє проведене опитування.

На рисунку 3.1 представлена динаміка користувачів онлайн-банкінгу в країнах ЄС за 2014 та 2019 роки.

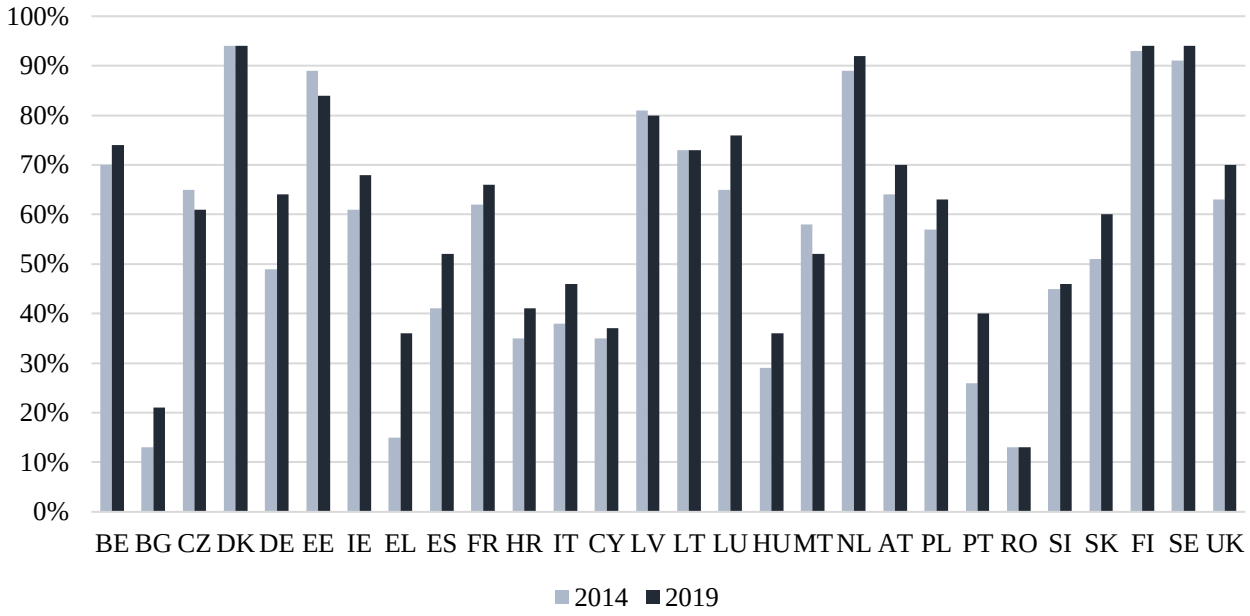


Рисунок 3.1 – Динаміка користувачів онлайн-банкінгу в країнах ЄС

Скорочення: BE – Бельгія, BG – Болгарія, CZ – Чехія, DK – Данія, EE – Естонія, IE – Ірландія, EL – Греція, ES – Іспанія, FR – Франція, HR – Хорватія, IT – Італія, CY – Кіпр, LV – Латвія, LT – Литва, LU – Люксембург, HU – Угорщина, MT – Мальта, NL – Нідерланди, AT – Австрія, PL – Польща, PT – Португалія, RO – Румунія, SI – Словенія, SK – Словаччина, FI – Фінляндія, SE – Швеція, UK – Великобританія.

Джерело: складено авторкою на основі [220, 221].

Для користувачів більшості європейських країн характерним є зростання операцій, які здійснюються ними із використанням онлайн-банкінгу. Так, це властиво Бельгії (+4%), Болгарії (+8%), Німеччині (+15%), Ірландії (+7%), Греції (+21%), Іспанії (+11%), Франції (+4%), Хорватії (+6%), Італії (+8%), Кіпру (+2%), Люксембургу (+11%), Угорщині (+7%), Нідерландам (+3%), Австрії (+6%), Польщі (+6%), Португалії (+14%), Словенії (+1%), Словаччині (+9%), Фінляндії (+1%), Швеції (+3%), Великобританії (+7%). Рівень використання онлайн-банкінгу за 6 років залишився незмінним або зменшився для користувачів Чехії

(-4%), Данії (0%), Естонії (-5%), Латвії (-1%), Литви (0%), Мальти (-6%), Румунії (0%). В цілому спостерігається позитивна тенденція зростання кількості клієнтів комп'ютерних банківських послуг, що в середньому складає приблизно 5%.

Проаналізуємо інші види комп'ютерних сервісів послуг, які користуються попитом серед населення європейських країн. Динаміка користувачів, що купують товари та послуги через Інтернет, представлена на рисунку 3.2.

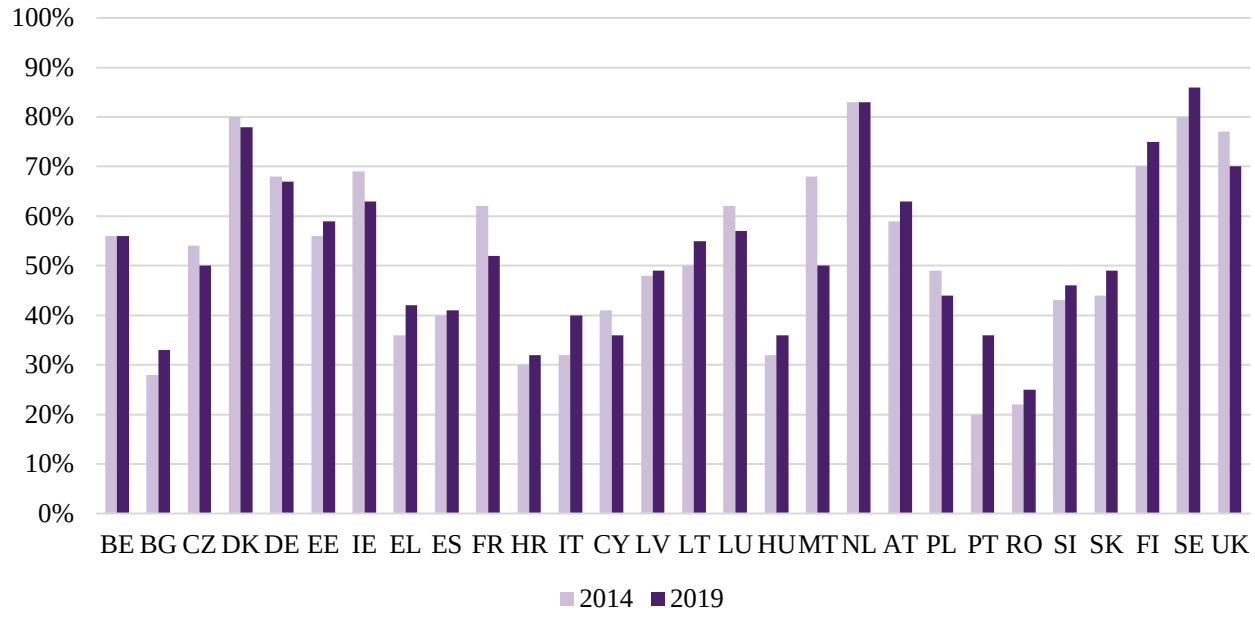


Рисунок 3.2 – Динаміка користувачів в країнах ЄС, що купують товари та послуги через Інтернет

Джерело: складено авторкою на основі [220, 221]

Аналізуючи дані рисунку 3.2, можна побачити, що перевагу здійсненню операцій купівлі товарів та послуг через засоби Інтернет надають жителі таких країн: Болгарії (+5%), Естонії (+3%), Греції (+6%), Іспанії (+1%), Хорватії (+2%), Італії (+8%), Латвії (+1%), Литви (+5%), Угорщини (+4%), Австрії (+4%), Португалії (+16%), Румунії (+3%), Словенії (+3%), Словаччини (+5%), Фінляндії (+5%), Швеції (+6%). За 6 років кількість операцій купівлі товарів та послуг залишилася незмінною або зменшилася для користувачів Чехії (-4%), Данії (-2%), Німеччини (-1%), Ірландії (-6%), Франції (-10%), Кіпру (-5%), Люксембургу (-5%), Мальти (-18%), Нідерландів (0%), Польщі (-5%), Великобританії (-7%). В

середньому для країн ЄС по даному показнику не спостерігаються зміни (0%), що говорить про стабільність настроїв населення в плані здійснення подібних операцій.

Також проаналізуємо динаміку користувачів, що продають товари та послуги через Інтернет (рисунок 3.3).

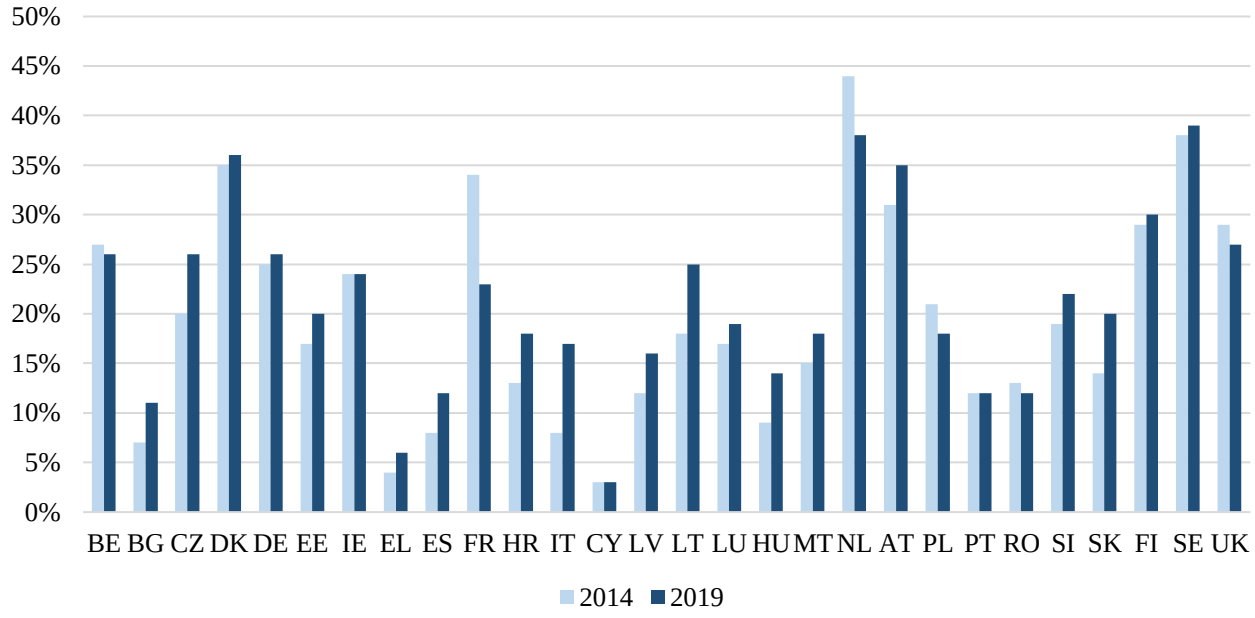


Рисунок 3.3 – Динаміка користувачів в країнах ЄС, що продають товари та послуги через Інтернет

Джерело: складено авторкою на основі [220, 221]

Дані рисунку 3.3 свідчать, що перевагу здійсненню операцій онлайн-продажу товарів та послуг надають жителі таких країн: Болгарії (+4%), Чехії (+6%), Данії (+1%), Німеччини (+1%), Естонії (+3%), Греції (+2%), Іспанії (+4%), Хорватії (+5%), Італії (+9%), Латвії (+4%), Литви (+7%), Люксембургу (+2%), Угорщини (+5%), Мальти (+3%), Австрії (+4%), Словенії (+3%), Словаччини (+6%), Фінляндії (+1%), Швеції (+1%). Кількість операцій продажу товарів та послуг через Інтернет за 6 років залишилася незмінною або зменшилася для користувачів Бельгії (-1%), Ірландії (0%), Франції (-11%), Кіпру (0%), Нідерландів (-6%), Португалії (0%), Румунії (-1%), Польщі (-3%), Великобританії

(-2%). В середньому для країн ЄС по даному показнику спостерігається зростання (+2%).

Тобто, не дивлячись на зростання впливу інформаційних загроз на різні види та сфери діяльності людини, спостерігається позитивна тенденція щодо використання населенням комп'ютерних та мобільних технологій, програмних додатків, Інтернету для здійснення ними операцій фінансово-економічного характеру, що може свідчити також й про зростання заходів інформаційної безпеки, які вживає населення, або зростання інформаційної обізнаності щодо активізації кіберзлочинців та шахраїв.

На рисунках 3.4-3.5 представлена інформація щодо заходів безпеки, які вживають опитувані.

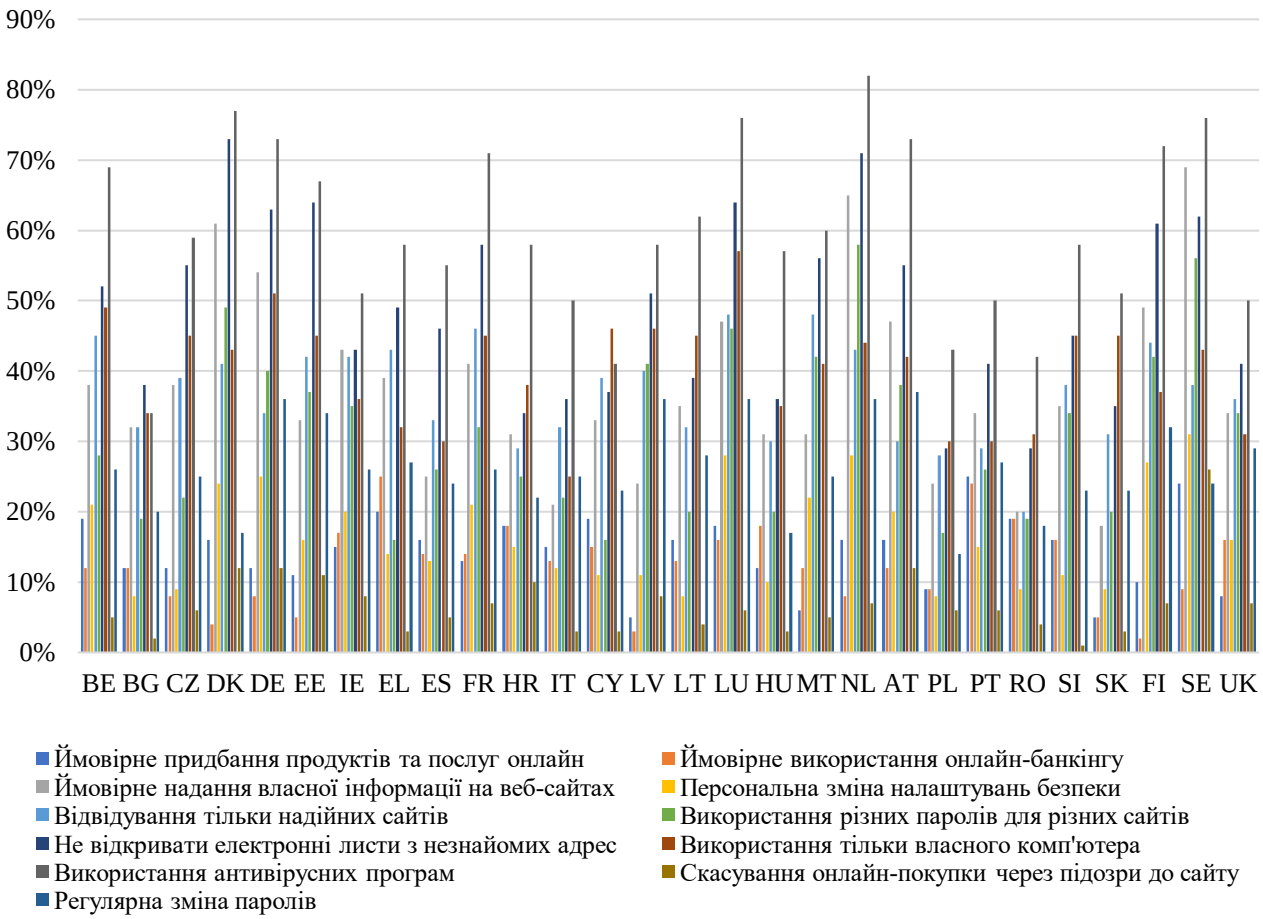


Рисунок 3.4 – Діаграма заходів інформаційної безпеки, які використовувало населення країн ЄС у 2014 році

Джерело: складено авторкою на основі [220, 221]

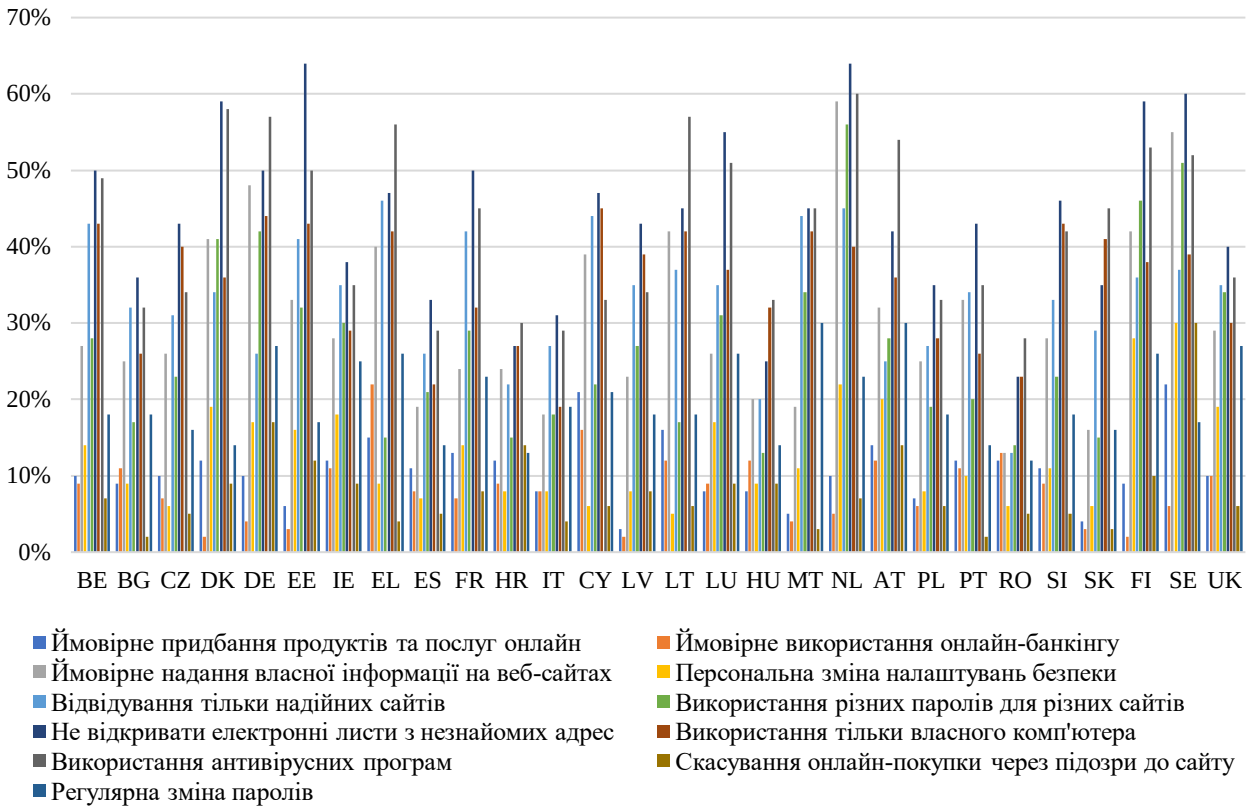


Рисунок 3.5 – Діаграма заходів інформаційної безпеки, які використовувало населення країн ЄС у 2019 році

Джерело: складено авторкою на основі [220, 221]

Аналізуючи дані рисунків 3.4-3.5, можна побачити, що в цілому у 2019 році в порівнянні із 2014 роком спостерігається зменшення відсотків респондентів, щодо застосування ними будь-яких заходів безпеки. Так, ймовірному придбанню продуктів та послуг онлайн надає перевагу менша кількість населення, що в середньому зменшилося на 4%. Тільки на Кіпрі та у Великобританії даний показник збільшився на 2%. Аналогічна ситуація спостерігається у відношенні до такого заходу, як ймовірне використання онлайн-банкінгу. Тільки в однієї країні спостерігається зростання даного показника (Кіпр +1%), що стосується інших, то тут відбувається падіння в середньому на 4%. Тобто респонденти ЄС зменшують ризик втрати інформації за рахунок зниження кількості операцій щодо придбання продуктів та послуг онлайн та операцій онлайн-банкінгу. З одного боку, кількість споживачів онлайн-послуг зростає в більшості країн (рисунки 3.1-3.2), а з іншого боку зменшується ймовірність того, що вони будуть

їх використовувати для того, щоб збільшити рівень захищеності своїх платіжних даних. Можна зробити висновок, що існує певна недовіра європейців до захищеності мобільного та Інтернет-банкінгу, тому вони менше готові ризикувати, щоб використовувати платіжні онлайн-сервіси.

Що стосується ймовірного надання власної інформації на веб-сайтах, то у 2019 році кількість таких респондентів знизилася в середньому на 7%, причому максимального рівня було досягнуто у Люксембургу (-21%) та Данії (-20%). Це говорить про те, що користувачі стали більш обережними в плані надання персональних даних в процесі користування ними онлайн-сервісів. Хоча в таких країнах, як Греція (+1%), Кіпр (+6%), Литва (+7%) та Польща (+1%), навпаки спостерігається збільшення даного показника, що може говорити про або зростання надійності онлайн-послуг, або зменшення кількості інцидентів щодо втрати та викрадення даних. Також знизилася кількість європейців, готових самостійно змінювати налаштування безпеки, що склало в середньому -4%. Тільки ситуація є зворотною для Болгарії (+1%), Фінляндії (+1%) та Великобританії (+3%). Можна відмітити, що це позитивна тенденція, оскільки трапляються випадки втрати даних за рахунок відкритості пристроїв та акаунтів користувачів, які не є достатньо обізнаними в даній сфері.

Такому способу персонального захисту, як відвідування тільки надійних сайтів, надає перевагу менша кількість опитуваних, що склало в середньому -4%. Хоча населення Греції (+3%), Кіпру (+5%), Литви (+5%), Нідерландів (+2%), Португалії (+5%), не нехтує даним заходом та звертає увагу на надійність веб-ресурсів. Знизилася також популярність такого способу у європейців, як використання різних паролів для різних сайтів (-4%). Але в деяких країнах користувачі продовжують надавати йому перевагу: Чехія (+1%), Німеччина (+2%), Кіпр (+6%), Польща (+2%) та Фінляндія (+4%). Також зменшилася кількість респондентів, які регулярно змінюють пароль, при чому цей показник в середньому знизився на 6% серед країн ЄС, хоча серед населення Мальти (+5%) та Польщі (+4%) спостерігається його зростання. Але скасувати онлайн-покупки

через підозру до сайту готова більша кількість європейців (+1%), окрім жителів Чехії (-1%), Данії (-3%), Мальти (-2%), Польщі (-4%) та Великобританії (-1%).

Найбільш популярними серед респондентів виявилися такі способи захисту, як використання антивірусних програм, використання тільки власного комп'ютера та захищеність шляхом не відкриття електронних листів з незнайомих адресів. В динаміці надання ним переваги користувачами з різних країн ЄС представлено на рисунку 3.6.

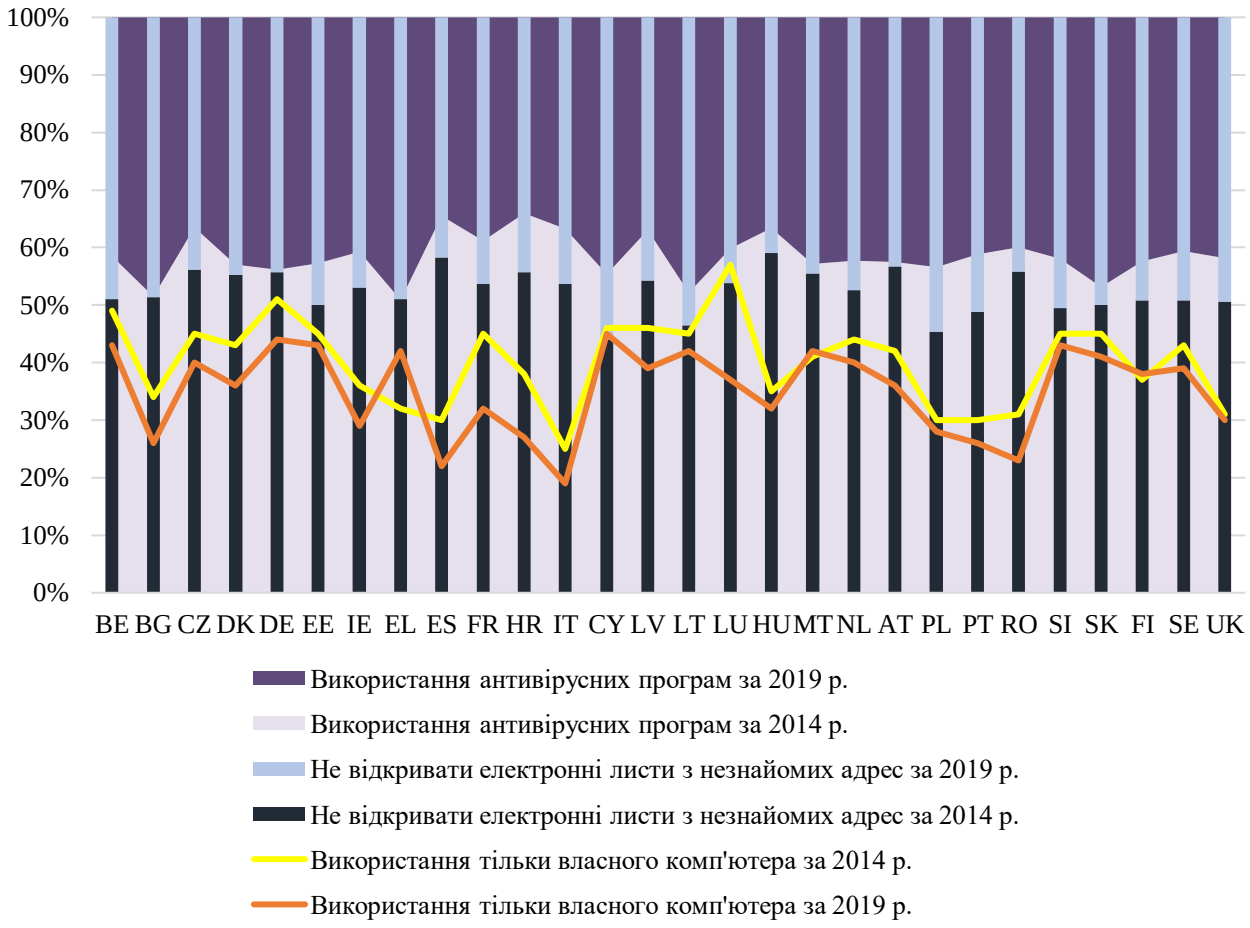


Рисунок 3.6 – Діаграма трьох найбільш популярних заходів інформаційної безпеки, які використовувало населення країн ЄС у 2014 та 2019 роках
Джерело: складено авторкою на основі [220, 221]

Хоча способи захисту, представлені на рисунку 3.6, обирає найбільша кількість користувачів, але в цілому спостерігається падіння даних показників. Так, спостерігається різке зниження використання антивірусних програм у 2019

році у порівнянні із 2014 роком, при чому в середньому це склало -17%. Опитувальні з кожної країни знизили рівень використання даного виду програмного забезпечення, що у контексті зростання кіберінцидентів, шахрайств та інформаційних витоків, є досить незрозумілим фактом. Ймовірно це можна пояснити тільки тим, що функції антивірусних програм зараз виконують вбудовані в операційну систему спеціальні програми-захисники. Наприклад, Windows Defender в операційній системі Windows. Або такі операційні системи, як MacOC, вже передбачають високий ступінь захисту шляхом обмеження завантаження неякісного програмного забезпечення та надання можливостей користуватися тільки ліцензійними програмами, які було протестовано у ручному режимі.

В середньому на 5% знизилося кількість респондентів, які використовують свій власний комп'ютер та не користуються сторонніми пристроями. Хоча у Греції (+10%), на Мальті (+1%) та у Фінляндії (+1%) цей показник зріс. Також на 5% зменшилася кількість європейців, які не відкривають підозрілі листи, що говорить або про збільшення довіри до програм, які можуть виявляти та блокувати такі листи, або все ж таки про зменшення обізнаності у питаннях персонального захисту. Хоча респонденти Кіпру (+10%), Литви (+6%), Польщі (+6%), Португалії (+2%), Словенії (+1%), звертають увагу на даний спосіб захисту та не відкривають електронні листи з незнайомих адрес.

В цілому можна зробити висновок, що за 6 років зменшилася кількість населення, яке активно продовжує захищати свої дані та цифрові пристрої, особливо в частині зниження використання антивірусних програм, використання тільки власного комп'ютера, невідкривання підозрілих листів, регулярної зміни паролів, використання різних паролів для різних сайтів, відвідування тільки надійних сайтів. Хоча респонденти готові відмовитися від онлайн-покупки, якщо сайт є підозрілим, не нададуть персональну інформацію та самостійно не будуть змінювати налаштування безпеки. Тобто можна припустити, що європейці намагаються вживати певні заходи безпеки, але найбільш дієвим з них надається

менша перевага. Це можливо тільки в умовах зниження інформованості населення щодо персональних заходів безпеки.

Проблема безпеки особистої інформації викликає занепокоєння у частини населення, особливо в частині неправомірного використання особистих даних (рисунок 3.7).

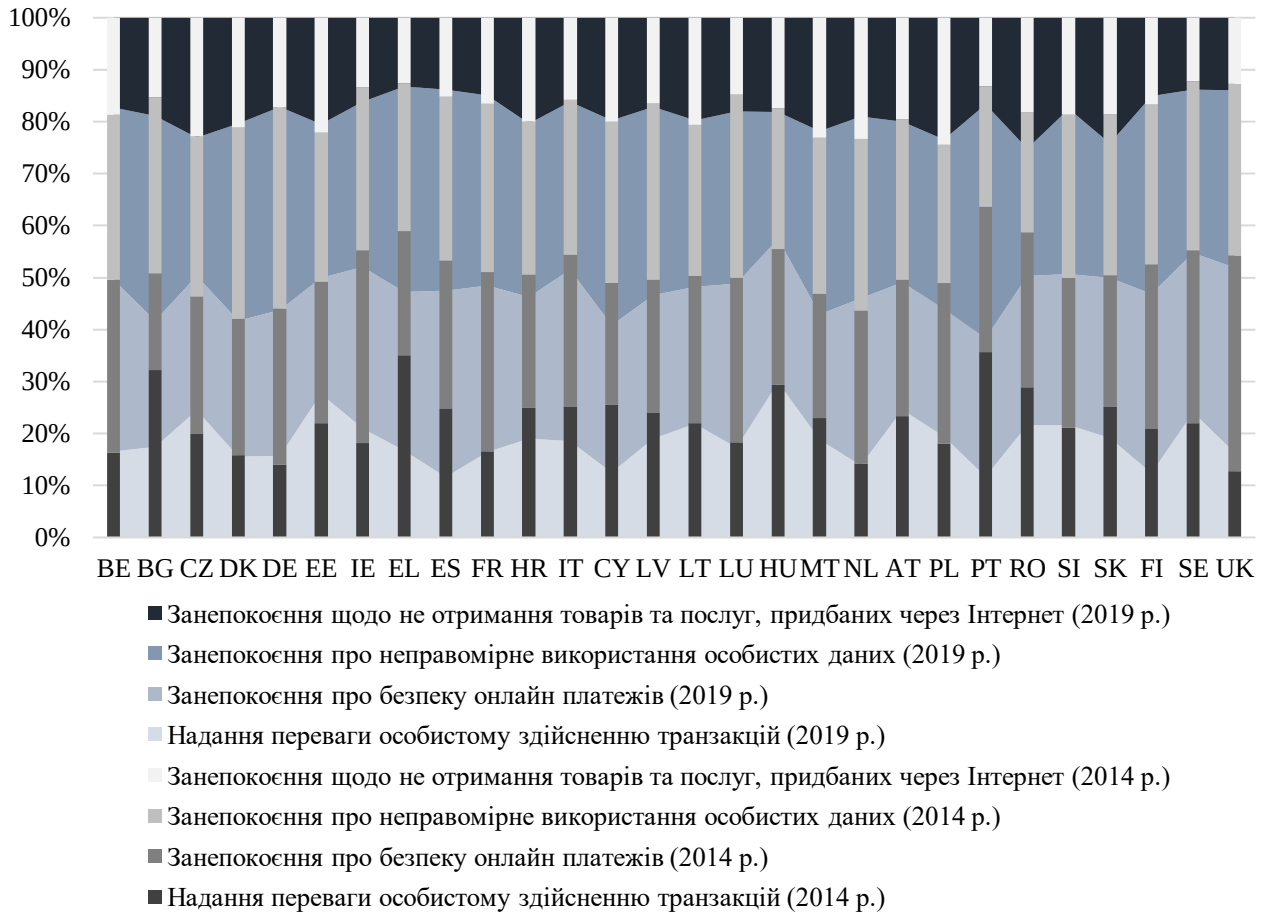


Рисунок 3.7 – Відсотки респондентів із країн ЄС, що занепокоєні персональною безпекою у 2014 та 2019 роках

Джерело: складено авторкою на основі [220, 221]

Так, середній відсоток занепокоєних європейців щодо неправомірного використання їх персональної інформації у 2019 році становив 44%, що перевищило даний показник 2014 року (41%) (рисунок 3.7). Найбільша кількість серед опитуваних, які стурбовані даною проблемою, належить Кіпру (60%), Германії (57%), Греції (57%), Португалії (54%), Іспанії (53%), Ірландії (53%), Болгарії (52%). При цьому зростання кількості схвильованих респондентів в

середньому становило 4%. Наступною проблемою є забезпечення безпеки онлайн-платежів, про що повідомили 38% європейців. При чому дане середнє значення не змінилося у 2019 році у порівнянні із 2014 роком. Це питання є найбільш важливим для населення Ірландії (52%), Іспанії (49%), Бельгії (46%), Великобританії (46%), Нідерландів (44%), Греції (44%), Франції (43%), Кіпру (43%), Словенії (43%). 24% респондентів також занепокоєні щодо недоотримання товарів та послуг, придбаних через Інтернет. При цьому даний показник зріс на 1% у 2019 році у порівнянні із 2014 роком. Найбільша кількість опитуваних належить Румунії (35%), Чехії (32%), Кіпру (30%), Хорватії (30%), Мальті (28%), Словаччині (29%). Що стосується надання переваги особистому здійсненню транзакцій, то середнє значення респондентів знизилося у 2019 році на 5% та склало 24%, хоча найбільш занепокоєними є населення Угорщини (38%), Ірландії (35%), Чехії (34%), Швеції (33%), Словенії (32%), Естонії (31%), Румунії (30%), Литви (30%). В цілому спостерігається тенденція зростання стурбованості респондентів щодо їх персональної безпеки, хоча з іншого боку падає рівень їх персонального захисту.

Проаналізуємо інформацію щодо інцидентів, які відбувалися із респондентами, в результаті чого вони ставали жертвами інформаційних та кіберзагроз. Так, на рисунку 3.8 представлено відсоткове співвідношення опитаних, яке характеризує факт того, чи становилися вони об’єктом загрози щодо викрадення особистих даних, чи ні. Спостерігається зниження кількості жертв інцидентів в середньому на 1% у 2019 році у порівнянні із 2014 роком, що є позитивною тенденцією. Але можна відмітити, що для таких країн, як Угорщина (12%), Австрія (11%), Румунія (11%), Хорватія (10%) та Люксембург (10%), є характерним найбільша кількість жертв даного виду інформаційних загроз. Країнами із найменшим рівнем є: Португалія (1%) та Литва (1%). Для всіх інших значення даного показника варіюється від 2 до 9%.

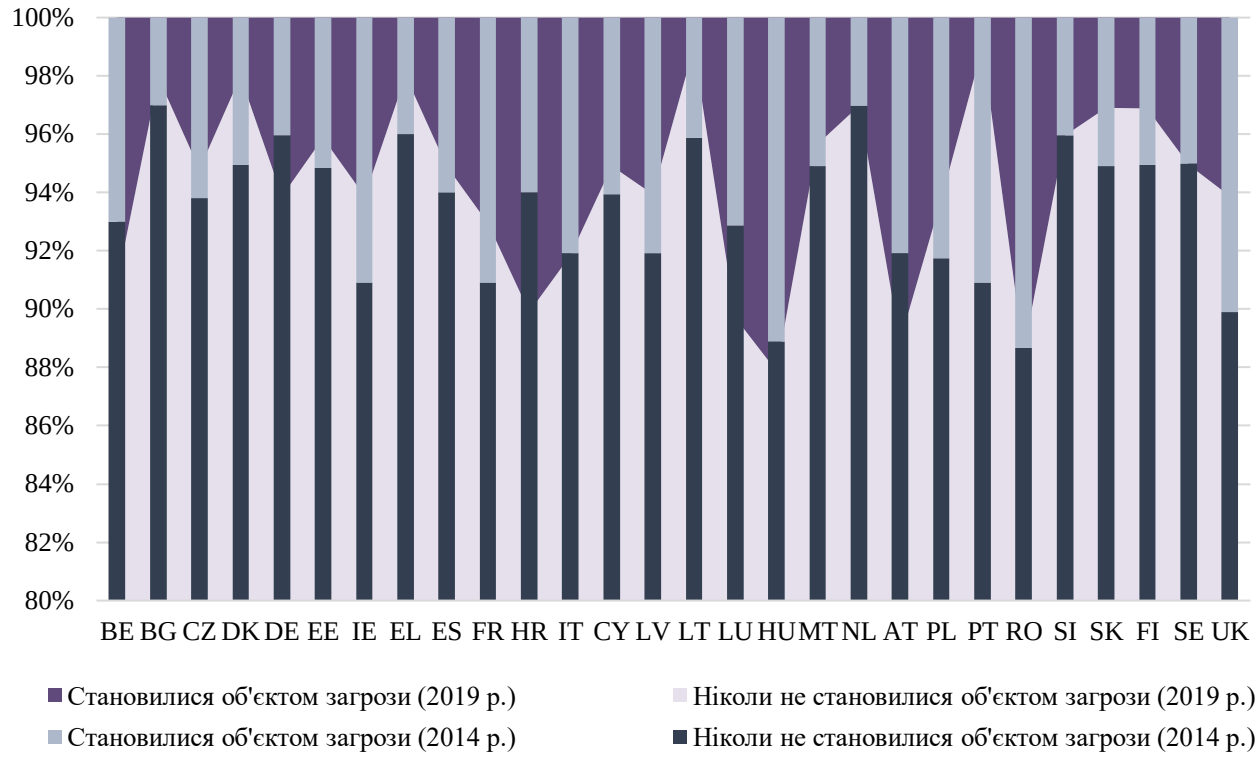


Рисунок 3.8 – Відсотки респондентів, які ставали жертвою викрадення особистих даних у 2014 та 2019 роках

Джерело: складено авторкою на основі [220, 221]

На рисунку 3.9 представлено співвідношення респондентів, які були або не були жертвою фішингу чи соціальної інженерії. У даному випадку ситуація дещо інша, оскільки спостерігається зростання кількості жертв на 2%. Але у деяких країнах кількість ошуканого населення досягало 72%, що характерно для Данії. Також високий рівень опитаних, які постраждали від даного виду загроз, серед таких країн як: Швеція (60%), Нідерланди (59%), Франція (47%), Німеччина (46%), Ірландія (46%). Найменший рівень постраждалих від соціальної інженерії характерний для населення Португалії (5%) та Греції (9%). Якщо аналізувати даний показник у порівнянні із 2014 роком, то практично для усіх країн він зріс, причому для Фінляндії (+23%), Німеччини (+14%) та Бельгії (+13%) він збільшився досить суттєво. Але спостерігається зменшення кількості ошуканих респондентів Португалії (-15%), Румунії (-8%), Греції (-8%), Мальти (-8%), Литви (-6%), Польщі (-6%), Словаччини (-3%), Італії (-2%), Словенії (-2%). Слід відмітити, що ймовірно такий розкид є результатом того, що об’єктами

інформаційних загроз є більш економічно активне населення країн із розвинутою економікою. Даний показник склав 38% у 2019 році для населення у віці 25-39 років та 37% для респондентів у віці 40-54 років. Також можна зазначити, що жертвами стали опитувані, що є самозайнятими (41%) або займають керівні позиції (49%). Також 53% з них відносять себе до вище середнього класу та 47% – до вищого [221]. Тобто можна зробити припущення, що найбільш привабливими для кіберзлочинців в плані фішингу та соціальної інженерії є фінансово забезпечені особи з найбільш розвинутих країн.

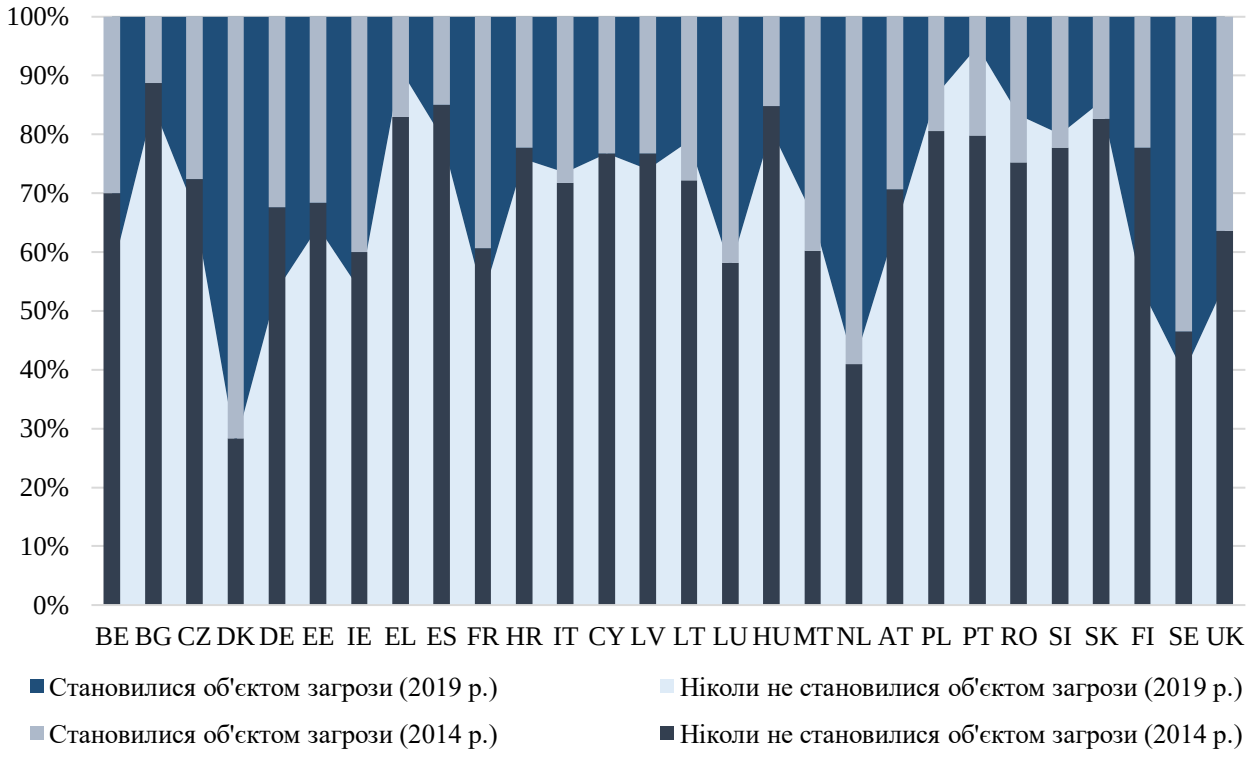


Рисунок 3.9 – Відсотки респондентів, які ставали жертвою фішингу або соціальної інженерії у 2014 та 2019 роках

Джерело: складено авторкою на основі [220, 221]

Проведемо аналіз інформації щодо інцидентів, пов’язаних із не отриманням доступу до онлайн-послуг через кібератаки. Так, на рисунку 3.10 можна побачити позитивну тенденцію щодо зниження кількості жертв у 2019 році у порівнянні із 2014 роком, що у середньому становило -6%.

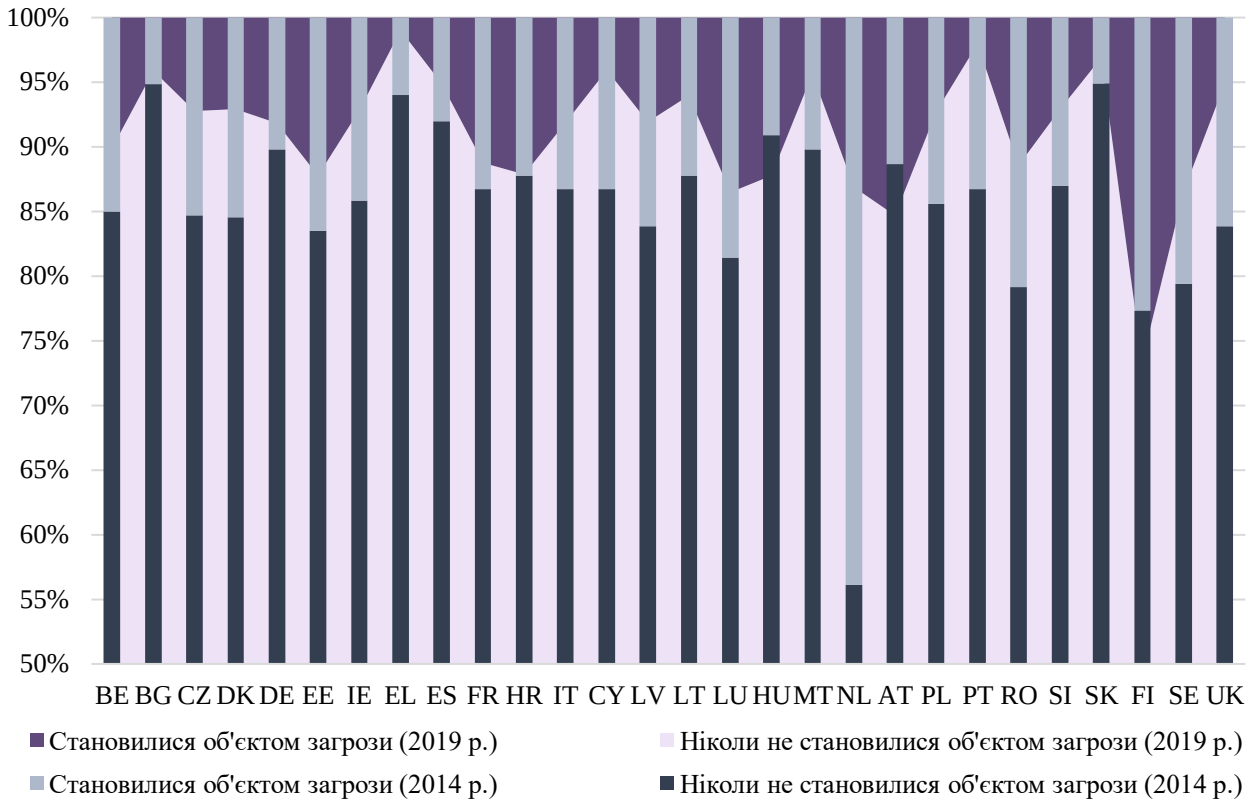


Рисунок 3.10 – Відсотки респондентів, які не змогли отримати доступ до онлайн-послуг через кібератаки у 2014 та 2019 роках

Джерело: складено авторкою на основі [220, 221]

Суттєве зниження даного показника відбулося у Нідерландах (-30%), Португалії (-11%) та Великобританії (-11%). Для респондентів Угорщини його значення за 6 років залишилося на тому самому рівні. Можна відмітити, що дана проблема є актуальною тільки для від 1% до 25% опитаних, при чому найбільше значення характерно для жителів Фінляндії (25%), Австрії (15%), а найменше – для Греції (1%) та Португалії (2%).

Що стосується інцидентів, пов’язаних із шахрайствами в онлайн-банкінгу та банківськими картками, то тут спостерігається зростання кількості респондентів, що стали жертвами даного виду (рисунок 3.11).

Хоча в середньому кількість ошуканого населення у 2019 році не змінилося по відношенню до 2014 року, але можна відмітити, що у ряді країн рівень даного показника збільшився.

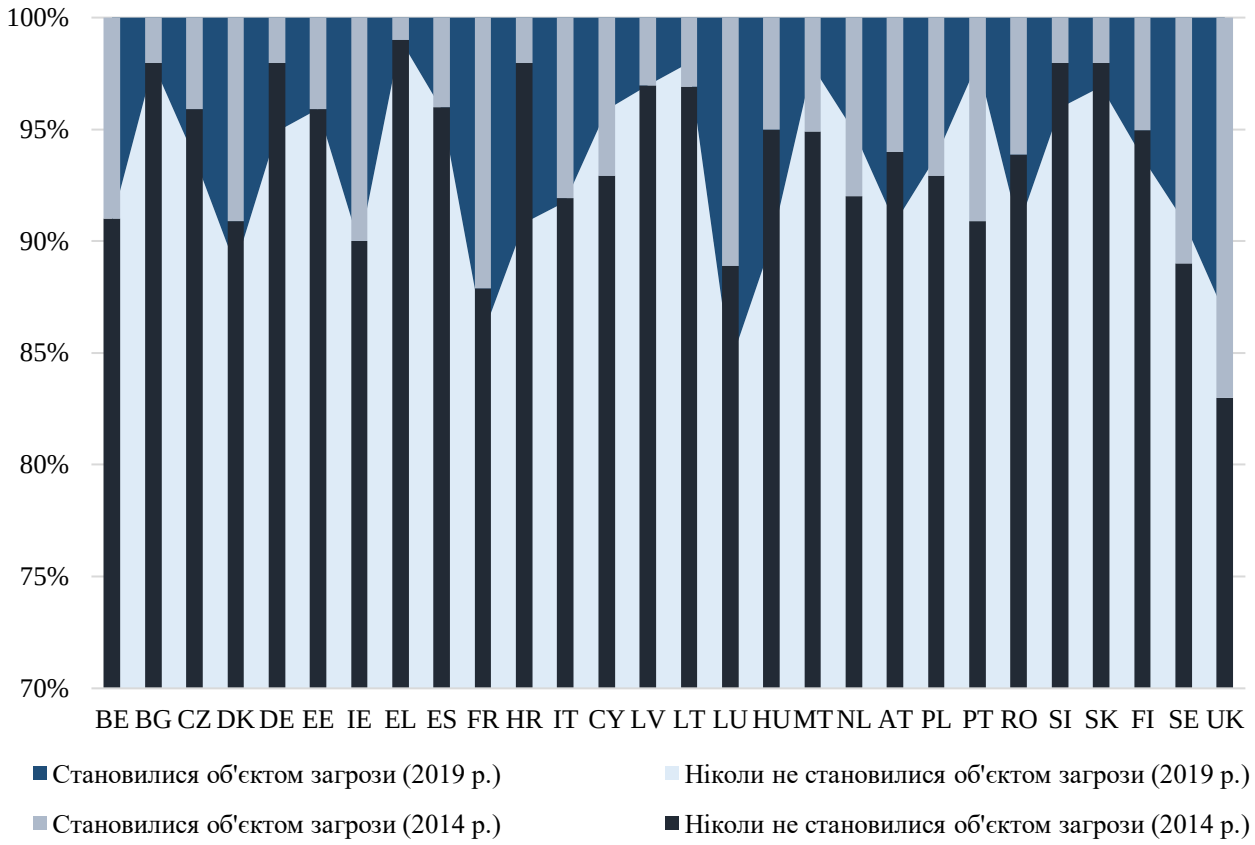


Рисунок 3.11 – Відсотки респондентів, які стали жертвами шахрайств в онлайн-банкінгу або із банківськими картками у 2014 та 2019 роках

Джерело: складено авторкою на основі [220, 221]

Це відбулося у Хорватії (+7%), Угорщині (+5%), Люксембурзі (+4%), Австрії (+3%), Германії (+3%), Румунії (+3%), Франції (+2%), Чехії (+2%), Данії (+2%), Словенії (+2%), Словаччині (+1%), Фінляндії (+1%). Для жителів Португалії (-7%), Великобританії (-4%), Кіпру (-3%), Мальти (-3%), Нідерландів (-3%), Швеції (-2%), Литви (-1%), Польщі (-1%) рівень постраждалих від шахрайств із банківськими картками знизився. Найбільший відсоток жертв – це респонденти у віці 40-54 роки (9%). Опитувані у віці 25-39 років склали 8%, 55 років та вище – 8%, 15-24 років – 6%. Найвищий відсоток постраждалих відноситься до професійної категорії топ-менеджменту (11%), а також є представниками вищого класу (11%) та тими, хто мають рівень достатку вище середнього (11%) [221].

На рисунку 3.12 представлено відсотки респондентів, які мали інциденти, пов’язані із вірусними атаками або знаходили вірусне програмне забезпечення на власних пристроях.

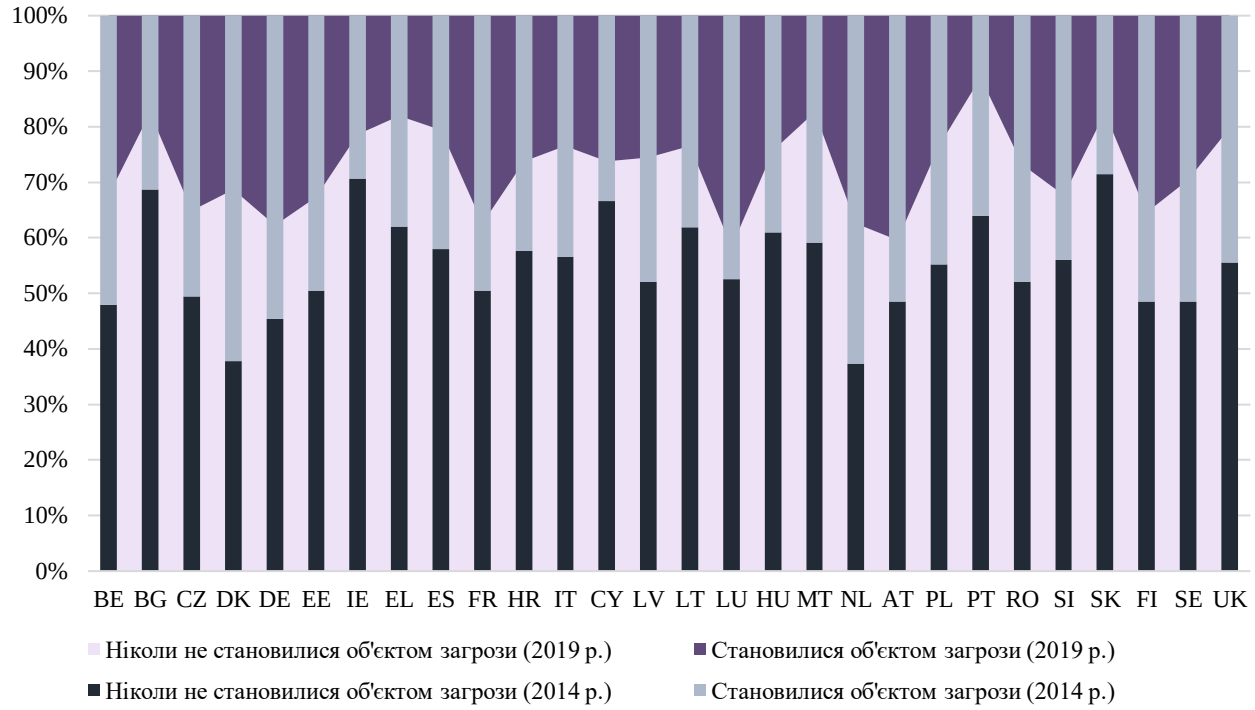


Рисунок 3.12 – Відсотки респондентів, які стали жертвами вірусної атаки у 2014 та 2019 роках

Джерело: складено авторкою на основі [220, 221]

На рисунку 3.12 можна чітко побачити, що за 6 років відбулося значне зниження кількості опитуваних, що мали дану проблему. Так, у 2014 році максимальне значення даного показника серед країн ЄС сягало 62%, що було характерним для жителів Нідерландів. Такі країни, як Данія (61%), Німеччина (54%), Бельгія (52%), Австрія (51%), Фінляндія (51%), Швеція (51%), Чехія (50%), мали кількість респондентів-жертв інциденту, яка перевищувала 50%. Найменша кількість постраждалих була у Словаччині (28%) та Ірландії (29%). Для всіх інших даний показник коливався в межах від 31% до 49%. Відповідно у 2019 році кількість опитуваних, що зіткнулися із такою проблемою, значно знизилася. В середньому по всім країнам даний показник зменшився на 17%. Максимальне значення було характерним для жителів Австрії (40%),

Люксембургу (40%), Німеччини (37%), Франції (37%), Нідерландів (37%), Фінляндії (34%), Чехії (34%), Словенії (32%), Бельгії (32%), Естонії (32%), Данії (31%). Відсоток респондентів таких країн, як Португалія (11%), Мальта (16%), Бельгія (17%), Словаччина (17%), Греція (18%), має найнижче значення. Оскільки попередньо було встановлено, що відбувається зниження використання антивірусного програмного забезпечення серед опитуваних, то зменшення кількості інцидентів на даному тлі може говорити тільки про те, що це ймовірно пов'язано із зростанням рівня захисту операційних систем, встановлених на пристроях. Також високий рівень випадків є характерним для молоді у віці 15-24 років (32%) та людей віком 35-44 років (32%). Серед інших опитуваних даний відсоток є нижчим. Найбільша кількість жертв даного виду інцидента відноситься до категорії менеджменту (37%), студентів (31%), самозайнятих (30%) та «білих комірців» (30%). При цьому більшість респондентів є представниками класу з рівнем достатку вище середнього (37%) [221]. Тобто підтверджується, що проблема вірусних атак у більшій мірі охоплює економічно активне населення із стабільним та високим доходом, хоча даний від інцидентів є характерним й для молодих людей, студентів, які ймовірно не мають додаткових коштів для використання антивірусних програм або останніх версій операційних систем.

Проаналізуємо інформацію щодо інцидентів, пов'язаних із зламуванням поштового акаунту або акаунту соціальних мереж (рисунок 3.13). Можна відмітити, що по даному виду випадків у 2019 році спостерігається зниження у порівнянні із 2014 роком. В середньому воно склало -2%. Це відбулося серед респондентів таких країн, як Португалія (-10%), Мальта (-9%), Греція (-6%), Великобританія (-6%), Бельгія (-5%), Нідерланди (-5%), Румунія (-5%), Данія (-4%), Іспанія (-4%), Італія (-4%), Литва (-4%), Польща (-2%), Болгарія (-1%), Ірландія (-1%). Але в деяких країнах відбулося зростання кількості опитуваних, які зіткнулися з подібним інцидентом, а саме: Франції (+5%), Австрії (+3%), Німеччині (+2%), Естонії (+1%), Угорщині (+1%), Фінляндії (+1%), Швеції (+1%).

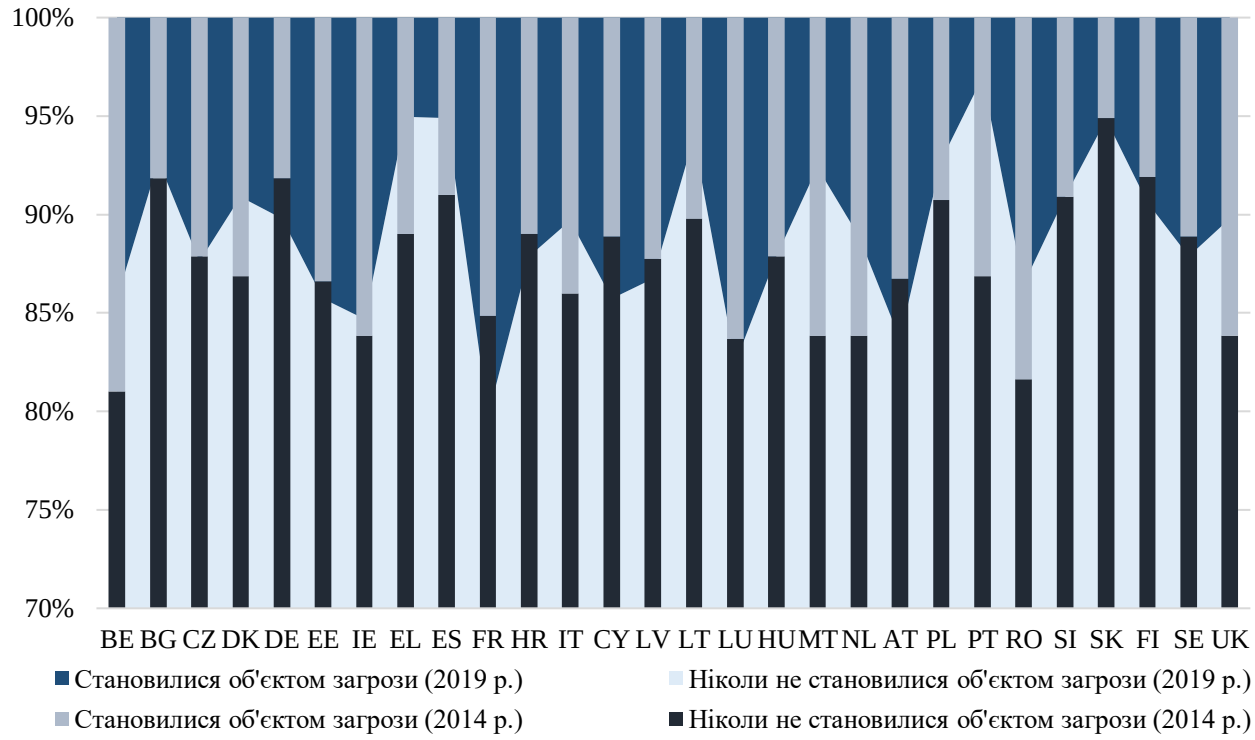


Рисунок 3.13 – Відсотки респондентів, які стали жертвами зламування поштового акаунту або акаунту соціальних мереж у 2014 та 2019 роках

Джерело: складено авторкою на основі [220, 221]

Кількість жертв даного інциденту становила від 3% до 20% у 2019 році та від 5% до 19% у 2014 році, при чому більшість постраждалих були у віці від 15 до 24 років (15%). При врахуванні професійної категорії більшість належала до менеджменту (14%), студентів (13%) та безробітних (13%) [221].

На рисунку 3.14 представлено відсотки респондентів, яким було запропоновано здійснити платіж, щоб повернути контроль над пристроєм. Цей інцидент пов'язаний із вимаганням грошей, що відбувається у процесі вірусної хакерської атаки. Наприклад, найбільш відомим такого роду інцидентом був вірус “Petya”, який розповсюдився серед великих українських компаній у червні 2017 року, в результаті чого зловмисники заробили більше $10 000 за розблокування комп’ютерів та також вимагали близько $256 000 за передачу приватних ключів для здійснення дешифрування даних [91]. Аналогом даного вірусу також був “WannaCry”, який у травні 2017 році вразив компанії Іспанії,

Росії, України, Тайваню та Британську національну службу охорони здоров'я, в результаті чого зловмисникам вдалося заробити більше $6 000 [115].

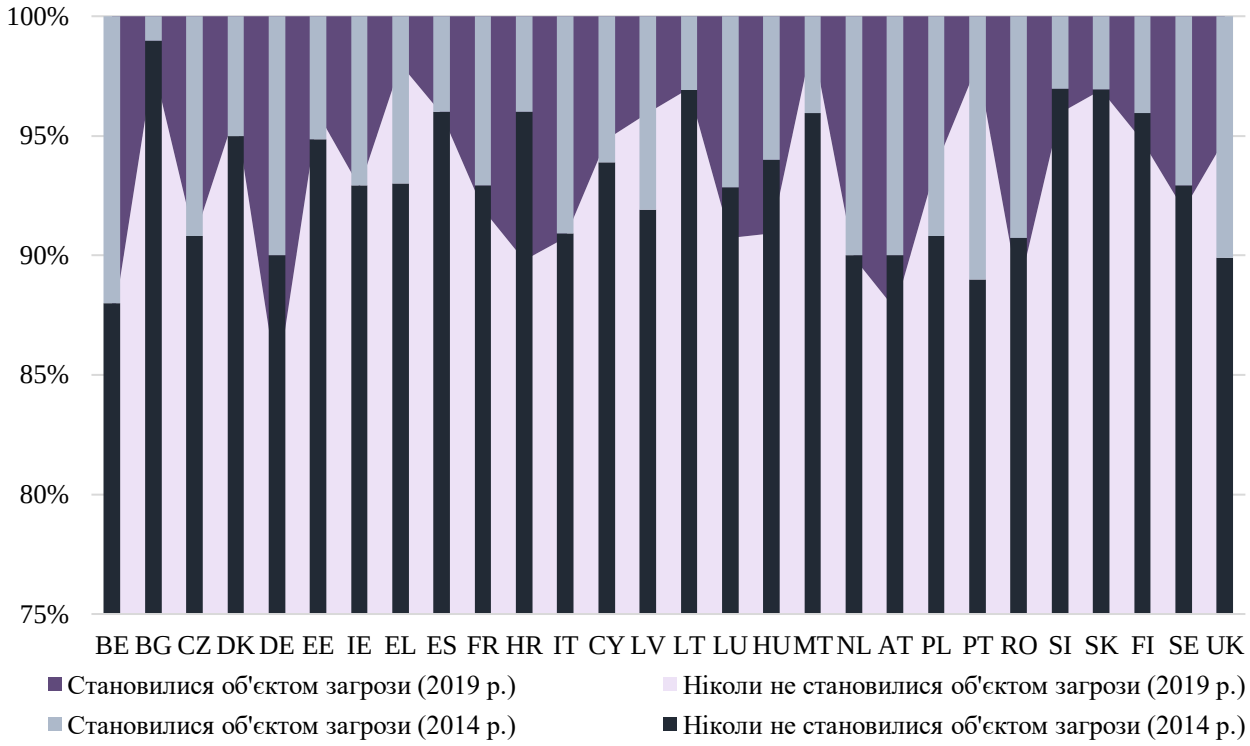


Рисунок 3.14 – Відсотки респондентів, яким було запропоновано здійснити платіж, щоб повернути контроль над пристроєм, у 2014 та 2019 роках
Джерело: складено авторкою на основі [220, 221]

На рисунку 3.14 можна побачити, що відсоток респондентів, які стали жертвами таких інцидентів, у 2019 році коливався від 1% до 15%, а у 2014 році – від 1% до 12%, хоча в середньому за 6 років змін по даному показнику не відбулося (0%). Слід відмітити, що кількість постраждалих у 2019 році збільшилася у таких країнах, як Хорватія (+6%), Німеччина (+5%), Угорщина (+3%), Австрія (+2%), Люксембург (+2%), Румунія (+2%), Бельгія (+1%), Болгарія (+1%), Франція (+1%), Словенія (+1%), Фінляндія (+1%), Швеція (+1%). Рівень даного показника для Португалії (-9%), Великобританії (-5%), Греції (-5%), Латвії (-4%), Мальти (-3%), Польщі (-3%), Данії (-1%), Естонії (-1%), Чехії (-1%) знизився у порівнянні із 2014 роком. Найбільш схильними до таких вірусних атак були самозайняті (11%) та представники менеджменту (10%) [221].

Результати проведеного аналізу свідчать про існування спільних рис для груп країн щодо застосування персональних заходів інформаційної безпеки та наслідками, які є результатами різного роду інцидентів. Це дозволяє сформувати гіпотезу щодо існування стійких національних патернів заходів забезпечення персональної інформаційної безпеки і наслідків її порушення, які сформувалися під впливом схожих тенденцій економічного добробуту населення. Для її доведення проведемо кластерний аналіз методом k-середніх (k-means clustering), суть якого полягає у розподілі спостережень на певні групи таким чином, щоб кожна з них відповідала певному кластеру з найближчим середнім значенням [172, с. 281]. Тобто при розподілі дані групи формуються з урахуванням їх подібності та мінімізації відстані кожної точки даних у групі із середнім значенням їх центроїда, що називається евклідовою відстанню та визначається за формулою (3.1) [65]:

$$J = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^{(j)} - c_j \right\|^2, \tag{3.1}$$

де J – цільова функція центроїда кластера;

c – центроїд кластера;

x – точка даних, з якої починається визначення евклідової відстані;

k – кількість кластерів;

j – скупчення;

n – кількість випадків;

i – випадок.

Алгоритм k-середніх передбачає виконання наступних кроків [63]:

1) випадковим чином ініціалізуються та відбираються k–кластери;

2) ініціалізуються центроїди, для чого відбувається перемішування даних, а потім випадковим чином вибираються k–точки даних для центроїдів;

3) обчислюється евклідова відстань між точками даних та усіма центроїдами, де призначається точка найближчому кластеру, та обчислюється

центроїд всіх точок шляхом визначення середнього значення всіх точок, які належать даному кластеру, за формулою (3.2) [93]:

$$c_i = \frac{1}{n}\sum_{j=i}^{n} x_i^{(j)}; \quad (3.2)$$

4) алгоритм виконується до тих пір, поки центроїди не будуть змінені, тобто присвоєння точок кластерам не буде змінюватися.

Для проведення розрахунків сформуємо таблицю із вхідними даними (див. табл. Д.1 додатку Д), яка буде включати інформацію щодо кількості респондентів-жителів європейських країн, які вживають різні заходи безпеки, та кількості опитаних, що були жертвами інцидентів. Результати аналізу були представлені на рисунках 3.4–3.6 та 3.8–3.14. Кластеризацію будемо проводити із використанням аналітичної платформи «Deductor Academic», яка дозволяє застосовувати сучасні методи аналізу та візуалізації даних [345]. Після завантаження даних важливо поділити їх на вхідні та вихідні. З цією метою було зазначено у якості вхідних даних всі заходи персональної безпеки, у якості вихідних – показники, що характеризують постраждалих від інформаційних інцидентів. В процесі налаштування було враховано:

- розбиття масиву даних на навчальну вибірку (95%) та тестову (5%);
- спосіб розподілу початкових даних – випадково;
- встановлення фіксованої кількості кластерів, яку було визначено експериментальним шляхом у кількості 7 за найменшою максимальною та середньою похибками кластеризації. Хоча збільшення кількості кластерів дає зменшення похибки, але також це призвело до формування кластерів із 1-го значення, що знижує якість кластеризації;
- проведення кластеризації.

Отримані зв’язки кластерів, діаграми розсіювання для вихідних даних, матриця порівняння та профілі кластерів наведені на рисунках Д.1-Д.10 додатку Д. На рисунку Д.1 можна побачити середні та максимальні похибки кластерів.

Оскільки експеримент відбувався для 2, 3, 4, 5, 6, 7 та 8 кластерів, то результати їх похибок представлені у таблиці 3.1.

Таблиця 3.1 – Середні значення похибок

Назва похибки	Кількість кластерів						
	2	3	4	5	6	7	8
Середнє значення максимальної похибки	1,0133	0,9673	0,6011	0,6122	0,6098	0,5454	0,4392
Середнє значення середньої похибки	0,6505	0,6247	0,3944	0,4666	0,4530	0,4123	0,3523

Із зменшенням кількості кластерів значення похибок знижуються, але було надано перевагу семикластерній моделі ніж восьмикластерній, тому що остання формує кластери із одного значення, що вже говорить про зниження якості кластеризації. Також чотирикластерна модель має досить непогані значення похибок, але один з її кластерів містить одне значення, тому вибір зупиняємо на семикластерній моделі. Діаграми розсіювання (рисунки Д.2 – Д.8 додатку Д) показують досить непогані результати, хоча є значення, які виходять за інтервали, але в цілому така картина є цілком придатною, що може обумовлюватися погрішністю вибірки та результатів опитування. Профілі кластерів відображають більш рівномірний розподіл значень по кожному з них (рисунок Д.10 додатку Д). Матриця порівнянь містить більшість значень, які перевищують 50%, що говорить про гарну якість моделі (рисунок Д.9 додатку Д).

На рисунку 3.15 представлений основний візуалізатор кластерної моделі – багатомірна діаграма результатів кластерного аналізу, яка показує кластери країн в залежності від співвідношення персональних заходів безпеки та наслідків інцидентів. 0-й кластер сформували – Чехія, Латвія, Мальта, Словенія та Словаччина; 1-й кластер – Бельгія, Естонія, Франція та Люксембург; 2-й кластер – Греція, Кіпр, Литва; 3-й – Ірландія, Австрія, Великобританія; 4-й –

Болгарія, Іспанія, Італія, Польща та Португалія; 5-й – Данія, Німеччина, Нідерланди, Фінляндія, Швеція; 6-й – Хорватія, Угорщина, Румунія.

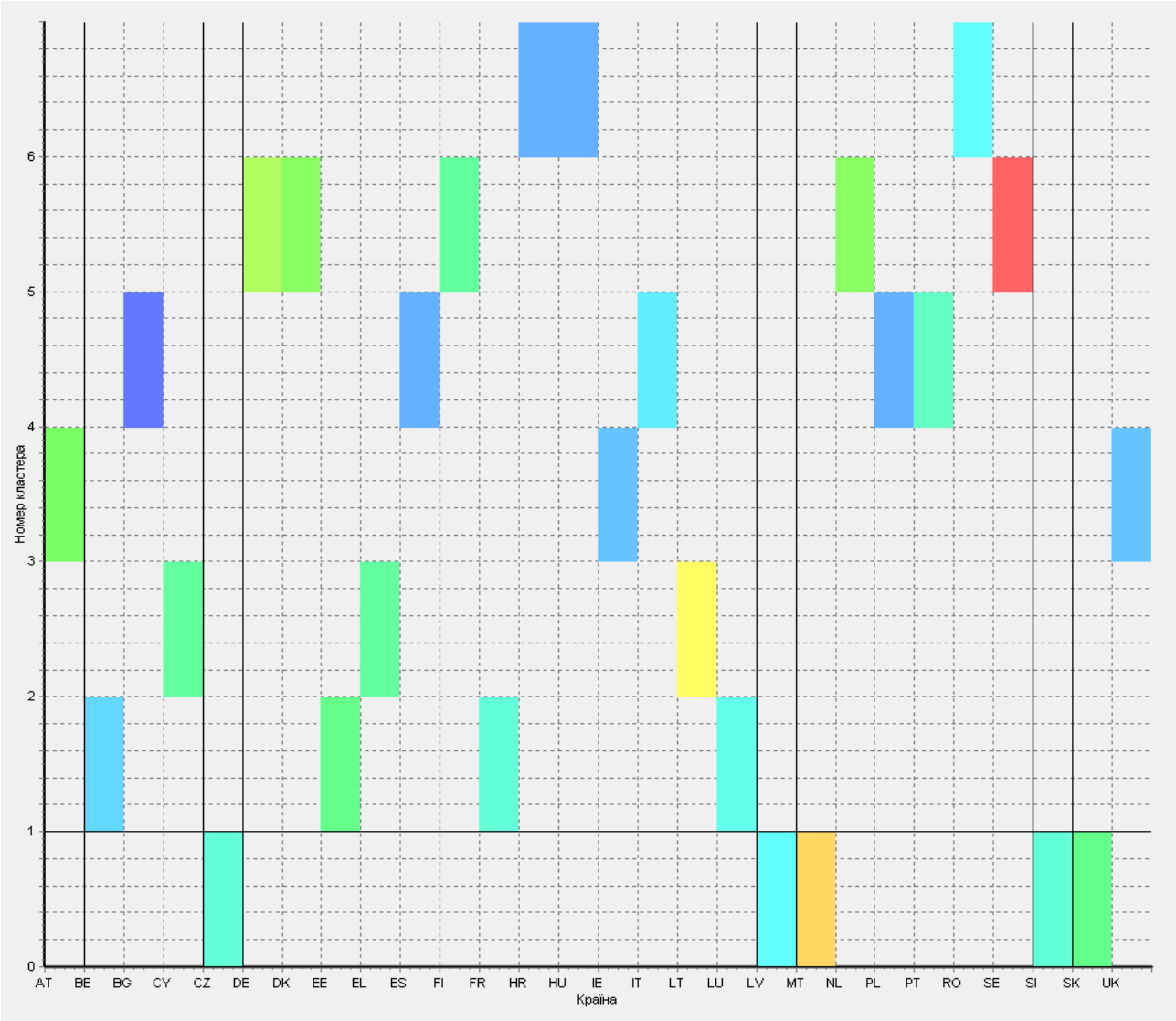


Рисунок 3.15 – Багатомірна діаграма результатів кластерного аналізу (складено авторкою)

Для кожного кластеру країн зазначимо рівень ВВП на душу населення, узятий за 2019 рік – рік проведення опитування [98], що дозволить підтвердити або спростувати гіпотезу про те, що настрої населення щодо використання засобів персональної інформаційної безпеки, результати якого призводять до появи схожих відповідних наслідків інформаційних інцидентів, сформувалися під впливом рівня добробуту, характерного для населення країн, близьких за

рівнем економічного розвитку (див. табл. 3.2).

Таблиця 3.2 – ВВП на душу населення країн, розподілених за кластерами

Назва країни	ВВП на душу населення, у поточних $US	Номер кластеру	Назва країни	ВВП на душу населення, у поточних $US	Номер кластеру
Латвія	32191,0	0	Болгарія	24789,6	4
Словаччина	34066,9	0	Польща	34431,2	4
Словенія	40983,4	0	Португалія	36639,3	4
Чехія	43299,6	0	Іспанія	42195,2	4
Мальта	46279,1	0	Італія	44248,2	4
Естонія	38915,2	1	Фінляндія	51426,0	5
Франція	49435,2	1	Швеція	55819,9	5
Бельгія	54904,7	1	Німеччина	56278,2	5
Люксембург	121292,7	1	Нідерланди	59554,2	5
Греція	30722,2	2	Данія	60178,5	5
Литва	38501,8	2	Хорватія	30140,8	6
Кіпр	41254,4	2	Румунія	32297,3	6
Великобританія	48698,1	3	Угорщина	34507,1	6
Австрія	58946,4	3	X	X	X
Ірландія	88240,9	3	X	X	X

Використовуючи дані таблиці 3.2, побудуємо візуалізацію даних (рисунок 3.16). Так, населення країн 6-го кластеру мають приблизно однаковий рівень ВВП на душу населення, який коливається в районі $30 140,8 – $34 507,1 (див. табл. 3.2). При цьому можна помітити, що територіально ці країни є близькими сусідами (рисунок 3.16). Для країн 5-го кластеру також є характерним приблизно однаковий рівень економічної активності населення, який перевищує його середнє значення серед аналізованих 28 країн ($47 508,47) та знаходиться в діапазоні $51 426,0 – $60 178,5 (див. табл. 3.2). На карті 3.16 чітко видно, що країни даного кластеру знаходяться у територіальній близькості. Країни 4-го кластеру мають досить широкий розкид у значеннях ВВП на душу населення ($24 789,6 – $44 248,2), хоча можна відмітити, що в середині кластеру Польща та Португалія мають приблизно однаковий рівень економічного добробуту ($34 431,2 та $36 639,3 відповідно), а також Іспанія та Італія ($42 195,2 та $44 248,2). Що стосується географічного розташування, то в межах даного кластеру Іспанія та Португалія є країнами-сусідами (рисунок 3.16).

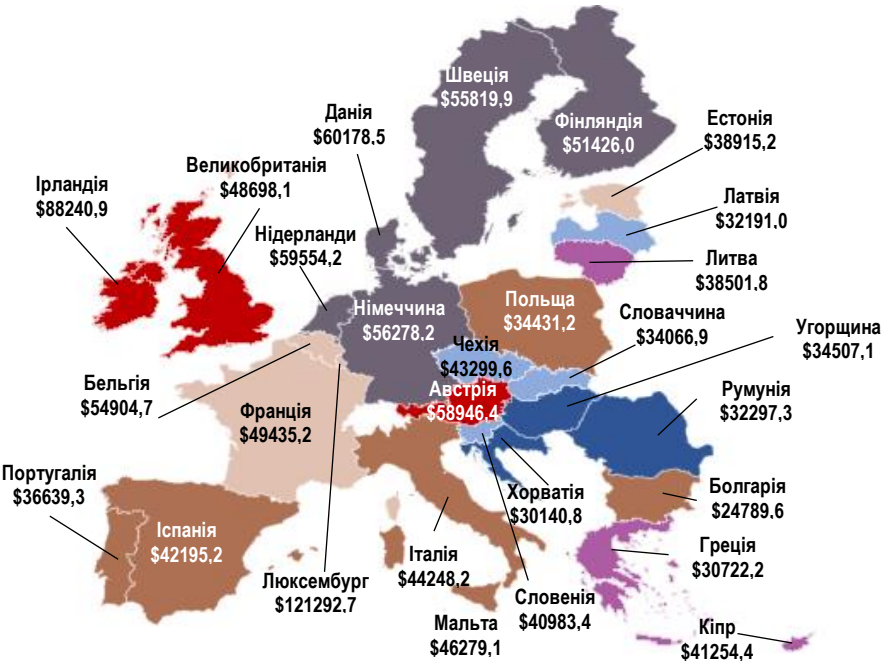


Рисунок 3.16 – Кластери країн (складено авторкою)

Населення країн 3-го кластеру також мають різний рівень якості життя населення, але їх значення перевищують середнє для усіх країн, що відносить їх до країн із високим рівнем розвитку. На карті 3.16 можна побачити, що дві країни мають територіальне сусідство – Великобританія та Ірландія. ВВП на душу населення країн 2-го кластеру знаходиться у межах $30 722,2 – $41 254,4, але Литва та Кіпр мають дуже близькі значення ($38 501,8 та $41 254,4 відповідно) (див. табл. 3.2). Також Греція та Кіпр мають близьке територіальне сусідство (рисунок 3.16). Показник економічного розвитку країн 1-го кластеру має найбільшу розбіжність. Для даної групи характерним є самий високий рівень економічної активності, що відповідає Люксембургу ($121 292,7), та самий низький – Естонії ($38 915,2). Не дивлячись на таку розбіжність, три країни в середині кластеру є країнами-сусідками із загальними кордонами – Франція, Бельгія та Люксембург (рисунок 3.16). Що стосується 0-го кластеру, то сюди увійшли країни із рівнем ВВП на душу населення нижче середнього рівня, хоча діапазон є досить широкий – $32 191,0 – $46 279,1 (див. табл. 3.2). У середині кластеру сформувалося дві групи, які мають близькі значення даного

показника – це Латвія, Словаччина та Словенія, Чехія, Мальта. При цьому Словенія, Словаччина та Чехія є країнами-сусідками (рисунок 3.16).

Виходячи з отриманих даних, можна зробити висновок, що настрої населення, пов'язані із використанням персональних заходів безпеки та отриманням відповідних наслідків інформаційних та кіберінцидентів, формуються під впливом рівня економічного розвитку країни та під впливом ментальних особливостей, сформованих завдяки близькому територіальному розташуванню країн-сусідок, що мають спільні кордони, історичні події, близькі культурні особливості (наприклад, Іспанія та Португалія; Великобританія та Ірландія; Греція та Кіпр; Фінляндія, Швеція, Німеччина, Нідерланди та Данія; Франція, Бельгія та Люксембург; Угорщина та Румунія). Тобто для цих країн є спільні риси, які характеризують відношення населення до організації власної інформаційної безпеки, формування самосвідомості та обізнаності щодо можливих наслідків. Сформульована вище гіпотеза є доведеною, але вона повинна також враховувати й вплив ментальних особливостей, сформованих історичною та географічною близькістю країн.

На останок проаналізуємо результати опитування європейців щодо їх думки стосовно факту зростання ризику стати жертвою кіберзлочину. Так, у 2019 році від 65% до 93% респондентів вважали, що ризик стати об'єктом інциденту зростає, а від 6% до 31% – не погоджувалися із цим (рисунок 3.17). У 2014 році від 70% до 94% опитаних допускали можливість збільшення рівня ризику для них, з іншого боку від 4% до 28% - не погоджувалися із цим (рисунок 3.17). Можна відмітити, що кількість респондентів, що думають негативно, знизилася практично у всіх країнах, окрім Болгарії (+8%), Польщі (+8%), Ірландії (+4%), Литви (+4%) та Естонії (+2%), що говорить про позитивні тенденції у напрямі із персональною безпекою. 85% європейців у віці 35-44 років досить критичні у цьому питанні, 16% опитаних у віці 15-24 не погоджуються із цим. Найбільш гострою є дана проблема для менеджменту компаній (87%), найменш критичною вона є для студентів (17%). Підвищення ризику стати жертвою кіберзлочину є

актуальним питанням для представників, які належать до найвищого класу по розподілу доходів (80%) та вище середнього (85%) [221].

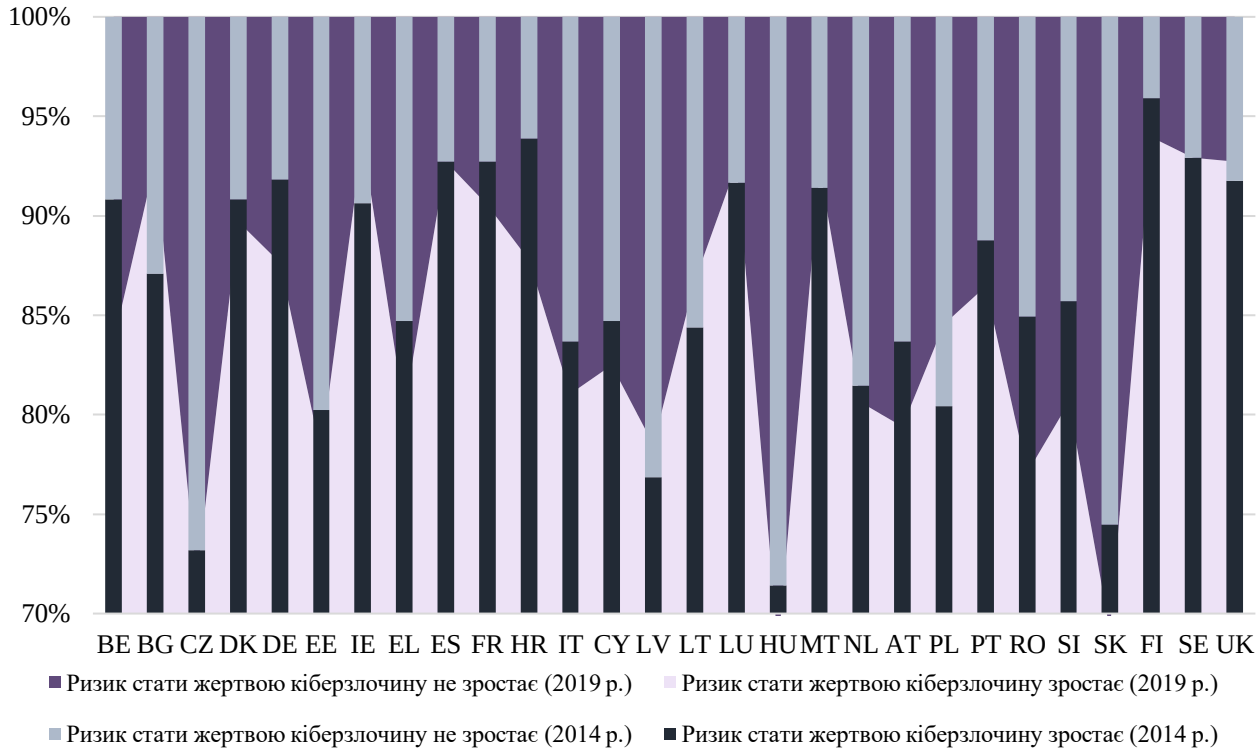


Рисунок 3.17 – Відсотки респондентів, які вважають, що ризик стати жертвою кіберзлочину зростає або не зростає, у 2014 та 2019 роках

Джерело: складено авторкою на основі [220, 221]

Хоча й спостерігається зниження кількості респондентів, яких хвилює зростання ризику стати об’єктом кіберінциденту, але при цьому зростає кількість опитуваних, які не можуть в достатній мірі забезпечити свій персональний кіберзахист. Тобто виникає певний парадокс, який можна пояснити тільки тим фактом, що ймовірно в процесі проведення опитування респонденти не пов’язували факт власного захисту із ризиком стати жертвою кіберзлочину. Так, в середньому відбулося зростання на 15% кількості європейців, які не можуть захистити себе у достатній мірі. У 2014 році від 49% до 89% респондентів вважали, що вони мають необхідний захист свої пристроїв, а від 9% до 39% – відповіли, що не мають (рисунок 3.18).

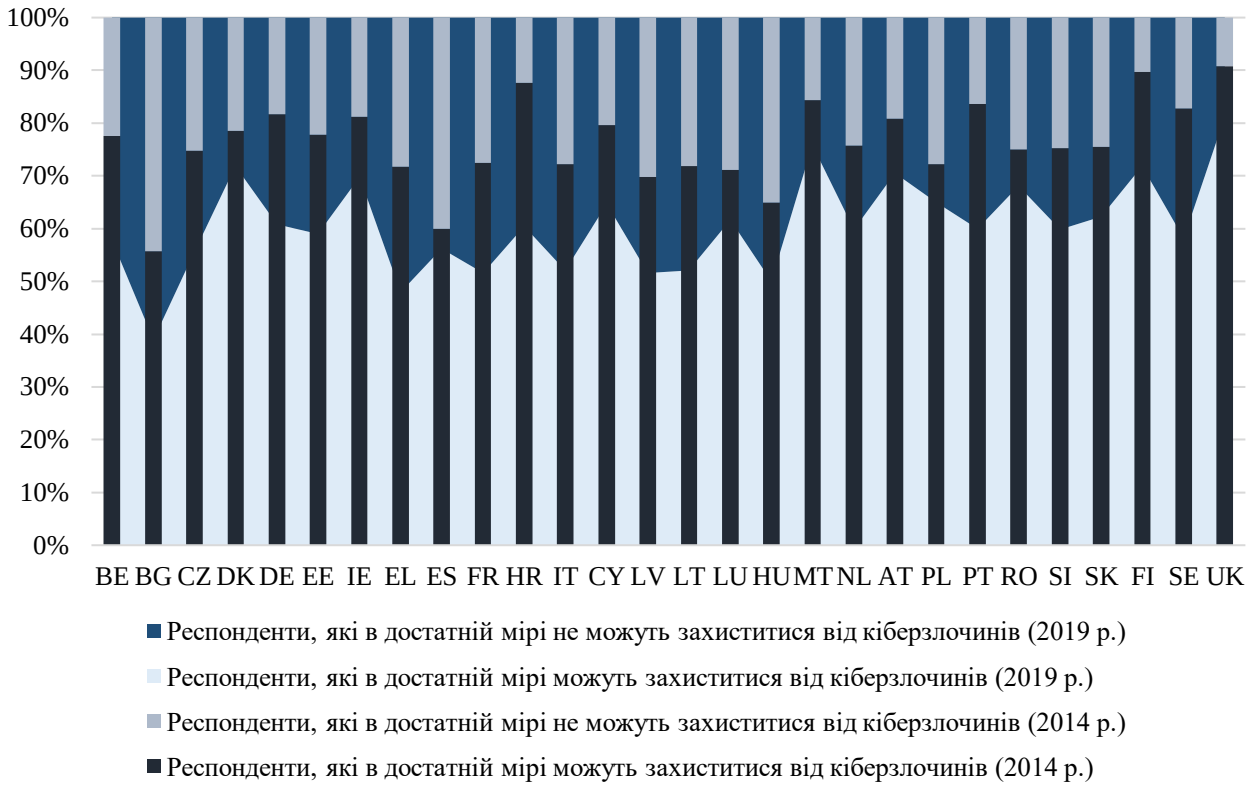


Рисунок 3.18 – Відсотки респондентів, які вважають, що можуть або не можуть захиститися у достатній мірі від кіберзлочинів, у 2014 та 2019 роках

Джерело: складено авторкою на основі [220, 221]

У 2019 році відбулися значні зміни у настроях європейського населення, що привело до таких співвідношень: 37% – 78% впевнені у достатності власного інформаційного захисту, а 18% – 58% – не впевнені. Найбільший ріст характерний для таких країн, як Хорватія (+26%), Швеція (+24%), Греція (+23%), Португалія (+22%), Німеччина (+20%). Найменше збільшення відбулося у Іспанії (+4%), Данії (+6%), на Мальті (+7%), у Люксембурpps (+8%), Польщі (+8%), Австрії (+9%) та Великобританії (+9%). Найбільша кількість опитуваних, які можуть себе захистити, знаходяться у віці 15-24 років (67%) та 25-39 років (65%), ті, які не можуть достатньо себе захистити – це населення у віці 40-54 років (40%) та вище 55 років (40%). Серед професійних категорій найбільш захищеними себе вважають студенти (68%) та менеджери (64%), найменш – домогосподарі (40%), пенсіонери (39%), офісні працівники (39%), працівники фізичної праці (38%) [221].

Узагальнення ключових аспектів запропонованої методології дослідження закономірностей формування в національній економіці домінуючих моделей забезпечення персональної інформаційної безпеки населення та представлення результатів її реалізації можна побачити на рисунку 3.19.

Заходи персональної ІБ, які застосовує населення країн ЄС (вхідні параметри)	**Наслідки кіберінцидентів, характерні для населення країн ЄС (вихідні параметри)**
1) свідоме надання переваги / відмова від придбання продуктів і послуг он-лайн; 2) свідоме надання переваги / відмова від використання онлайн-банкінгу; 3) свідоме надання / відмова в наданні власної інформації на вебсайтах; 4) персональна зміна налаштувань безпеки; 5) відвідування лише надійних сайтів; 6) використання різних паролів для різних сайтів; 7) ігнорування електронних листів із незнайомих адрес; 8) використання лише власного комп'ютера; 9) використання антивірусних програм; 10) скасування онлайн-покупок через підозри до сайту; 11) регулярна зміна паролів	Стали жертвою: 1) відмови в доступі до онлайн-послуг через кібератаки; 2) викрадення особистих даних; 3) фішингу або соціальної інженерії; 4) зламування поштового акаунта або акаунта соціальних мереж; 5) шахрайств в онлайн-банкінгу або з банківськими картками; 6) якій було запропоновано здійснити платіж, щоб повернути контроль над пристроєм; 7) вірусної атаки

Проведення кластерного аналізу методом k-means:

1) ініціалізація випадково та відбір k-кластерів; 2) ініціалізація центроїдів за допомогою перемішування даних та відбору випадково k-точок даних для центроїдів; 3) обчислення евклідової відстані між точками даних та усіма центроїдами; 4) призначення точки найближчому кластеру та обчислення центроїда всіх точок за допомогою визначення середнього значення тих, які належать цьому кластеру; 5) виконання алгоритму доти, поки центроїди не будуть змінені.

Результати кластерного аналізу

№ кластеру	Склад кластеру	Характерні заходи персональної ІБ*	Країни з кластеру, що є близькими за рівнем ВВП на душу населення	Країни з кластеру, що є близькими за географічним розміщенням
0	Латвія, Словаччина, Словенія, Чехія, Мальта	**1**, 2, 3, 4, 8, 10	1) Латвія, Словаччина; 2) Чехія, Словенія; 3) Чехія, Мальта	Словаччина, Словенія, Чехія
1	Естонія, Франція, Бельгія, Люксембург	5, **7**, 8, 9	Франція, Бельгія	Франція, Бельгія, Люксембург
2	Греція, Литва, Кіпр	**1**, **2**, 3, 4, **5**, 6, **8**	Литва, Кіпр	Греція, Кіпр
3	Великобританія, Австрія, Ірландія	2, 4, **11**	Великобританія, Австрія	Великобританія, Ірландія
4	Болгарія, Польща, Португалія, Іспанія, Італія	3, 4, 5, 6, 7, **8, 9**, 10, 11	1) Іспанія, Італія; 2) Польща, Португалія	Португалія, Іспанія
5	Німеччина, Нідерланди, Фінляндія, Швеція, Данія	1, **2**, **3**, **4**, **6**, **7**, 8, **9**, **10**	Фінляндія, Швеція, Німеччина, Нідерланди, Данія	Фінляндія, Швеція, Німеччина, Нідерланди, Данія
6	Хорватія, Румунія, Угорщина	2-**5**, **6**, **7**, 8, **9**, **11**	Хорватія, Румунія, Угорщина	Хорватія, Румунія, Угорщина

* Нумерація заходів ІБ відповідно до переліку вхідних параметрів; виділені ті, що переважають для кластеру (більше ніж 90 %)

Рисунок 3.19 – Методологія та результати кластерного аналізу країн ЄС за 2019 р. щодо зв’язку заходів персональної інформаційної безпеки (ІБ) та наслідків кіберінцидентів (складено авторкою)

Таким чином, отримані результати аналізу персональних заходів безпеки та наслідків кіберзагроз для населення країн ЄС, а також підтвердження гіпотези щодо впливу рівня економічного розвитку та національних традицій на формування стійких національних патернів заходів забезпечення персональної інформаційної безпеки, дозволяють зробити висновки щодо можливості екстраполяції даних результатів також й для України. На нашу думку, українське населення має спільні характеристики із населенням Білорусії, Молдови та Російської Федерації щодо використання заходів персональної безпеки завдяки близькому рівню добробуту та географічному положенню, що в подальшому можна використати для визначення ключових проблем стосовно персонального захисту населення.

Отримані висновки засвідчують, що в більшості випадків тенденції змін використання різного роду заходів персонального захисту відбуваються завдяки зниження обізнаності населення щодо кіберзлочинності та заходів боротьби із нею. Тому необхідно сформувати на державному рівні концепцію щодо підтримки освітньої діяльності населення для підвищення рівня його обізнаності із можливими інструментами інформаційного захисту. Це можливо в умовах розповсюдження дистанційного навчання, яке дозволяє охопити широке коло слухачів, а також знижує витрати на його організацію. При цьому не слід обмежувати освітні заходи віковою категорією слухачів або спрямовувати на окремі цільові групи, а зробити їх доступними для широких верств населення.

Окрім цього також рівень добробуту населення впливає на його можливості щодо придбання більш якісного програмного забезпечення та вживання різного роду інструментів захисту. У цьому питанні держава повинна також спрямовувати зусилля щодо надання можливостей для створення стартапів щодо розробки заходів безпеки для мало забезпечених верств населення, а також здійснення їх фінансування за рахунок бюджетних коштів або грантових програм. Такі заходи сприятимуть підвищенню довіри населення до державних органів як гаранту забезпечення національної та інформаційної безпеки у країні.

3.2 Вплив рівня кібербезпеки країни на її привабливість для легалізації кримінальних доходів

Розвиток світової економіки, досягнення економічного добробуту, підвищення стандартів життя та безпеки населення є безперечно пріоритетними питаннями сучасного світового співтовариства. Але поряд із цим становиться більше можливостей для забезпечення вільного руху грошей, джерелом отримання яких є незаконні фінансові операції, тероризм, шахрайство та інші кримінальні дії. Нелегальний оборот коштів та фінансування організованої злочинності стають головними проблемами, які загрожують економіці будь-якої країни. При цьому банківська система бере досить активну участь у цьому, оскільки саме вона забезпечує процес, який призводить до легалізації подібних фінансових операцій. Також система інформаційної безпеки (кібербезпеки) банку відіграє не останню роль, оскільки від рівня її організації та відповідності міжнародним стандартам залежить те, як швидко можна не допустити здійснення операцій із коштами, отриманими з незаконних джерел. Можна сказати, що високий рівень безпеки зменшує ризик фінансування тероризму із використанням банківської системи. Саме тому одним із завдань інформаційної безпеки є забезпечення безпеки транзакцій у банках з метою не допущення тих, які є незаконними.

Відслідковування фінансових операцій, джерелом походження яких є кримінальна діяльність, це прерогатива фінансового моніторингу, який здійснюється первинними суб’єктами (банками, страховими компаніями, ломбардами, тощо) та державою. Але проблема полягає в тому, що інколи такі суб’єкти зацікавлені у здійсненні подібних операцій, перевага від яких є вищою для них, ніж штрафні санкції, накладені за здійснення транзакцій із незаконними коштами. Хоча в будь-якій країні існує ряд законодавчих актів, які регламентують питання, пов’язані із здійсненням такого роду діяльності, але явище легалізації кримінальних доходів існує та набуває колосальних розмірів.

Останнім часом у міжнародному економічному співтоваристві багато зусиль спрямовано на вивчення та вимірювання взаємозв'язку між економікою, політикою, безпекою та організованою злочинністю. Ці дії повинні виходити за межі однієї країни для того, щоб відстежувати та блокувати нелегальні грошові потоки, де б вони не були приховані. Ефективних інструментів, які повністю дозволяють запобігати відмиванню грошей, не існує, що негативно впливає на економічну безпеку будь-якої країни. Тому потрібні методики, які дозволять не тільки на рівні економічних агентів впливати на процес легалізації кримінальних доходів, але й на рівні держави будувати прогнози та виявляти потенційні ризики фінансування тероризму однією країною в іншій. Саме для цього досить ефективним буде застосування гравітаційного моделювання. Даний підхід було розглянуто у праці Уолтера Ізарда "Location Theory and Trade Theory: Short-Run Analysis" (1954) для міжнародної торгівлі у міжнародній економіці. Його суть полягала у врахуванні географічного розподілу при територіальній проекції соціально-економічного життя суспільства, що дозволяло визначити кількісні характеристики економічного ландшафту населених пунктів через територіальні диспропорції розміщення промислових підприємств, транспортних вузлів, попиту та пропозиції на ринку праці, тощо.

У даній роботі буде використано методику гравітаційного моделювання для оцінки рівня привабливості країн для легалізації кримінальних доходів. При цьому її буде модернізовано з урахуванням рівня інформаційної безпеки країни, а також з виділенням тих ключових факторів, які впливають на ризик легалізації незаконних доходів економічними агентами одних країн у банківській системі інших. Це дозволить виявити ті країни, контрагенти яких є потенційно зацікавленими у відмиванні кримінальних коштів.

Спочатку дослідимо, чи існує зв'язок між рівнем інформаційної безпеки та ризиком легалізації коштів. Для цього визначимо коефіцієнти кореляції між показниками, які є ідентифікаторами рівня забезпечення інформаційної безпеки у країні, тобто “Глобальним індексом кібербезпеки”, “Національним індексом кібербезпеки”, “Індексом розвитку інформаційних та комунікаційних

технологій", "Індексом мережевої готовності", "Рівнем цифрового розвитку", та "Базельським індексом протидії відмиванню коштів" (AML), який використовується для оцінки ризику відмивання грошей та фінансування тероризму [20]. Для проведення дослідження було сформовано набір даних по 121 країнам світу за 2018 рік [21]. Розрахунки було проведено із застосуванням програми «MS Excel», результати яких представлено у таблиці 3.3:

Таблиця 3.3 – Розраховані коефіцієнти кореляції та визначена тіснота зв'язку

	GCI	ICT DI	NRI	NCSI	DDL
Коефіцієнт кореляції між AML індексом та показниками інформаційної безпеки	-0,5298	-0,7749	-0,4703	-0,6060	-0,7323
Тіснота зв'язку	значний	сильний	помірний	значний	сильний

Так, отримані значення коефіцієнтів кореляції свідчать, що між показниками-складовими інформаційної безпеки та індексом протидії відмиванню коштів існує лінійний зв'язок, тіснота якого варіюється від помірного до сильного, при чому його вид є оберненим для всіх індексів. Це говорить про те, що чим вище рівень безпеки, інформатизації та цифровізації в країні, тим нижче ризик легалізації кримінальних доходів в країні. Особливо впливає на нього ступінь розвитку інформаційно-комунікаційних та цифрових технологій. Можна зробити припущення, що використання технологій критично впливає на процес прийняття рішень у фінансовому секторі, зменшуючи дію людських чинників в процесі моніторингу транзакцій та надання дозволу на їх проведення. Що стосується показників, які оцінюють рівень безпеки та протистояння загрозам, то їх вплив на ризик легалізації кримінальних доходів є значним. Можна вважати, що чим краще захищені транзакції та інформаційні системи банку, тим нижче буде ризик здійснення операції, пов'язаної із відмиванням коштів, отриманих незаконним шляхом. Для розробки методики та проведення дослідження оберемо "Національний індекс кібербезпеки", оскільки

саме він стосується визначення рівня протидії інформаційним загрозам, тобто безпосередньо пов'язаний із ризиками, а також є одним із гарно корельованих показників. При чому цей індекс виступатиме фактором-дестимулятором, оскільки має обернений вплив на індекс протидії відмиванню коштів.

Окрім обраного фактору інформаційної безпеки визначимо ті показники, які можуть впливати на формування привабливості країни для відмивання коштів з боку іншої країни. Так, на основі аналізу та синтезу наукових досліджень з питань протидії легалізації кримінальних доходів було виділено 8 показників, отриманих з офіційних сайтів світових організацій: Світового банку – "Валовий внутрішній продукт на душу населення, у поточних доларах США" (GDP) [98], "Вимоги до центрального уряду" (CCG) [51]; Мережі податкової юстиції – "Індекс фінансової таємниці" (FCI) [90]; організації "Transparency International" – "Індекс сприйняття корупції" (CPI) [55]; Інституту економіки та миру – "Глобальний індекс тероризму" (GTI) [103]; "The Legatum Institute" – "Індекс процвітання" (LPI) [235]; з бази-даних «Глобальна Економіка» – "Індекс щастя" (HI) [111]; «NUMBEO» – "Індекс злочинності" (CI) [61].

Вибір перелічених показників обумовлено наступними твердженнями.

"Валовий внутрішній продукт на душу населення країни" показує рівень її економічного добробуту, платоспроможності населення. Збільшення значення даного показника говорить про зростання обсягів виробництва товарів та послуг, формування умов в країні, сприятливих для інших держав, які намагаються легалізувати кошти, отримані незаконним шляхом, що сприяє зниженню рівня привабливості для відмивання коштів. Даний показник виступає в якості фактора-дестимулятора.

"Індекс фінансової таємниці" характеризує, наскільки інтенсивно правова та фінансова системи країн дозволяє заможнім злочинцям приховувати та відмивати гроші, отримані із різних незаконних джерел по всьому світу. Чим вища оцінка даного показника, тим гірші позиції країни у світовому рейтингу, тобто вона сприяє відмиванню коштів, отриманих в результаті кримінальних дій. Для країн, що легалізують кошти, ризик легалізації відповідно знижується,

оскільки для них формується сприятливе середовище, тобто привабливість таких країн для відмивання коштів зростає. Даний фактор виступає стимулятором.

“Вимоги до центрального уряду” свідчить про рівень довіри до центрального уряду в частині його фінансових зобов’язань. Країни з високим рівнем довіри формують несприятливі умови для легалізації кримінальних доходів для країн, що легалізують, оскільки даний фактор ймовірно свідчить про зростання ризику легалізації та зниження її привабливості. В моделі показник виступатиме дестимулятором.

“Індекс злочинності” – фактор-стимулятор, який свідчить про нестабільність в країні, що викликається високим рівнем злочинності та створенням криміногенних ситуацій у країні. Відповідно, такий стан генерує менший рівень небезпеки для розміщення фінансових ресурсів. З позиції осіб, які легалізують кримінальні доходи, конфлікти між злочинними угрупуваннями, випадки насилля, створюють сприятливі для легалізації умови. Тобто підвищення рівня даного показника буде говорити про високий рівень привабливості для легалізації коштів іншою країною.

“Індекс сприйняття корупції” є фактором-дестимулятором в моделі, оскільки відображає ефективність роботи правоохоронних органів щодо виявлення фактів корупції. В країнах із високим значенням даного показника створюються умови, менш сприятливі для розміщення фінансових потоків. Вони є менш привабливими для країн, що легалізують кошти, оскільки ризики легалізації для них збільшуються.

“Глобальний індекс тероризму” показує рівень терористичної активності в країнах світу. Вибір даного показника обумовлюється збільшенням випадків терористичних актів, що впливає на національну та економічну безпеку країни в цілому. Даний показник виступає фактором-стимулятором, оскільки країн, що легалізують кошти, приваблюють країни з високим рівнем тероризму, тому що умови є сприятливими для відмивання доходів, законність походження яких є не підтвердженою.

“Індекс щастя” характеризує рівень добробуту населення країни з позиції

не його фінансового стану, а з позиції якості життя, що забезпечується відповідним рівнем екологічної безпеки, станом медицини і т.п. Країни, в яких проживає щасливе населення, є найменш привабливими для країн, що легалізують кошти, оскільки мають також й підвищені стандарти захисту інформації. Відповідно фактор виступає дестимулятором, оскільки привабливість легалізації із збільшенням значення показника знижується.

“Індекс процвітання” – показник добробуту країни, який відображає різні параметри: економіку, управління, освіту, здоров’я, безпеку, екологію тощо. Для дослідження береться різниця між добробутом країни, яка легалізує кошти, та країни, в якій кошти будуть відмиватися. Чим більше різниця між добробутом країн, тим кращі умови для легалізації.

З обраних показників сформовано набір даних по 159 країнам світу за 2018 рік. Його було проаналізовано на предмет відсутності значень показників для певних країн та очищено від таких спостережень. В результаті для моделювання було обрано дані тільки для 71 країни. Для перевірки правильності визначення факторів-стимуляторів та дестимуляторів розрахуємо коефіцієнти кореляції між обраними факторами та “Базельським індексом протидії відмиванню коштів” [20], що було виконано за допомогою MS Excel (див. табл. 3.4):

Таблиця 3.4 – Міжфакторна кореляція для показників оцінки привабливості легалізації

	CCG	GDP	CI	CPI	GTI	HI	PI	FCI	AML
CCG	1								
GDP	-0,0121	1							
CI	-0,1130	-0,4657	1						
CPI	0,0490	0,8166	-0,5802	1					
GTI	0,1846	-0,1163	0,1663	-0,1749	1				
HI	-0,0223	0,7148	-0,4273	0,6875	-0,1153	1			
PI	0,0920	0,8243	-0,6572	0,9287	-0,2078	0,8090	1		
FCI	0,1944	0,5588	-0,2580	0,3608	0,1739	0,3127	0,3601	1	
AML	-0,0437	-0,3698	0,5305	-0,6036	0,3370	-0,4987	-0,6614	0,1772	1

Знак коефіцієнту кореляції (див. табл. 3.4) між “Базельським індексом протидії відмиванню коштів” та іншими показниками відповідає твердженням

щодо визначення факторів-стимуляторів та дестимуляторів. Тобто "–" показує, що це фактор-дестимулятор, "+" – фактор-стимулятор. Що стосується отриманих високих значень міжфакторної кореляції для факторів, то це свідчить про існування між ними лінійної залежності. Оскільки для запропонованої методики не будується регресійна модель та не оцінюються параметри, для яких це призводить до нестійкості, то наявність міжфакторної кореляції не впливатиме на загальний результат.

Для оцінки рівня привабливості країн світу, що характеризується також ступенем ризику легалізації кримінальних доходів та фінансування тероризму, пропонується науково-методичний підхід, який базується на гравітаційному моделюванні. Результат дозволить визначити можливості легалізації фінансових ресурсів однією країною в іншій з урахуванням рівня протидії кіберзагрозам.

На *першому етапі* необхідно провести нормалізацію даних. Це пов'язано з тим, що показники, які використовуються для побудови моделі, мають різну розмірність. Тому їх треба привести до співставного вигляду від 0 до 1. Також треба врахувати той факт, що дані показники впливають по різному на привабливість країни для легалізації кримінальних доходів. Тобто, збільшення значення показника призводить до ситуації, коли рівень привабливості однієї країни для відмивання коштів збільшується для іншої, і навпаки. Відповідно, маємо справу із стимулятором. Якщо зміни значення показника призводять до обставин, коли із збільшенням показника рівень привабливості для легалізації кримінальних доходів знижується, і навпаки, то мова йде про дестимулятор.

Для нормалізації використаємо рівняння абсолютної нормалізації (3.3), що дозволить його застосувати як для стимуляторів, так й дестимуляторів, а також провести рівномірну нормалізацію:

$$x_{ij}^{+} = \frac{x_{ij}}{x_{max_j}}, x_{ij}^{-} = \frac{x_{min_j}}{x_{ij}}, \tag{3.3}$$

де x_{ij}^{+}, x_{ij}^{-} – нормалізоване значення j-го показника характеристики рівня привабливості для легалізації кримінальних доходів та фінансування тероризму, як для стимуляторів (+), так й для дестимуляторів (–), для і-ої розглянутої країни;

x_{ij} – початкове (емпіричне) значення j-го показника характеристики рівня привабливості для легалізації для і-ої країни;

x_{min_j} – мінімальна величина j-го показника характеристики визначення рівня привабливості для легалізації для всіх країн дослідження;

x_{max_j} – максимальна величина j-го показника характеристики визначення рівня привабливості для легалізації для всіх країн дослідження.

Значення показника “Вимоги до центрального уряду”, який використовується для моделювання, є як від’ємними, так й додатними. Відповідно, застосування абсолютної нормалізації до нього не дозволить отримати його значення від 0 до 1. Оскільки цей фактор виступає дестимулятором, то для нього застосовуємо нормалізацію Севіджа (3.4), що дозволить уникнути даної проблеми:

$$x_{ij}^{-} = \frac{x_{max_j} - x_{ij}}{x_{max_j} - x_{min_{ij}}}. \quad (3.4)$$

На *другому етапі* методики розрахунку визначаємо вагові коефіцієнти для обраних показників. З цією метою було проведено експертне опитування фахівців, які є компетентними в питаннях банківських ризиків, економічної та інформаційної безпеки, а також науковців, які працюють над проблемами розробки заходів протидії легалізації кримінальних коштів. Для роботи з експертами використовується метод аналізу ієрархії в частині отримання вагових коефіцієнтів.

Експертам було запропоновано заповнити матрицю, представлену у вигляді таблиці 3.5:

Таблиця 3.5 – Матриця попарного порівняння факторів, що заповнюється експертами

	GDP	FCI	CCG	CI	CPI	GTI	HI	NCSI
GDP	1	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}
FCI	$1/a_{12}$	1	a_{23}	a_{24}	a_{25}	a_{26}	a_{27}	a_{28}
CCG	$1/a_{13}$	$1/a_{23}$	1	a_{34}	a_{35}	a_{36}	a_{37}	a_{38}
CI	$1/a_{14}$	$1/a_{24}$	$1/a_{34}$	1	a_{45}	a_{46}	a_{47}	a_{48}
CPI	$1/a_{15}$	$1/a_{25}$	$1/a_{35}$	$1/a_{45}$	1	a_{56}	a_{57}	a_{58}
GTI	$1/a_{16}$	$1/a_{26}$	$1/a_{36}$	$1/a_{46}$	$1/a_{56}$	1	a_{67}	a_{67}
HI	$1/a_{17}$	$1/a_{27}$	$1/a_{37}$	$1/a_{47}$	$1/a_{57}$	$1/a_{67}$	1	a_{78}
NCSI	$1/a_{18}$	$1/a_{28}$	$1/a_{38}$	$1/a_{48}$	$1/a_{58}$	$1/a_{68}$	$1/a_{78}$	1

Матриця заповнюється шляхом попарного порівняння критеріїв за важливістю по шкалі, представленій у таблиці 3.6:

Таблиця 3.6 – Шкала, за якою заповнюється матриця попарного порівняння

Відносна оцінка важливості критерія	Якісна оцінка	Пояснення
1	Однаково важливий	Обидва елементи вносять однаковий вклад у досягнення кінцевої цілі
3	Не набагато важливий	Існують вербальні висловлювання відносно пріоритету одного елемента щодо іншого, але ці висловлювання досить непереконливі
5	Суттєво важливіший	Існують достатньо переконливі доведення та логічні критерії, що один з елементів є більш важливим (вагомішим)
7	Значно важливіший	Існує переконливе доведення великої значущості одного елемента в порівнянні з іншим
9	Абсолютно важливіший	Усвідомлення пріоритету одного елемента щодо іншого максимально підтверджується
2; 4; 6; 8	Проміжні оцінки між двома сусідніми судженнями	Потрібен певний компроміс
$\frac{1}{\nu}; \nu = 1, ..., 9$	Обернені значення ненульових оцінок	Протилежні оцінки та судження щодо пріоритету одного елементу у відношенні до іншого
0	Непорівняність	Немає сенсу в порівнюванні елементів

В процесі заповнення матриці, якщо елемент і важливіше елементу j, то на перетині рядку і та стовпчика j в клітинку (i; j) ставиться ціле число, якщо навпаки, то ставиться обернене число, тобто дріб. В клітинку (j; i) на перетині

рядка j та стовпчика і ставиться обернене до цілого числа, або ціле, що є оберненим до дробу.

Після цього в кожній матриці, в якій експерт поставив свої оцінки, для кожного фактору у рядку знаходимо ваговий коефіцієнт за формулою (3.5):

$$\omega_i^k = \frac{\sqrt[n]{\prod_{j=1}^{n} a_{ij}^k}}{\sum_{i=1}^{n} \sqrt[n]{\prod_{j=1}^{n} a_{ij}^k}}, \tag{3.5}$$

де ω_i^k – ваговий коефіцієнт для кожного фактору і, що оцінюється k-им експертом;

a_{ij}^k– оцінка, яку ставить k-ий експерт і-ому фактору;

n – кількість факторів, які підлягають оцінці.

Перед визначенням узагальненої оцінки для вагового коефіцієнту необхідно перевірити узгодженість експертів за допомогою коефіцієнта конкордації, який розраховується за формулою (3.6) та парної рангової кореляції – формулою (3.7):

$$K = \frac{\sum_{j=1}^{n} d_j^2}{\frac{1}{12}[m^2(n^3 - n) - m\sum_{i=1}^{m} T_i]}, \tag{3.6}$$

де *K* – коефіцієнт конкордації;

m – кількість експертів, які прийняли участь в дослідженні;

n – кількість факторів дослідження;

$d_j = \sum_{i=1}^{m} R_{ij} - \frac{\sum_{j=1}^{n}\sum_{i=1}^{m} R_{ij}}{n}$;

R_{ij} – ранг оцінки *i*-им експертом *j*-ого фактору;

$T_i = \sum_{l=1}^{L}(t_l^3 - t_l)$;

L – кількість груп зв’язаних (однакових) рангів;

t_l – кількість зв’язаних рангів в кожній групі;

$$P_{\alpha\beta} = 1 - \frac{\sum_{j=1}^{n} \psi_j^2}{\frac{1}{6} \times (n^3 - n) - \frac{1}{12}\left(T_\alpha + T_\beta\right)}, \quad (3.7)$$

де $P_{\alpha\beta}$ – коефіцієнт парної рангової кореляції;

ψ_j – різниця по модулю величин рангів оцінок j-ого фактору, поставлених експертами α і β;

$\psi_j = \left|R_{\alpha j} - R_{\beta j}\right|$;

T_α, T_β – показники зв'язаних рангів оцінок експертів α і β, що визначаються аналогічно, як і для коефіцієнта конкордації;

n – кількість факторів дослідження.

Для перевірки статистичної значущості коефіцієнта конкордації застосовується критерій Пірсона, який розраховується за формулою (3.8):

$$\chi_p^2 = \frac{\sum_{j=1}^{n} d_j^2}{\frac{1}{12}\left[mn \times (n+1) - \frac{1}{n-1}\sum_{i=1}^{m} T_i\right]}. \quad (3.8)$$

Якщо коефіцієнт конкордації буде наближатися до 1, то це буде свідчити про високий рівень узгодженості між експертами. Отримане значення критерію Пірсона покаже його статистичну значущість, що визначається шляхом порівняння розрахованого значення із табличним. При його перевищенні мова йде про підтвердження статистичної значущості коефіцієнту конкордації.

Значення коефіцієнта парної рангової кореляції буде показувати зв'язок між парами експертів. Якщо результат буде від 0,7 до 1, тобто між результатами експертного опитування існує сильний зв'язок, – тільки за цих умов можна зробити висновок про узгодженість між експертами. Якщо їх думки не узгоджені, то необхідно обрати тих, думки яких слабко корелюють з іншими, та результати їх опитування виключити з розгляду.

Після визначення узгодженості експертів у підсумку розраховується середньоарифметичне значення вагових коефіцієнтів, отриманих за формулою

(3.5), яке буде означати важливість (внесок) кожного із факторів в моделі за формулою (3.9):

$$\omega_j = \frac{\sum_{i=1}^{m} \omega_i^k}{m}. \tag{3.9}$$

Сума отриманих значень вагових коефіцієнтів повинна дорівнювати 1.

Після знаходження вагових коефіцієнтів на *третьому етапі* визначається інтегральний показник кількісної оцінки рейтингу певної країни щодо характеристики визначення рівня привабливості для легалізації кримінальних доходів та фінансування тероризму за допомогою метрики Мінковського (3.10). Він дозволяє враховувати вплив факторів на основі їх позицій, як стимуляторів, так і дестимуляторів:

$$IRA_i = 1 - \sqrt{\sum_{j=1}^{k} \omega_j \left|1 - x_{ij}^{+}\right|^2 + \sum_{j=k+1}^{n} \omega_j \left|1 - x_{ij}^{-}\right|^2}, \tag{3.10}$$

де IRA_i – інтегральна рейтингова оцінка характеристики рівня привабливості для легалізації *i-ою* країною;

ω_j – вагові коефіцієнти для *j*-го показника.

З урахуванням того, що для оцінки рівня привабливості країни для легалізації кримінальних доходів та фінансування тероризму було обрано 8 факторів (дев'ятий фактор буде використовуватися для чисельника кінцевої формули), то інтегральний показник буде розраховуватися за формулою (3.11):

$$IRA(x_i) = 1 - \sqrt{\begin{matrix}\omega_1(1-x_1^-)^2 + \omega_3(1-x_3^-)^2 + \omega_5(1-x_5^-)^2 + \omega_7(1-x_7^-)^2 + \\ +\omega_8(1-x_8^-)^2 + \omega_2(1-x_2^+)^2 + \omega_4(1-x_4^+)^2 + \omega_6(1-x_6^+)^2\end{matrix}}, \tag{3.11}$$

де x_1^- – нормалізоване значення “ВВП на душу населення” як фактора-дестимулятора;

x_2^+ – нормалізоване значення “Індексу фінансової таємниці” як фактора-стимулятора;

x_3^- –нормалізоване значення “Вимог до центрального уряду” як фактора-дестимулятора;

x_4^+ –нормалізоване значення “Індексу злочинності” як фактора-стимулятора;

x_5^- – нормалізоване значення “Індексу сприйняття корупції” як фактора-дестимулятора;

x_6^+ –нормалізоване значення “Глобального індексу тероризму” як фактора-стимулятора;

x_7^- – нормалізоване значення “Індексу щастя” як фактора-дестимулятора;

x_8^- – нормалізоване значення “Національного індексу кібербезпеки” як фактора-дестимулятора.

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

Четвертим етапом буде побудова гравітаційної моделі ризику легалізації. З цією метою за основу використаємо рівняння закону гравітаційного тяжіння та гравітаційної сили в суспільних явищах, тобто формулу (3.12):

$$M_{ij} = k\frac{p_i p_j}{d_{ij}^2}, \tag{3.12}$$

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

k – коефіцієнт відповідності (для економічних об’єктів не застосовується);

p – деяка значимість об’єкта;

d_{ij}^2 – відстань між об’єктами.

Використовуючи даний підхід, ідентифікуємо рівень привабливості для легалізації наступним чином: окрема країна «притягує» операції, пов’язані із

відмиванням коштів, в інші з силою, що прямо пропорційна рейтинговій оцінці характеристики рівня привабливості для легалізації розглянутої країни, а також є обернено пропорційною квадрату величини “Індексу процвітання”, тобто використаємо формулу (3.13):

$$SVA_k = \frac{IRA_k \cdot IRA_r}{d_{kr}^2}, \quad (3.13)$$

де SVA_k – кількісна оцінка величини (сили) взаємодії між r-ю розглянутою країною та k-ю країною в розрізі рівня привабливості для легалізації;

IRA_k – інтегральна рейтингова оцінка характеристики рівня привабливості для легалізації k-ї країни, яка передає ризик у цесію;

IRA_r – інтегральна рейтингова оцінка характеристики рівня привабливості для легалізації r-ї країни, яка приймає ризик легалізації;

d_{kr} – величина, яка представляє собою нормалізовану різницю між добробутом k-ї та r-ї країни, яка визначається за допомогою рівняння (3.14):

$$d_{kr} = |LPI_k - LPI_r|^+, \quad (3.14)$$

де LPI_k – значення «Індекс процвітання” для країни k;

LPI_r – значення «Індекс процвітання” для країни r.

Для знаходження нормалізованої різниці між добробутом країн використаємо рівняння (3.15) для природньої нормалізації, оскільки даний фактор є стимулятором для нашої моделі:

$$x_{ij}^+ = \frac{x_{ij} - x_{min_j}}{x_{max_j} - x_{min_{ij}}}. \quad (3.15)$$

На основі розрахованих значень кількісної оцінки величини (сили) взаємодії між країнами в розрізі ризику легалізації будується матриця, яка дозволить оцінити взаємодію між різними країнами світу.

Але при побудові даної матриці необхідно значення знов нормалізувати, оскільки кількісна оцінка ризику повинна бути від 0 до 1. Для цього використовуємо рівняння нормалізації Харрінгтона (3.16), яке дозволить нівелювати розкид в отриманих значеннях:

$$SVA'_k = \exp(-\exp(-SVA_k)). \quad (3.16)$$

Отримане значення буде знаходитися в межах від 0 до 1 та свідчити: якщо значення наближається до 0, то країна має низький рівень привабливості для легалізації, тобто ризик для економічних агентів, що легалізують, є високим; якщо значення наближається до 1, то країна матиме високий рівень привабливості, тобто ризик легалізації є низьким.

Розрахунки за запропонованим науково-методичним підходом проводилися із використанням «MS Excel». На першому етапі методики було проведено нормалізацію факторів-стимуляторів та дестимуляторів за формулами (3.3) та (3.4). Результати розрахунків представлені у таблиці Е.1 додатку Е. На другому етапі – отримано результати експертного опитування важливості факторів (див. табл. Е.2 додатку Е). Було залучено 7 експертів-фахівців з питань банківської справи, економічної безпеки, які є також й науковими дослідниками, які займаються проблематикою протидії відмиванню коштів. Узгодженість думок експертів було оцінено за коефіцієнтом конкордації, який отримано рівним 0,8698 за формулою (3.8). Його значення наближається до 1, що свідчить про високий рівень узгодженості між експертами. Статистичну значущість даного коефіцієнта підтверджує критерій Пірсона, визначений за формулою (3.10). Отримане значення критерію дорівнює 42,6191, що перевищує табличне значення, рівне 12,5916. Узгодженість між думками експертів також підтверджують значення коефіцієнту парної рангової кореляції, розраховані за формулою (3.9), результати яких представлені в таблиці 3.7:

Таблиця 3.7 – Матриця парної рангової кореляції узгодженості думок між експертами

Номера експертів							
	1	2	3	4	5	6	7
1	-	0,7857	0,9048	0,8810	0,9524	0,9048	0,7619
2		-	0,8333	0,9286	0,7381	0,7381	0,7381
3			-	0,9048	0,9048	0,9524	0,9286
4				-	0,8571	0,8333	0,8095
5					-	0,9048	0,7381
6						-	0,8095
7							-

Значення парної рангової кореляції є позитивними, що говорить про однонаправленість думок експертів. Коефіцієнти варіюються в межах від 0,7381 до 0,9524, що свідчить про сильний та дуже сильний тісний зв'язок, тобто існування узгодженості між експертами. За результатами оцінки приймаємо отримані значення як достовірні.

Далі розраховано усереднену оцінку факторів (див. табл. Е.3 додатку Е) та отримано ваги за формулою (3.11), які будуть використовуватися у гравітаційному моделюванні (див. табл. 3.8).

Таблиця 3.8 – Вагові коефіцієнти для факторів моделі

Фактори	Ваги
ВВП на душу населення	0,0634
Індекс фінансової таємниці	0,1824
Вимоги до центрального уряду	0,0629
Індекс злочинності	0,0911
Індекс сприйняття корупції	0,1603
Глобальний індекс тероризму	0,1419
Індекс щастя	0,0248
Національний індекс кібербезпеки	0,2732
Сума	1,0000

За результатами отриманих вагів видно, що найбільшу вагу має фактор

“Національний індекс кібербезпеки”, “Індекс фінансової таємниці”, “Індекс сприйняття корупції” та “Глобальний індекс тероризму”. Тобто дані фактори чинять найбільший вплив на оцінювання привабливості країни для легалізації кримінальних доходів. Отримані значення вагів дозволили розрахувати інтегрований показник та знайти кількісну оцінку величини (сили) взаємодії між певною розглянутою країною та k-ю країною в розрізі її привабливості щодо легалізації, що представлено у таблицях Е.4 – Е.5 додатку Е.

Проведемо детальний аналіз результатів гравітаційного моделювання для трьох країн – України, Польщі та Німеччини. Україну було обрано як країну, що розвивається та має середній рівень розвитку інформаційної безпеки, Німеччину та Польщу – як розвинуті країни, але з різним рівнем добробуту, а також високим та вище середнього рівнем інформаційної безпеки.

В таблиці Е.5 додатку Е представлено результати визначеного SVA'_k для України, а на рисунку 3.20 – карта привабливості різних країн світу для легалізації доходів з боку економічних агентів України.

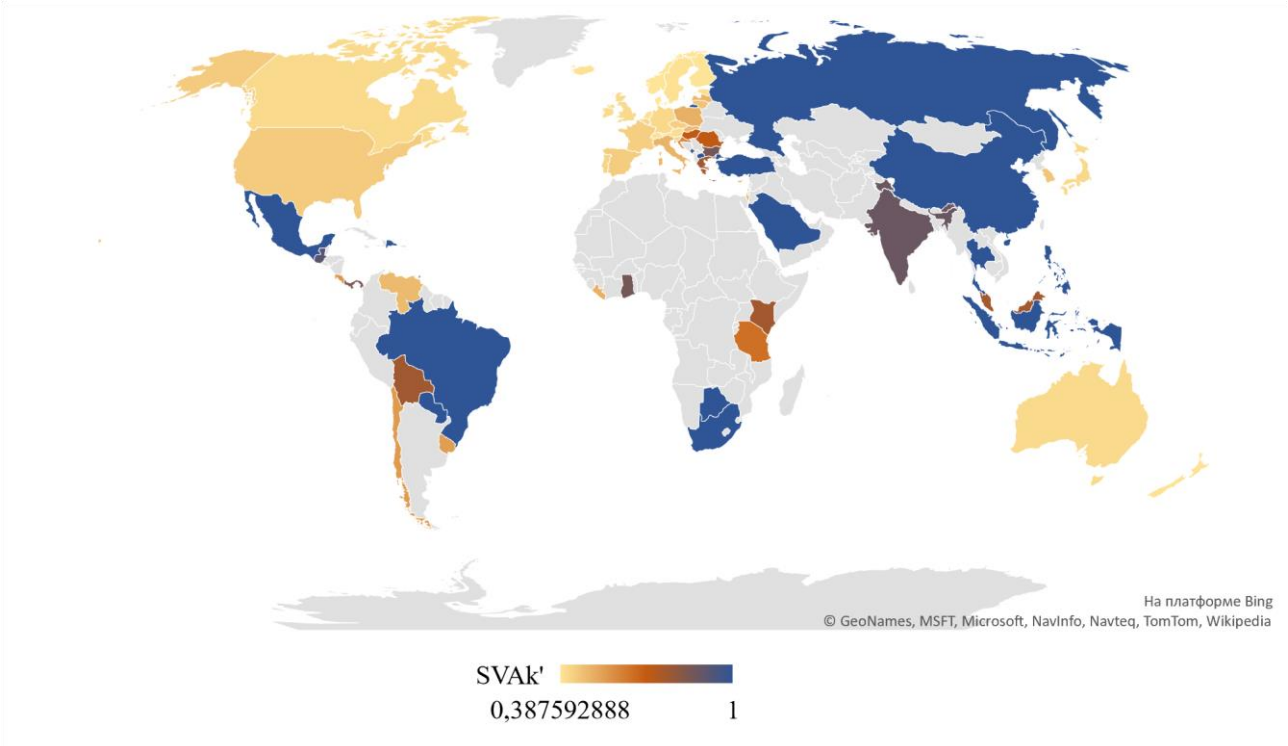


Рисунок 3.20 – Карта привабливості легалізації доходів для України в різних країнах світу (складено авторкою)

Дані рисунку 3.20 показують, що найменш привабливими країнами для легалізації доходів з боку України є Данія, Норвегія, Фінляндія, Нова Зеландія, Ісландія, Швейцарія, Естонія, Нідерланди, Австрія, Швеція та інші, які відносяться до країн з високим рівнем добробуту, протидії корупції, тощо. Завдяки своєму високому рівню розвитку вони створюють передумови для легалізації коштів, але ці країни також впроваджують високі стандарти захисту та боротьби із відмиванням коштів для збереження економічної безпеки країни, що знижує можливості інших країн для легалізації кримінальних доходів та підвищує рівень їх безпеки. Також варто відмітити, що для першої п'ятірки країн середній рівень національного показника кібербезпеки дорівнює 65,71, що свідчитиме про вплив рівня кіберзахисту на зменшення привабливості для відмивання коштів.

Такі країни, як Болівія, Гана, Гватемала, Індія, Туреччина, Танзанія, Філіппіни, тощо, переважно не випереджають Україну у економічному розвитку та добробуті (окрім деяких країн). Але для них є характерним рівень кібербезпеки нижче середнього (для першої п'ятірки він дорівнює 40,52). Відповідно рівень привабливості легалізації коштів в цих країнах для економічних суб'єктів України збільшується. Така картина спостерігається й для інших країн з низькими показниками економічного розвитку та добробуту, що можна прослідкувати на рисунку 3.20. Але вони є привабливими для відмивання коштів, оскільки мають високі показники корупції, рівень злочинності та низький рівень кібербезпеки, тощо.

Тобто для таких країн, як Україна, є привабливими для легалізації доходів країни із низьким рівнем кібербезпеки. Країни з високим рівнем добробуту є привабливими для легалізації, оскільки надають більше фінансових можливостей та гарантій отримання прибутків, але рівень їх кібербезпеки знижує привабливість відмивати кошти з боку економічних агентів України.

Визначимо, як впливає наявність фактору інформаційної безпеки на рівень привабливості України для легалізації незаконних доходів контрагентами інших країн. Результати цих значень представлені у таблиці 3.9.

Таблиця 3.9 – Вплив рівня кібербезпеки України на її привабливість для легалізації незаконних доходів контрагентами інших країн

Країна	Рівень привабливості	Країна	Рівень привабливості	Країна	Рівень привабливості
Guatemala	1,0000	Montenegro	0,5371	Belgium	0,4274
India	1,0000	Panama	0,4927	Ireland	0,4270
Kenya	1,0000	Malaysia	0,4831	Australia	0,4255
Ghana	1,0000	Bulgaria	0,4793	Malta	0,4238
Bolivia	1,0000	Greece	0,4727	Slovakia	0,4234
Turkey	1,0000	United States	0,4549	Sweden	0,4220
Tanzania	1,0000	Mauritius	0,4529	Luxembourg	0,4219
Philippines	1,0000	Chile	0,4521	Japan	0,4209
Russian Federation	0,9996	Israel	0,4497	Czech Republic	0,4209
Botswana	0,9993	Hungary	0,4496	Netherlands	0,4205
South Africa	0,9991	Romania	0,4484	Switzerland	0,4198
Paraguay	0,9975	Cyprus	0,4471	Singapore	0,4187
Saudi Arabia	0,9963	Italy	0,4424	Lithuania	0,4167
Dominican Republic	0,9948	Costa Rica	0,4401	Austria	0,4143
Thailand	0,9431	France	0,4385	Portugal	0,4124
Liberia	0,9414	Uruguay	0,4384	Slovenia	0,4092
Mexico	0,9313	Germany	0,4362	Finland	0,4078
Brazil	0,9143	Croatia	0,4337	New Zealand	0,4064
Venezuela	0,8961	Spain	0,4335	Norway	0,4059
China	0,8767	Poland	0,4319	Iceland	0,4056
Indonesia	0,8533	United Kingdom	0,4309	Estonia	0,4030
Bahrain	0,7622	Latvia	0,4296	Denmark	0,4014
Trinidad and Tobago	0,7340	Canada	0,4289	X	X
North Macedonia	0,6380	Korea	0,4286	X	X

Отримані результати (див. табл. 3.9) свідчать, що для України рівень привабливості знижується для тих країн, для яких розраховане значення є найменшим. Це країни з високим рівнем економічного добробуту. Отримане значення свідчить про те, що вони не зацікавлені у здійсненні подібних операцій за рахунок нестабільного економічного розвитку України та зниження можливостей щодо отримання прибутків. З іншого боку, країни, які є найменш розвиненими або мають невисокий рівень добробуту, найбільш зацікавлені у відмиванні коштів саме в Україні. Ймовірно це можливо за рахунок низького рівня протидії українського законодавства та фінансово-банківської системи

щодо здійснення таких операцій. Можна також припустити, що їх приваблюватиме високий рівень корупції та наявність військового конфлікту на Сході України.

Отримані висновки є значущими для діяльності національних регуляторів. Українським державним установам, таким як Національна комісія, що здійснює державне регулювання у сфері ринків фінансових послуг, Державна служба фінансового моніторингу, Національний банк України, що виконують регулювання питань щодо руху фінансових потоків за межі України, доцільно посилити напрямки відслідковування операцій, які будуть здійснюватися в країни з високим рівнем привабливості для легалізації доходів. Це можливо за рахунок встановлення певних обмежень та розширення інформації стосовно джерел доходів суб'єктів господарювання.

В таблиці Е.5 додатку Е наведено результати розрахунків SVA'_k, за запропонованою методикою для Польщі. На рисунку 3.21 представлена карта привабливості легалізації доходів економічними суб'єктами Польщі в різних країнах світу.

Дані рисунку 3.21 показують, що найменш привабливими країнами для легалізації доходів для Польщі є Ліберія, Венесуела, Танзанія, Норвегія, Данія, Болівія, Гана, Фінляндія, Нова Зеландія, Гватемала та інші. Частина з цих країн відноситься до країн із низьким рівнем добробуту, протидії корупції, рівнем щастя та рівнем кібербезпеки. Інша частина країн є найбільш економічно розвиненими та мають високий рівень кібербезпеки. Це можна пояснити тим, що ці країни відрізняються від Польщі значеннями аналізованих показників, при чому як в найкращу сторону, так й найгіршу. Тому для економічних агентів Польщі найменш розвинені країни не будуть привабливими за рахунок існування високих ризиків, пов'язаних із нестабільністю економічного, політичного та соціального становища. Розвинуті ж країни за рахунок високого рівня кібербезпеки та дотримання стандартів із боротьби проти відмивання коштів сприятимуть зменшенню фінансових потоків, які мають ознаки нелегальних.

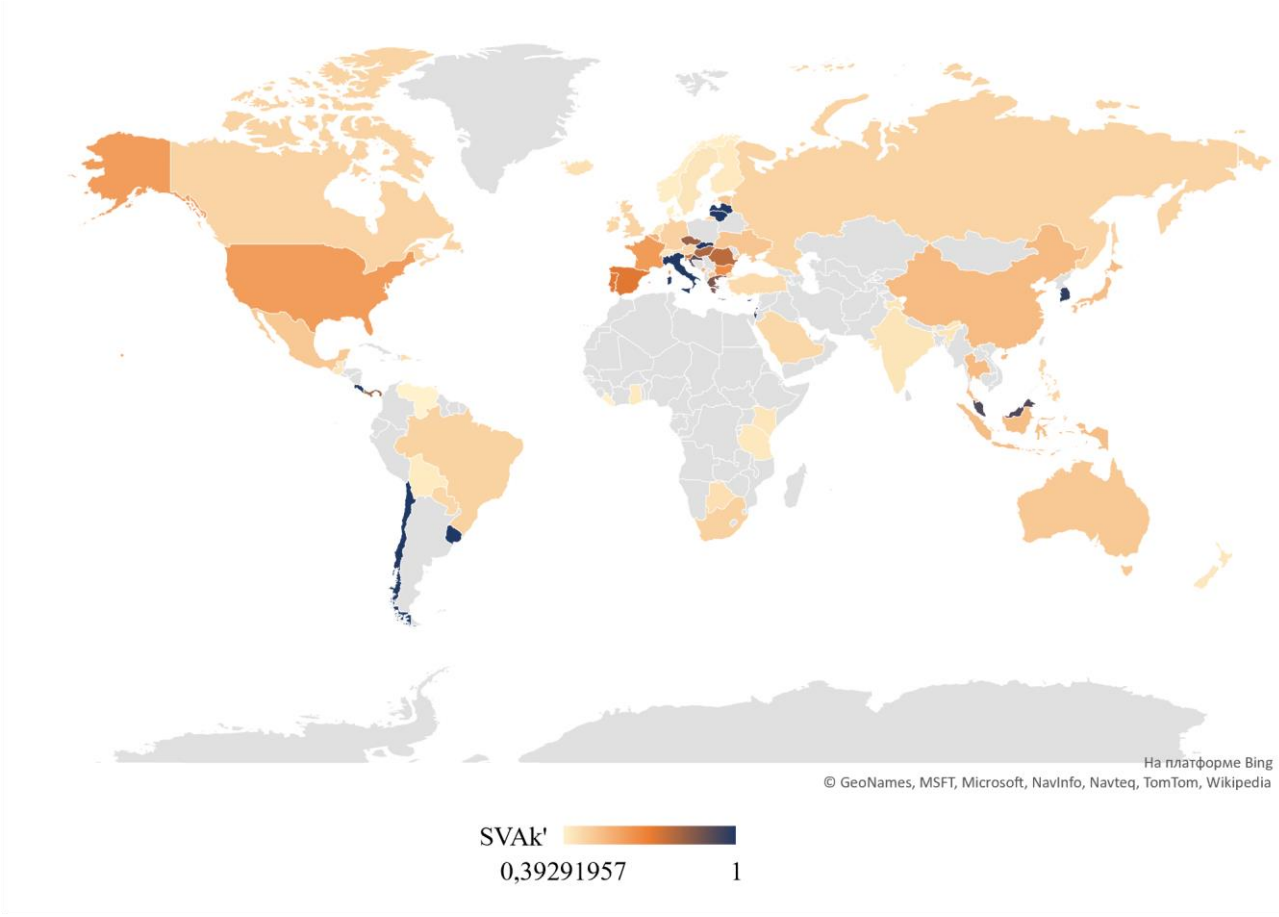


Рисунок 3.21 – Карта привабливості легалізації доходів для Польщі в різних країнах світу (складено авторкою)

Такі країни, як Чилі, Кіпр, Латвія, Литва, Словаччина, Уругвай, Італія, Коста Ріка, Ізраїль, Південна Корея та інші, що мають значення SVA'_k, близьке до “1”, є більш привабливими для легалізації кримінальних доходів з боку Польщі. Така картина спостерігається завдяки тому факту, що вони мають схожі із Польщею показники добробуту та вони є близькими за рівнем інформаційної безпеки, що можна прослідкувати з даних таблиці Е.5 додатку Е. Високий рівень привабливості обумовлений тим, що це країни із середнім рівнем кібербезпеки та фінансової таємниці. Відповідно, ризик втрати коштів для Польщі в процесі легалізації буде помірним, чому також сприятимуть умови щодо обмежень припливу ресурсів за кордону. Отримані висновки повинні зацікавити регуляторні органи Польщі в плані посилення нагляду за витоком коштів у країни, які попали в топ привабливих для легалізації.

Результати впливу фактору “Національний індекс кібербезпеки” на рівень привабливості країн у гравітаційній моделі представлені у таблиці 3.10.

Таблиця 3.10 – Вплив рівня кібербезпеки Польщі на її привабливість для легалізації незаконних доходів контрагентами інших країн

Країна	Рівень привабливості	Країна	Рівень привабливості	Країна	Рівень привабливості
Chile	1,0000	Romania	0,6807	South Africa	0,4904
Cyprus	1,0000	Japan	0,6383	Philippines	0,4895
Latvia	1,0000	Australia	0,6291	North Macedonia	0,4884
Lithuania	1,0000	Bulgaria	0,6061	New Zealand	0,4878
Slovakia	1,0000	Estonia	0,5944	Russian Federation	0,4837
Italy	1,0000	Germany	0,5858	Tanzania	0,4808
Uruguay	1,0000	Canada	0,5727	Finland	0,4774
Israel	1,0000	United Kingdom	0,5713	Brazil	0,4735
Costa Rica	1,0000	Ireland	0,5647	Kenya	0,4728
Korea	0,9995	Singapore	0,5625	Turkey	0,4724
Czech Republic	0,9013	Bahrain	0,5620	Paraguay	0,4713
Mauritius	0,8966	Montenegro	0,5609	Saudi Arabia	0,4709
Malaysia	0,8941	Austria	0,5477	Norway	0,4676
Spain	0,8888	Luxembourg	0,5448	India	0,4588
Croatia	0,8825	Thailand	0,5283	Denmark	0,4572
Slovenia	0,8287	China	0,5217	Dominican Republic	0,4561
Portugal	0,8282	Netherlands	0,5210	Botswana	0,4513
Greece	0,7711	Indonesia	0,5138	Guatemala	0,4465
United States	0,7553	Trinidad and Tobago	0,5103	Liberia	0,4391
Panama	0,7501	Iceland	0,5096	Bolivia	0,4375
France	0,7451	Sweden	0,5088	Ghana	0,4358
Malta	0,7329	Switzerland	0,5048	Venezuela	0,4315
Hungary	0,6951	Ukraine	0,5033	X	X
Belgium	0,6874	Mexico	0,4972	X	X

Результати таблиці 3.10 показують, що Польща не є привабливою для легалізації кримінальних доходів для таких країн, як Венесуела, Гана, Болівія, Лівія, Гватемала, Ботсвана, Домініканська Республіка та інші. Тобто для країн з низьким рівнем економічного добробуту можливості для легалізації доходів будуть знижені за рахунок впливу рівня її кібербезпеки. З іншого боку, для таких

країн, як Чилі, Кіпр, Латвія, Литва, Словаччина, Італія, Уругвай, Ізраїль та інші рівень кібербезпеки Польщі не впливає на зниження рівня її привабливості. Тобто для Польщі знижується рівень її привабливості для переважної більшості країн за рахунок підвищення ризику легалізації для них, оскільки на це впливає рівень кіберзахисту. Отримані результати підтверджують той факт, що такий фактор, як інформаційна безпека (кібербезпека), є значущим та впливатиме на можливості злочинців легалізувати кримінальні доходи. У випадку її високого значення це може призводити до обмеження фінансових потоків від економічних суб'єктів тих країн, для яких Польща є найбільш привабливою.

В таблиці Е.5 додатку Е наведено результати двох варіантів розрахунків SVA'_k – кількісної оцінки величини (сили) взаємодії між Німеччиною та іншими країнами, що характеризує ступінь їх привабливості для легалізації німецьких економічних агентів, а на рисунку 3.22 представлена карта.

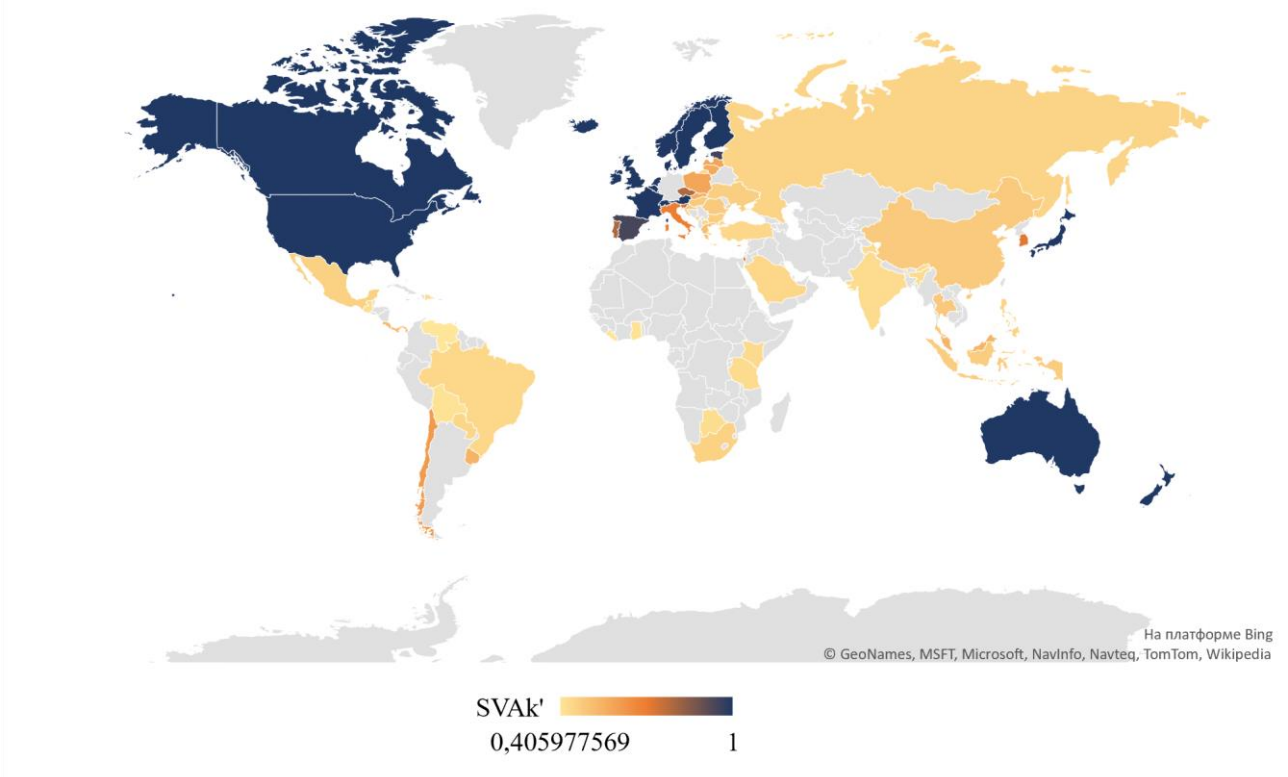


Рисунок 3.22 – Карта привабливості легалізації доходів для Німеччини в різних країнах світу (складено авторкою)

Такі країни, як Австрія, Канада, Ірландія, Ісландія, Люксембург, Нідерланди, Нова Зеландія, Сінгапур, Великобританія, Швейцарія, Австралія, Фінляндія, Швеція, США, є країнами з високим рівнем економічного розвитку та економічної безпеки. Для Німеччини вони є найбільш привабливими для легалізації кримінальних доходів, оскільки вони є близькими з нею за рівнем економічного розвитку та процвітання. Тобто вони мають більше умов для отримання додаткових прибутків з вкладених коштів. Але оскільки в даних країнах діють підвищені стандарти кібербезпеки, то на практиці питання їх привабливості будуть спірними. Хоча, наприклад, такі країни, як Швейцарія, США, Сінгапур, Люксембург, які мають найвищі показники фінансової секретності, зацікавлені у подібних операціях, оскільки не дозволяють розкривати умови здійснення транзакцій. Тому для Німеччини вони в цьому плані є найбільш привабливими, не зважаючи на рівень їх кібербезпеки.

Навпаки, такі країни, як Ліберія, Венесуела, Танзанія, Болівія, Гана, Ботсвана, Гватемала, Індія, Кенія, Домініканська Республіка та інші, результати розрахунків для яких представлені в таблиці Е.5 додатку Е та на рисунку 3.22, не є привабливими для легалізації кримінальних доходів з боку економічних суб’єктів Німеччини, оскільки їх економічний розвиток не сприяє процесам відмивання доходів, а також пов'язаний із підвищеним ризиком втрат для економічних агентів, оскільки для таких країн характерне нестабільне політичне становище, можливі озброєнні конфлікти та війни.

Отримані висновки для Німеччини можливо використати для розробки стратегії моніторингу та контролю фінансових потоків в країни з високим рівнем привабливості для легалізації кримінальних доходів, що сприятиме зниженню виведення грошей з країни та зменшенню їх втрат через відведення у тінь.

Що стосується впливу фактору рівня інформаційної безпеки Німеччини на її привабливість для відмивання коштів з боку інших країн, то результати розрахунків представлені у таблиці 3.11.

Таблиця 3.11 – Вплив рівня кібербезпеки Німеччини на її привабливість для легалізації незаконних доходів контрагентами інших країн

Країна	Рівень приваб-ливості	Країна	Рівень приваб-ливості	Країна	Рівень приваб-ливості
Austria	1,0000	Slovenia	0,6361	Russian Federation	0,4158
Canada	1,0000	Israel	0,6200	Indonesia	0,4155
Iceland	1,0000	Korea	0,6096	Ukraine	0,4153
Ireland	1,0000	Italy	0,5670	India	0,4150
Luxembourg	1,0000	Cyprus	0,5018	Turkey	0,4140
Netherlands	1,0000	Chile	0,4921	Venezuela	0,4135
New Zealand	1,0000	Latvia	0,4813	Mexico	0,4135
Singapore	1,0000	Lithuania	0,4795	Croatia	0,4129
United Kingdom	1,0000	Poland	0,4748	Paraguay	0,4104
Australia	1,0000	Slovakia	0,4618	Saudi Arabia	0,4093
Switzerland	1,0000	Uruguay	0,4491	Trinidad and Tobago	0,4083
Sweden	1,0000	Costa Rica	0,4413	Hungary	0,4077
Finland	1,0000	Tanzania	0,4347	Guatemala	0,4069
United States	1,0000	Malaysia	0,4313	Romania	0,4062
Denmark	1,0000	Kenya	0,4255	Brazil	0,4052
Norway	1,0000	Bahrain	0,4236	Bolivia	0,4049
Japan	0,9973	Thailand	0,4228	Dominican Republic	0,4041
Belgium	0,9964	Mauritius	0,4222	Botswana	0,4025
France	0,9940	Greece	0,4200	Ghana	0,4022
Malta	0,9531	Philippines	0,4199	North Macedonia	0,4018
Spain	0,9151	Panama	0,4192	Montenegro	0,4010
Estonia	0,9039	China	0,4186	Bulgaria	0,4007
Portugal	0,6891	South Africa	0,4184	X	X
Czech Republic	0,6710	Liberia	0,4179	X	X

Результати розрахунків таблиці 3.11 свідчать, що Німеччина є привабливою для економічних суб’єктів таких країн, як Австрія, Канада, Ісландія, Ірландія, Люксембург, Нідерланди, Нова Зеландія та інші. Тобто рівень її кібербезпеки в меншій мірі впливає на її привабливості для цих країн. Це не свідчить про недоліки її кіберзахисту, оскільки це може бути обумовлено рядом інших причин, таких як те, що ризики отримання високих прибутків від відмивання коштів для економічних агентів інших країн є значно меншими ніж бути заблокованим службами кіберзахисту банківської системи Німеччини. А також вона займає 5-те місце за рівнем фінансової секретності, що також

підвищує її привабливість. Такі країни, як Болгарія, Чорногорія, Північна Македонія, Гана, Ботсвана, Домініканська республіка, Болівія, Бразилія та інші, змінюють свій вектор привабливості Німеччини у бік збільшення ризику для легалізації за рахунок високого рівня кібербезпеки. В цілому результати свідчать про те, що рівень інформаційної безпеки Німеччини підвищує ризик легалізації коштів для ряду країн, оскільки даний фактор може бути ключовим у випадку обмеження здійснення подібних операцій.

Що стосується впливу кібербезпеки на привабливість легалізації для інших країн (див. табл. Е.5 додатку Е), то отримані результати підтверджують загальну тенденцію для інших країн. Тобто рівень безпеки в певній мірі знижує привабливість країни для відмивання злочинних доходів, що сприятиме декримінализації фінансового сектору будь-якої країни.

Такий процес, як легалізація незаконних доходів та фінансування тероризму, для будь-яких країн світу, як правило, носить несприятливий характер, особливо для економічної безпеки країни. По-перше, він сприяє зростанню тіньового сектору в економіці, оскільки частина доходів скривається. По-друге, бюджет держави втрачає значні кошти, оскільки з таких доходів, як кримінальні, не сплачуються податки. По-третє, легалізація незаконних доходів сприяє створенню та розповсюдженню шахрайських схем щодо фінансових потоків. По-четверте, збільшується відтік інвестицій та знижується привабливість бізнесу. По-п’яте, збільшуються витрати держави на боротьбу із фінансовою злочинністю. Все це призводить до підриву устоїв економічної безпеки країни, може впливати на появу та збільшення терористичних загроз для суспільства, що врешті-решт може призвести також й до порушення соціальної безпеки в країні.

Запропонована методика покликана сприяти виявленню тих країн, які створюють найбільш сприятливі умови для легалізації кримінальних доходів для тих, які є схожими за рядом факторів впливу на ризик. Її застосування на рівні фінансових структур дозволить сформувати інформаційну базу для прийняття управлінських рішень щодо підвищення рівня економічної безпеки країни, оскільки це надає можливості концентрувати увагу саме на тих країнах, які є

привабливими для легалізації кримінальних доходів. Впровадження даної методики сприятиме розробці нових інструментів моніторингу, аналізу, оцінки та прогнозування фінансових операцій, здійснення яких можливе за межами країни. Так, це дозволить створити механізм взаємодії з іншими країнами в плані визначення цільових видів діяльності, джерел походження ресурсів, тощо. В свою чергу, це потребуватиме удосконалення законодавчої бази для фінансово-кредитних установ, суб'єктів господарювання, а також осіб, що придбають нерухомість, акції закордоном, або є пов'язаними з іншими посередниками.

Інформація, яка є результатом реалізації запропонованої методики, слугує підґрунтям для удосконалення стандартів економічної політики країни з боку посилення економічної безпеки та розвитку партнерських відносин з іншими країнами. Це можливе за рахунок розвитку нових інформаційних технологій щодо збору та обміну інформацією не тільки в середині країни стосовно фінансових потоків, але й по всьому світу, за рахунок залучення нових учасників. Також встановлена значущість фактору кібербезпеки, який впливає на ризик легалізації та підвищує його рівень для злочинців та кримінальних угрупувань. В частині безпеки можна запровадити ряд ефективних технологій та методик, які зроблять можливим автоматичне проведення ідентифікації джерел доходів та характеру операцій, що дозволить, не порушуючи банківську таємницю, позначати операції із сумнівними джерелами доходу та повідомляти про спробу їх здійснення у правоохоронні органи. Подібну ідентифікацію доцільно впроваджувати на рівні банків як обов'язковий елемент звітності банківських установ перед державою. Також перспективним напрямом є процес інтеграції системи інформаційної безпеки банку та системи протидії відмиванню грошових коштів, що сприятиме підвищенню ефективності не тільки в частині зниження витрат на обидві системи, але й збільшення можливостей здійснення автоматизованих перевірок на основі єдиної інтегрованої бази даних.

Узагальнення методології та результатів проведеного дослідження впливу рівня кібербезпеки країни на її привабливість для операцій із легалізації коштів представлено на рисунку 3.23.

Етап 1. Визначення зв'язку між складовими ІБ та Базельським індексом протидії відмиванню коштів (БІПВК) на основі кореляційного аналізу: БІПВК ↔ Глобальний індекс кібербезпеки (–0,53; значний зв'язок); БІПВК ↔ Індекс розвитку інформаційно-комунікаційних технологій (–0,77; сильний); БІПВК ↔ Індекс мережевої готовності країни (–0,47; помірний); БІПВК ↔ Національний індекс кібербезпеки (НІК) (–0,61; значний); БІПВК ↔ Рівень цифрового розвитку (–0,73; сильний)

Етап 2. Вибір факторів впливу на формування привабливості країни для відмивання коштів із боку іншої країни: ВВП на душу населення (ВВП); Вимоги до центрального уряду (ВЦУ); Індекс фінансової таємниці (ІФТ); Індекс сприйняття корупції (ІСК); Глобальний індекс тероризму (ГІТ); Індекс щастя (ІЩ); Індекс злочинності (ІЗ); НІК; Індекс процвітання (ІП)

Етап 3. Проведення нормалізації значень факторів: використання абсолютної нормалізації для всіх факторів, окрім ВЦУ (використання нормалізації Севіджа)

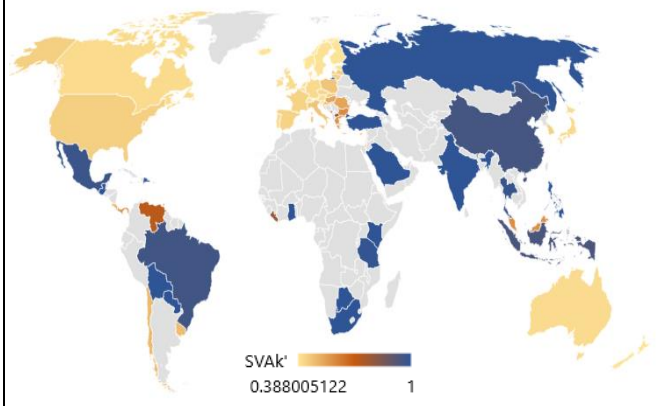
Етап 4. Визначення вагових коефіцієнтів для обраних факторів: а) проведення експертного опитування щодо важливості одного фактору стосовно до іншого з використанням методу аналізу ієрархії в частині отримання вагових коефіцієнтів: $\omega_i = \sum_{i=1}^{m} \omega_i^k / m$, де ω_i – середньоарифметичне значення вагових коефіцієнтів для *i*-го фактору; *m* – кількість експертів (було залучено 7 експертів); ω_i^k – ваговий коефіцієнт для кожного фактору *i*, що оцінюється *k*-м експертом: $\omega_i^k = \sqrt[n]{\prod_{j=1}^{n} a_{ij}^k} \Big/ \sum_{i=1}^{n} \sqrt[n]{\prod_{j=1}^{n} a_{ij}^k}$, де a_{ij}^k – оцінка, яку ставить *k*-й експерт *i*-му фактору; *n* – кількість факторів, що підлягають оцінюванню; б) перевірка узгодженості думок експертів за допомогою коефіцієнта конкордації (0,8698 – високий рівень), критерія Пірсона (42,6191 – підтвердження статистичної значущості коефіцієнта конкордації) та парної рангової кореляції (значення від 0,7381 до 0,9524 – сильний та дуже сильний тісний зв'язок)

Етап 5. Визначення інтегральної рейтингової оцінки для характеристики рівня привабливості країни щодо легалізації кримінальних доходів із використанням метрики Мінковського:

$IRA_i = 1 - \sqrt{\sum_{j=1}^{k} \omega_j \left|1 - x_{ij}^{+}\right|^2 + \sum_{j=k+1}^{n} \omega_j \left|1 - x_{ij}^{-}\right|^2}$, де: $IRA(x_i)$ – інтегральна рейтингова оцінка рівня привабливості *i*-ї країни щодо легалізації кримінальних доходів; x_j^- – нормалізоване значення *i*-го фактору-дестимулятора (x_1^- – ВВП; x_3^- – ВЦУ; x_5^- – ІСК; x_7^- – ІЩ; ; x_8^- – НІК); x_j^+ – нормалізоване значення *i*-го фактору-стимулятора (x_2^+ – ІФТ; x_4^+ – ІЗ; x_6^+ – ГІТ); ω_1 – ω_8 – вагові коефіцієнти, визначені на етапі 4

Етап 6. Побудова гравітаційної моделі рівня привабливості країн: а) використання рівняння закону гравітаційного тяжіння та гравітаційної сили в суспільних явищах: $SVA_k = IRA_k \cdot IRA_r / d_{kr}^2$, де SVA_k – кількісна оцінка величини (сили) взаємодії між *k*-ю країною та r-ю країною в розрізі рівня їх привабливості; IRA_k – інтегральна рейтингова оцінка рівня привабливості *k*-ї країни, суб'єкти якої легалізують незаконні кошти; IRA_r – інтегральна рейтингова оцінка рівня привабливості *r*-ї країни, щодо якої здійснюється легалізація; d_{kr}^2 – величина, яка являє собою нормалізовану різницю, знайдену за допомогою природньої нормалізації, між добробутом *k*-ї та *r*-ї країн: $d_{kr} = |LPI_k - LPI_r|^+$, де LPI_k – значення ІП для *k*-ї країни; LPI_r – значення ІП для *r*-ї країни; б) нормалізація за допомогою функції Харрінгтона: $SVA'_k = \exp(-\exp(-SVA_k))$; в) інтерпретація результатів: значення, близьке до 1, – підвищений рівень привабливості країни для легалізації; 0 – країна має низький рівень привабливості

Етап 7. Ідентифікація результатів



а) привабливість різних країн світу для легалізації брудних коштів українськими контрагентами (з урахуванням рівнів кібербезпеки цих країн)

б) вплив рівня кібербезпеки України на її привабливість для легалізації незаконних доходів контрагентами інших країн (фрагмент)

Країна	РП	Країна	РП
Країни, для яких рівень привабливості (РП) України щодо її використання в незаконних операціях є:			
найбільшим		*найменшим*	
Кенія	1,0000	Данія	0,4014
Індія	1,0000	Естонія	0,4030
Гватемала	1,0000	Ісландія	0,4056
Гана	1,0000	Норвегія	0,4059
Болівія	1,0000	Нова Зеландія	0,4064
Туреччина	1,0000	Фінляндія	0,4078
Танзанія	1,0000	Словенія	0,4092
Філіппіни	1,0000	Португалія	0,4124
Росія	0,9996	Австрія	0,4143
Ботсвана	0,9993	Литва	0,4167

Рисунок 3.23 – Методологія та результати дослідження впливу рівня кібербезпеки країни на її привабливість для операцій із легалізації коштів (складено авторкою)

3.3 Вплив «інформаційних бульбашок» на функціонування глобального цифрового економічного простору

В сучасному світі найбільшого поширення набуває практика інформаційного впливу на різні сфери діяльності, як на рівні держави, так й на глобальному. Влада інформації перетворюється на вирішальну силу при управлінні суспільством, зміщуючи акценти впливу фінансових й політичних державних важелів на другорядний план. Розвиток сучасних інформаційних технологій охопив майже всі галузі суспільної діяльності, в тому числі й мистецтво ведення інформаційних війн. Їх роль протягом останнього десятиліття неухильно зростає, оскільки відмінною їх особливістю є відсутність видимих руйнівних наслідків, а також поступове, майже непомітне втілення в усіх сферах суспільної, політичної та економічної життєдіяльності.

Інформаційна війна – це сучасний вид озброєння, який застосовується різними державами світу з метою дестабілізації певної сфери діяльності в країні. Це відбувається шляхом використання різних інструментів, таких як кібершпигунство, пропаганда, хакерські атаки, веб-вандалізм, викрадення конфіденційної інформації, тощо. Як правило, той, хто застосовує інструменти ведення інформаційної війни, намагається вплинути на конкретний об’єкт та порушити його функціонування або змінити його відповідно до інших правил, або взагалі зруйнувати. Наслідки від цього можуть бути непередбачуваними та відчутними протягом тривалого періоду часу. Деякі країни створюють спеціальні підрозділи, діяльність яких спрямована на ведення інформаційних війн проти інших держав з метою втручання в їх політичне, соціальне та економічне життя.

Безболісно подолати наслідки інформаційних війн неможливо, оскільки вони здатні проникнути в усі сфери життєдіяльності суспільства та вкрай негативно тиснути на людство. Сторона, що програє в інформаційній війні, може втратити контроль, стати підвладною стороні-переможцю, стикнутися з

руйнуванням працездатності економічної системи, порушенням політичної стабільності, знищенням непотрібних переможцю структур, і навіть системи національної безпеки. Але особливо відчутними є наслідки в економічній сфері, оскільки за часту об’єктом кіберзлочинів є фінансова інформація, втрата якої може призвести до фінансових втрат.

Відповідно питання захисту від такої зброї повинно бути одним із найвищих пріоритетів для систем національної та світової безпеки. Так, в цьому напрямку Тімом Бернерсом-Лі, творцем Всесвітньої павутини, 25 листопада 2019 року був запропонований «Мережевий контракт», який являє собою план дій для уряду, компаній та окремих осіб щодо захисту в мережі від різного роду інформаційного впливу. Тобто вони повинні узяти на себе обов’язки щодо захисту мережі від різного роду інформаційних фейків, неправдивих політичних новин, порушення конфіденційності та іншого роду зловживань [157].

Також деякі країни створюють спеціальні підрозділи реагування, які займаються виявленням та попередженням ймовірних проявів інформаційних війн. Окрім цього уряд багатьох країн сприяє розробці національної стратегії інформаційного захисту та протидії кібертероризму, організації спеціалізованих органів та інститутів, що діють в цьому напрямку. Сучасні вчені та науковці також звертають увагу на питання протидії інформаційним війнам та намагаються знайти ефективні рішення. У цьому напрямку можна виділити математичний інструментарій, застосування якого дозволяє моделювати ситуації, пов’язані зі здійсненням кібератак, та прогнозуванням наслідків. Роботи подібного характеру спрямовані на створення додаткових заходів, які дозволять виявляти слабкі місця в системах захисту, та надалі вибудовувати ефективну системи інформаційного захисту. Саме тому напрям дослідження, присвячений вирішенню питання моделювання розповсюдження наслідків інформаційних війн як фактору економічної дестабілізації країни, є актуальним та практично значущим.

Вирішенню проблеми інформаційних війн присвячено багато праць зарубіжних та вітчизняних науковців, які займалися дослідженням їх різних

аспектів. Так, Робінсон М., Джонс К. та Яніке Х. намагалися проаналізувати існуючі визначення кібервійни та визначити основні дослідницькі задачі у цій галузі [203]. МакКей Б. та Мунро І. приділили увагу такому аспекту, як використання різних організацій для здійснення інформаційних війн, що призводить до зміну політичних ландшафтів у країні [171]. Кріллі К. розкриває сутність методів, які використовують різні терористичні групи у процесі ведення інформаційної війни, особливо робиться акцент на застосуванні Інтернет-технологій та сучасні засоби комунікації [60]. Дродж К. розглядає правові аспекти, які стосуються захисту прав громадян у випадку ведення інформаційної війни, а також проводить паралелі між даним фактом, війною та озброєним конфліктом [76].

Кенні М. аналізує поняття кібертероризму та формулює основну ідею, що більшість сучасних кібератак не досягають рівня кібертероризму, хоча вони дуже успішно використовуються спеціальними урядовими організаціями для збору інформації, коштів, проведення вербування прибічників, тощо [140]. Кнапп К. Дж. та Боултон В.Р. досліджують основні тенденції стосовно інформаційних війн у світі та наголошують на тому, що вони демонструють перетворення інформаційної війни з політичного та військового інструменту у комерційну проблему, оскільки вони почали активно використовуватися для промислового шпигунства [143]. Окремо слід виділити ідеї Брайанта В. [36] та Кларка Р. [52] стосовно трансформації інформаційних війн у технічні інформаційні атаки та кібервійни.

Особливої уваги заслуговують напрацювання науковців, які стосуються розробки різних інструментів, механізмів та технологій протидії здійснення інформаційних війн та різного роду кібертерористичних атак. Так, Хекман К.Є., Уолш М.Дж., СтехФ.Дж., О'Бойл, Т.А., Дікато С.Р., Гербер А.Ф. представили результати дослідження системи “cyber wargame”, яка використовується для тестування платформи кібербезпеки динамічного мережевого захисту, яка дозволяє надавати зловмисникам неправдиву інформацію замість реальної [113]. Місра С., Сінгх Р., Рохіт Мохан С.В. запропонували спеціальний механізм

виявлення кібератак з використанням радіоперешкод для бездротових мереж [177]. Дудду В. досліджує напрямки застосування методів інтелектуального аналізу з метою протидії кібератакам та інформаційному тероризму та розглядає різні методи захисту у відповідністю із моделями загроз для систем машинного навчання [77].

Хоча вирішенню проблеми «інформаційних війн» приділено значну увагу з боку дослідників, економістів та вчених, але в науковій літературі й досі відсутня чітка методика подолання та попередження такої серйозної загрози.

Поняття «інформаційна війна» є широким та охоплює діяльність спеціалізованих угрупувань або окремих осіб, яка набуває значних масштабів та спрямована на викрадення інформації, її викривлення, порушення цілісності, використання у злочинних цілях, тощо. Основними інструментами інформаційної війни є масові хакерські кібератаки, кібершпигунство, інформаційна пропаганда, вірусні атаки з метою збору конфіденційної інформації, централізовані атаки на сервери, мережі, підробка кодів, програмного, технічного забезпечення, пристроїв введення-виведення, тощо. Крім цього можна виділити ряд показників, які дозволяють оцінити масштаби ведення інформаційних війн та зрозуміти вплив цього явища на життєдіяльність країни та світу в цілому. Так, на рисунку 3.24 представлена інфографіка таких показників, яку було складено із використанням програмного продукту “VISME” на основі статистичних даних, зібраних міжнародними організаціями та аналітиками.

Кожні 39 секунд у світі відбувається кібератака, що говорить про масовість та розповсюдженість даного явища (рисунок 3.24). Це пов’язано із зростанням технічних можливостей для кіберзлочинців та доступністю різних пристроїв для хакерів, мінімальна ціна за які складає 1 долар. Тільки у 2018 році компанія Cisco заблокувала 7 трлн. загроз, що складає близько 20 млрд. загроз на день [178]. Кіберзлочини поступово набувають масового характеру, оскільки пов’язані із відносною простотою здійснення та за часту уникненням відповідальності за рахунок існування часового лагу між здійсненням та виявленням.

Рисунок 3.24 – Інфографіка основних показників інформаційних війн
Джерело дослідження: побудовано авторкою на основі [178, 85, 37]

Статистика для США показує, що вони складають близько 10-12% від загального обсягу злочинів (рисунок 3.24). Їх мета може бути різною, хоча близько 11% кібератак пов’язують саме із кібершпигунством, що дозволяє ряду країн викрадати секретні дані, які використовуються проти інших, або приводять до дисбалансу в політичній чи економічні сферах. Так, близько 26,3% ударів кібервійн спрямовані проти США, при чому доля Китаю в цьому складає 31,6% [178]. Лідерами в галузі ведення кібервійн проти інших країн є Китай та Росія, хоча Іран, США, Великобританія та ряд інших країн щільно займаються цим питанням (рисунок 3.24).

Окрім цього можна виділити таку форму інформаційної війни, як промислове кібершпигунство, яке направлене на підрив діяльності крупних компаній. Найбільшими жертвами в цьому є підприємства роздрібної торгівлі, IT-компанії та уряд (рисунок 3.24), хоча промислові компанії та фінансово-кредитні установи за показниками інформаційних атак також наближаються до лідерів. Це пов'язано не тільки з тим, що діяльність злочинців спрямована на викрадення фінансової інформації саме цих важливих для економіки об'єктів, але й це також відбувається за рахунок слабкої організації їх систем захисту. Даний фактор є характерним для більшості компаній світу та у випадку зберігання подібної тенденції може призвести до важких фінансових наслідків не тільки для них, але й для економіки країни в цілому. Так, на рисунку 3.25 представлено інфографіку основних фінансових наслідків, отриманих в результаті здійснення інформаційних війн.

Фінансові втрати від кібервійн по всьому світу склали 0,8% від світового ВВП у 2018 році. При цьому прогнозується зростання збитків у геометричній прогресії, що буде складати щорічно близько 6 трлн. дол. у 2021 році (рисунок 3.25). На долю Азіатсько-Тихоокеанського регіону припадає близько 1,745 трлн. дол. економічних втрат, що говорить про зростання його важливості для кіберзлочинців, оскільки сьогодні в багатьох країнах даного регіону зосереджені великі IT-компанії та нафтові підприємства. Набуває популярності кібершахрайства із криптовалютами. Так, було виявлено близько 76 млрд. доларів незаконних операцій із криптовалютою, що наближається за світовими обсягами до незаконних операцій із наркотиками [178]. Окрім цього набувають поширення кіберзлочини, які здійснюються за допомогою цифрової реклами, що прогнозується досягти 44 млрд. доларів у 2022 році [178]. Як правило, дані операції призводять до легалізації цих коштів, що врешті-решт негативно впливає на розвиток економіки будь-якої країни.

Рисунок 3.25 – Інфографіка основних фінансових наслідків інформаційних війн
Джерело дослідження: побудовано авторкою на основі [178, 85, 37]

Країнами світу ведеться боротьба із наслідками інформаційних війн, що полягає у посиленні заходів інформаційної безпеки в цілому та кібербезпеки зокрема. Так, у 2019 році світові витрати на захист інформації склали 124 млрд. дол., що перевищує їх суму у 2018 році (114 млрд. дол.). Прогнозується її зростання у 2022 році до 170,4 дол. [178]. Окрім цього можна виділити таку проблему, як неякісне програмне забезпечення для захисту даних. У 2021 році світові втрати від його функціонування склали 20 млрд. дол., що перевищило даний показник у попередні роки практично у 2 рази (рисунок 3.25). Також зростають витрати компаній на підготовку фахівців у галузі захисту інформації.

Прогнозується збільшення даного показника до 10 млрд. дол. у 2027 році, в порівнянні з 1 млрд. дол. у 2014 році [178]. При цьому негативні аспекти від впливу кібервійн проявляються також й в тому, що компанії мають проблеми, пов'язані із подальшою їх діяльністю. Тобто багатьом з них (60%) дуже важко відновлювати інформацію та продовжувати свою роботу на попередньому рівні (рисунок 3.25). Особливо це проблематично для малих підприємств, які можуть потребувати підтримки з боку держави.

Таким чином, інформаційні війни здійснюють вплив на різні сфери діяльності та результатом цього, як правило, є зростання фінансових збитків та витрат, пов'язаних із підвищенням ефективності систем захисту. Дана проблема вимагає пошуку універсальних підходів, реалізація яких дозволила б спрогнозувати потенційні результати для окремої країни, отримані в процесі реалізації інформаційних війн. Саме тому пропонуємо використовувати підхід ударної хвилі, який дозволить сприймати виникнення наслідків кібервійн у якості «інформаційних бульбашок».

«Інформаційною бульбашкою» є певна подія, яка непередбачувана та відбувається не на постійній основі, але її виникнення призводить до конкретних результатів, за часту до збільшення негативних наслідків протягом певного часу. У якості такої «бульбашки» може виступати один із розповсюджених заходів інформаційної війни інформаційна атака, сутність якої полягає у швидкому та стрімкому зростанні інформаційних активностей у інформаційному середовищі стосовно конкретного об'єкту, проти якого спрямована атака. Це все, як правило, призводить до паразитарного вкиду (вивільнення енергії), коли спостерігається найбільший обсяг активностей, та завершується розривом такої «інформаційної бульбашки». Після цього протягом певного періоду відбуваються коливання інформаційних сутностей, що відображають результати подій реального сектору, які інформаційно ідентифіковані у глобальному інформаційному просторі. Наслідки від цього можуть зростати у геометричній прогресії та привести до економічної дестабілізації країни. Специфічні особливості та масштаби виникнення «інформаційних бульбашок» як негативних наслідків

інформаційних війн, в свою чергу, визначають вектори їх поширення в економічній та соціальній сферах та впливають на різні канали. Все це формує передумови для можливої математичної формалізації розповсюдження наслідків інформаційних атак як факторів економічної дестабілізації країни у вигляді розриву «інформаційної бульбашки» – ударно-хвильової моделі Сєдова-Тейлора. Застосування зазначеного підходу до моделювання полягає у доцільності формуванні основної гіпотези щодо наявності «інформаційних бульбашок» та їх розривів як передвісників процесів економічної дестабілізації країни в розрізі інформаційного поля.

Модель Сєдова-Тейлора [210, 231], яка дозволяє описати ударну хвилю, має вигляд формули (3.17):

$$R_s(t) = a \cdot t^b,$$
$$b = \frac{s+2}{n+2},\ a = \left(\frac{E_d/\left(\tau_0^s l_0^{3-n}\right)}{\rho}\right)^{1/(n+2)}, \tag{3.17}$$

де n – просторовий вимір ($n=1$ для плоского простору, $n=2$ для циліндричного простору, $n=3$ для сферичного простору);

s – фактор швидкості виділення енергії ($s=0$ для випадку миттєвого виділення, $s=1$ для випадку виділення з постійною швидкістю);

E_d – енергія, що виділяється при детонації і має наступні характеристики: l_0 - довжина, τ_0 - час;

ρ – щільність атмосферного повітря.

Адаптуємо формулу (3.17) для опису моделі ударної хвилі розповсюдження наслідків інформаційних війн як факторів дестабілізації економіки країни. Оскільки в процесі опису соціально-економічної системи втрачає сенс просторова характеристика, кожен спектр вертикального (макро- та мікрорівень) та горизонтального (держави та економічних агентів) секторів буде мати власний канал розповсюдження, а замість просторових характеристик виникає необхідність використання фактору часу. Запишемо формулу, яка

дозволить кількісно описати «тиск» ударної хвилі розриву «інформаційної бульбашки» та тенденцію його згасання, що супроводжує процес послідовного розсіювання енергії – проявів та каналів економічної дестабілізації країни. Модель Сєдова-Тейлора з урахуванням адаптації набуває вигляду (3.18) [280]:

$$\Delta R(t) = \frac{E}{t^4} + a_1\left(\frac{E}{t^4}\right)^{3/4} + a_2\left(\frac{E}{t^4}\right)^{2/4} + a_3\left(\frac{E}{t^4}\right)^{1/4}, \quad (3.18)$$

де $\Delta R(t)$ – зміна інформаційних активностей у глобальному цифровому просторі, що ідентифікує інформаційну атаку, яка здійснюється у вигляді інформаційних вкидів та відбувається за період t;

E – енергія в початковий момент після розриву бульбашки, що в нашому випадку пропонується інтерпретувати як результат, пов'язаний із втратою інформаційних активностей, які ідентифікують події реального сектору цифрової економіки;

t – період часу після розриву «інформаційної бульбашки» (кількість днів);

a_1, a_2, a_3 – характеристики середовищ поширення ударних хвиль наслідків інформаційних атак.

Оскільки виникає необхідність мінімізації втрат реального сектору, наслідки чого ідентифікуються у вигляді інформаційних сутностей у глобальному інформаційному просторі, що виступають однією із форм прояву «інформаційної війни», розглянемо модель Сєдова-Тейлора з точки зору оптимізаційної задачі нелінійного програмування з урахуванням різних варіантів «інформаційної бульбашки» та напрямків дестабілізації. Для цього в розрізі кожного із них необхідно ідентифікувати «вид інформаційної атаки» та відповідно розрив «інформаційної бульбашки», яка буде характеризувати ударну хвилю, що виникла та повинна поступово розсіятися. Таким чином, параметри моделі (3.18) мають забезпечити мінімально можливий рівень втрат інформаційних активностей, які ідентифікують наслідки розриву бульбашки у реальному секторі для кожного прояву дестабілізації економіки країни,

наприклад, банківської сфери, підприємств, держави в цілому. Враховуючи наведені аргументи, оптимізаційна задача моделювання розповсюдження наслідків інформаційних атак як фактору економічної дестабілізації країни з урахуванням різних їх проявів та каналів набуває загального (універсального) вигляду (3.19):

$$\begin{cases} U_i \to min \\ U_i = \sum_{j=1}^{V} U_{ij}^{t_j} = \\ = \sum_{j=1}^{V} \left(\frac{z_{t_j}^i}{\tau_j^i} + a_1 \left(\frac{z_{t_j}^i}{\left(\tau_j^i\right)^2} \right)^{3/4} + a_2 \left(\frac{z_{t_j}^i}{\left(\tau_j^i\right)^3} \right)^{2/4} + a_3 \left(\frac{E z_{t_j}^i}{\left(\tau_j^i\right)^4} \right)^{1/4} \right), \end{cases} \quad (3.19)$$

де U_i – розсіювання енергії ударної хвилі в і-му каналі поширення економічної дестабілізації країни;

V – кількість видів інформаційних війн (хакерські атаки, кібершпигунство, інформаційна пропаганда, тощо);

$z_{t_j}^i$ – значення початкової енергії в момент часу t_j, тобто початкові значення інформаційних активностей для відповідних каналів поширення до початку здійснення інформаційної війни;

t_j – момент часу початку *j*-ого виду інформаційної війни в *i*-му напрямку дестабілізації економіки країни;

τ_j^i – тривалість *j*-ого виду інформаційної війни в *i*-му напрямку дестабілізації економіки країни.

Застосування формули (3.19) дозволить змоделювати ситуацію розповсюдження наслідків різних видів інформаційних війн, які проявляються у вигляді інформаційної ідентифікації результатів, отриманих суб'єктами реального сектору: фінансових втрат для підприємств, банків, держави.

У дисертаційній роботі для моделювання реакції економічних агентів у глобальному цифровому економічному просторі на розриви «інформаційних

бульбашок» були обрані кількісні критерії: значення інформаційних активностей (сутностей) у глобальному цифровому просторі, які характеризують поведінку суб'єктів цифрової економіки та різні види кіберзагроз. Так, було отримано щоденні дані на основі результатів запиту глобальної веб-статистики (Global Web Statistics "Statoperator") за період з 05.08.2017 по 20.10.2017 [104]. Розраховане значення коефіцієнту кореляції між ними дорівнює 0,52, що свідчить про помітний зв'язок та можливість використання даних для побудови моделі Сєдова-Тейлора.

На основі рівнів, обраних для дослідження двох часових рядів, були ідентифіковані «інформаційні бульбашки» та прояви їх розриву для даних інформаційних активностей щодо кіберінцидентів: 29.11.2017, 26.11.2018, 03.12.2019, 19.06.2020 (рисунок 3.26). Зазначені дати чітко ідентифікуються як аномальні рівні у вигляді несподіваного стрімкого стрибка з подальшим встановленням попереднього рівня відповідного рівня часового ряду. Для кожного з виділених проявів розриву «інформаційної бульбашки» кількісні показники відображають зміну «маси», яка носить стрибкоподібний характер, і при цьому визначає енергію, яку буде переносити відповідна ударна хвиля.

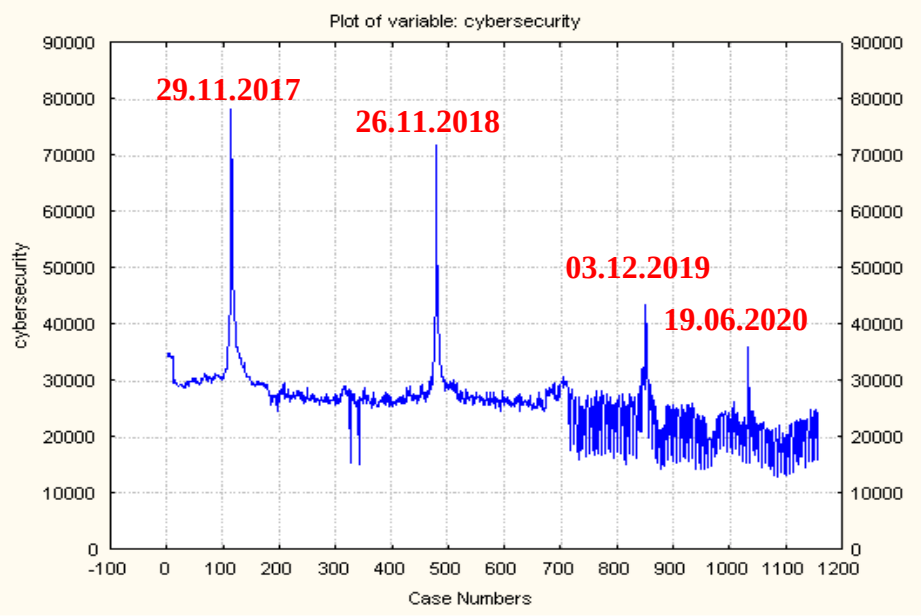


Рисунок 3.26 – Виявлені періоди розривів «інформаційних бульбашок» у глобальному цифровому просторі за даними інформаційних активностей, що ідентифікують кіберзагрози, з 05.08.2017 до 20.10.2020 (складено авторкою)

На рисунку 3.27 представлена динаміка інформаційних активностей, які характеризують поведінку суб'єктів цифрової економіки у інформаційному просторі.

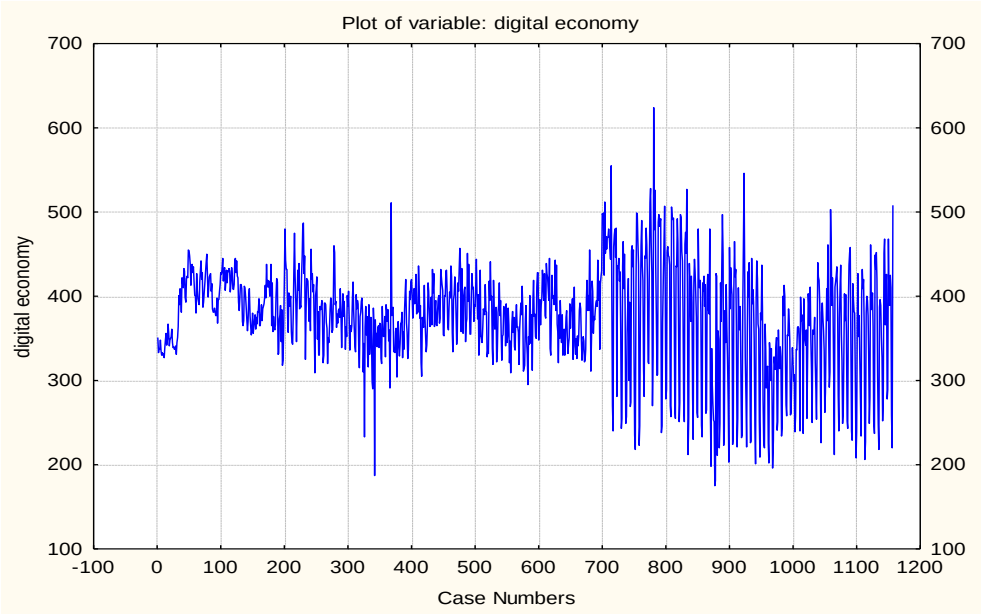


Рисунок 3.27 – Динаміка інформаційних активностей, які характеризують поведінку суб'єктів цифрової економіки, з 05.08.2017 по 20.10.2020 (складено авторкою)

Починаючи із зазначених дат розриву «інформаційної бульбашки» ударна хвиля у будь-якому разі буде розповсюджуватися, однак може і не дійти до реального сектору чи, дійшовши, не завдати значного впливу. Тому проведемо розрахунки початкових енергій розривів у моменти удару за формулою (3.18) (див. табл. 3.12).

Таблиця 3.12 - Початкові енергії розривів у моменти удару

Дата	Кіберзагрози	Цифрова економіка	ΔR	E/t4	(E/t4)^3/4	(E/t4)^2/4	(E/t4)^1/4
27.11.2017	78044	405	-25	32,50	13,61	5,70	2,39
26.11.2018	71898	433	75	29,95	12,80	5,47	2,34
03.12.2019	43396	480	224	18,07	8,77	4,25	2,06
19.06.2020	36057	375	17	15,02	7,63	3,88	1,97

Для формалізації моделі Сєдова-Тейлора, яка використовується для опису моделі ударної хвилі розповсюдження наслідків інформаційних атак в процесі

дестабілізації сектору цифрової економіки країни, виникає необхідність визначення періоду часу після розриву «інформаційної бульбашки» (кількість днів) щодо її розповсюдження. Для вирішення даного питання проведемо автокореляційний аналіз із використанням аналітичного пакету «STATISTICA» та побудуємо корелограми нульових різниць для обох часових рядів – рівня активностей щодо кіберзагроз та цифрової економіки (рисунки 3.28-3.31).

	Autocorrelation Function (Spreadsheet7) cybersecurity (Standard errors are white-noise estimates)			
Lag	Auto-Corr.	Std.Err.	Box & Ljung Q	p
1	0,839112	0,029361	816,767	0,00
2	0,696489	0,029348	1379,969	0,00
3	0,634138	0,029336	1847,250	0,00
4	0,608598	0,029323	2278,023	0,00
5	0,611561	0,029310	2713,379	0,00
6	0,690392	0,029297	3268,685	0,00
7	0,748913	0,029285	3922,691	0,00
8	0,640405	0,029272	4401,328	0,00
9	0,526176	0,029259	4724,726	0,00
10	0,487890	0,029246	5003,015	0,00
11	0,473660	0,029234	5265,538	0,00
12	0,488874	0,029221	5545,439	0,00

Рисунок 3.28 – Значення автокореляційної функції нульових різниць часового ряду активностей щодо кіберзагроз (складено авторкою)

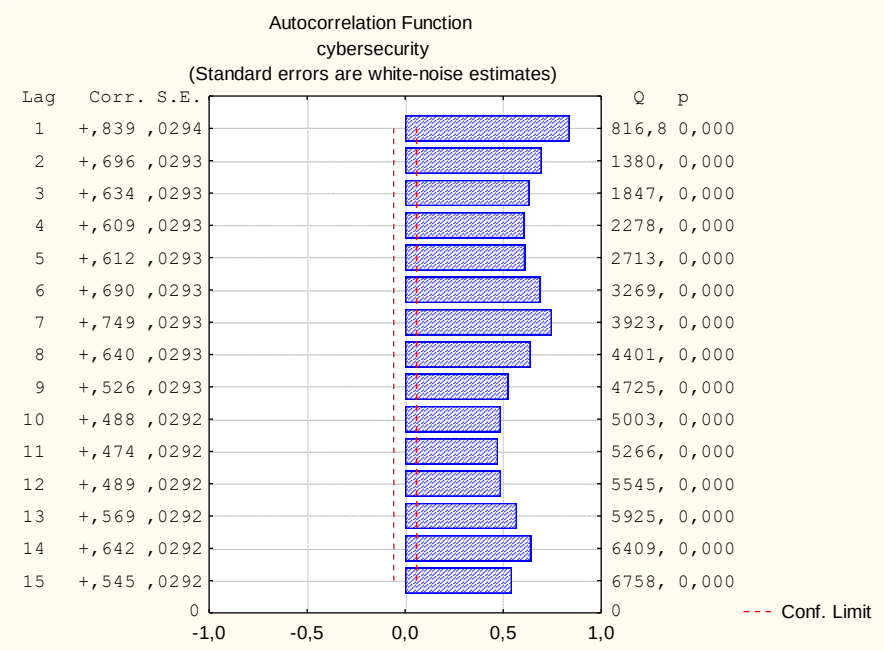


Рисунок 3.29 – Корелограма нульових різниць часового ряду активностей щодо кіберзагроз (складено авторкою)

Lag	Autocorrelation Function (Spreadsheet7) digital economy (Standard errors are white-noise estimates) Auto-Corr.	Std.Err.	Box & Ljung Q	p
1	0,492937	0,029361	281,865	0,00
2	0,065055	0,029348	286,779	0,00
3	-0,061062	0,029336	291,111	0,00
4	-0,072860	0,029323	297,285	0,00
5	0,034030	0,029310	298,633	0,00
6	0,412232	0,029297	496,615	0,00
7	0,702627	0,029285	1072,279	0,00
8	0,404279	0,029272	1263,026	0,00
9	0,010894	0,029259	1263,165	0,00
10	-0,090965	0,029246	1272,839	0,00
11	-0,093841	0,029234	1283,143	0,00
12	-0,001421	0,029221	1283,145	0,00

Рисунок 3.30 – Значення автокореляційної функції нульових різниць часового ряду активностей щодо цифрової економіки (складено авторкою)

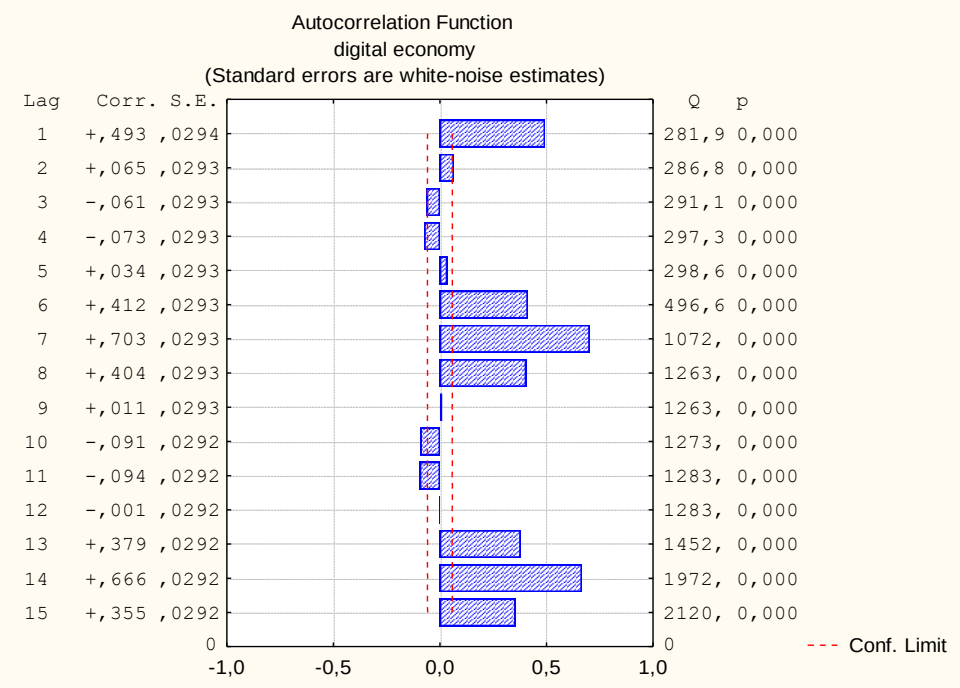


Рисунок 3.31 – Корелограма нульових різниць часового ряду активностей щодо цифрової економіки (складено авторкою)

Аналіз рисунків 3.28 та 3.29 в розрізі автокореляційної функції та графічного її представлення у вигляді корелограми дозволяє зробити висновок про наявність періодичних коливань рівнів часового ряду активностей щодо кіберзагроз кожні 7 днів. Аналогічна ситуація спостерігається й в розрізі

часового ряду активностей щодо цифрової економіки (рисунки 3.30–3.31), тому в якості періоду часу після розриву «інформаційної бульбашки» (кількість днів) щодо її розповсюдження, пропонується обрати 7 денний період часу.

Наступним етапом формалізації моделі Сєдова-Тейлора, яка використовується для опису моделі ударної хвилі розповсюдження наслідків інформаційних атак в ході дестабілізації процесів реального сектору цифрової економіки, виступає необхідність визначення коефіцієнтів моделі розсіювання енергії ударних хвиль. Для цього, враховуючи дані таблиці 3.12 щодо початкових рівнів енергії розривів у моменти криз та ідентифікований за допомогою автокореляційного аналізу семиденний період часу після розриву «інформаційної бульбашки» щодо її розповсюдження її наслідків, запишемо оптимізаційну модель (3.19) у вигляді системи рівнянь (3.20). Зазначимо, що для формування системи обмежень були використані рівності в розрізі кожного моменту розриву «інформаційної бульбашки», в яких значення функції Сєдова-Тейлора дорівнювали абсолютним приростам поточного рівня часового ряду активностей щодо цифрової економіки до їх попереднього рівня.

$$\begin{cases} \frac{78044}{7^4} + a_1\left(\frac{78044}{7^4}\right)^{\frac{3}{4}} + a_2\left(\frac{78044}{7^4}\right)^{\frac{2}{4}} + a_3\left(\frac{78044}{7^4}\right)^{\frac{1}{4}} \to min \\ \frac{78044}{7^4} + a_1\left(\frac{78044}{7^4}\right)^{\frac{3}{4}} + a_2\left(\frac{78044}{7^4}\right)^{\frac{2}{4}} + a_3\left(\frac{78044}{7^4}\right)^{\frac{1}{4}} = -25 \\ \frac{71898}{7^4} + a_1\left(\frac{71898}{7^4}\right)^{\frac{3}{4}} + a_2\left(\frac{71898}{7^4}\right)^{\frac{2}{4}} + a_3\left(\frac{71898}{7^4}\right)^{\frac{1}{4}} = 75 \\ \frac{43396}{7^4} + a_1\left(\frac{43396}{7^4}\right)^{\frac{3}{4}} + a_2\left(\frac{43396}{7^4}\right)^{\frac{2}{4}} + a_3\left(\frac{43396}{7^4}\right)^{\frac{1}{4}} = 224 \\ \frac{36057}{7^4} + a_1\left(\frac{36057}{7^4}\right)^{\frac{3}{4}} + a_2\left(\frac{36057}{7^4}\right)^{\frac{2}{4}} + a_3\left(\frac{36057}{7^4}\right)^{\frac{1}{4}} = 17 \end{cases} \quad (3.20)$$

Пошук у формулі (3.20) коефіцієнтів Сєдова-Тейлора для опису моделі ударної хвилі розповсюдження наслідків інформаційних атак в ході дестабілізації процесів реального сектору економіки здійснювався із

використанням інструментарію MS Excel «Пошук рішення» (метод ОПГ – метод узагальненого приведеного градієнта) (рисунок 3.32).

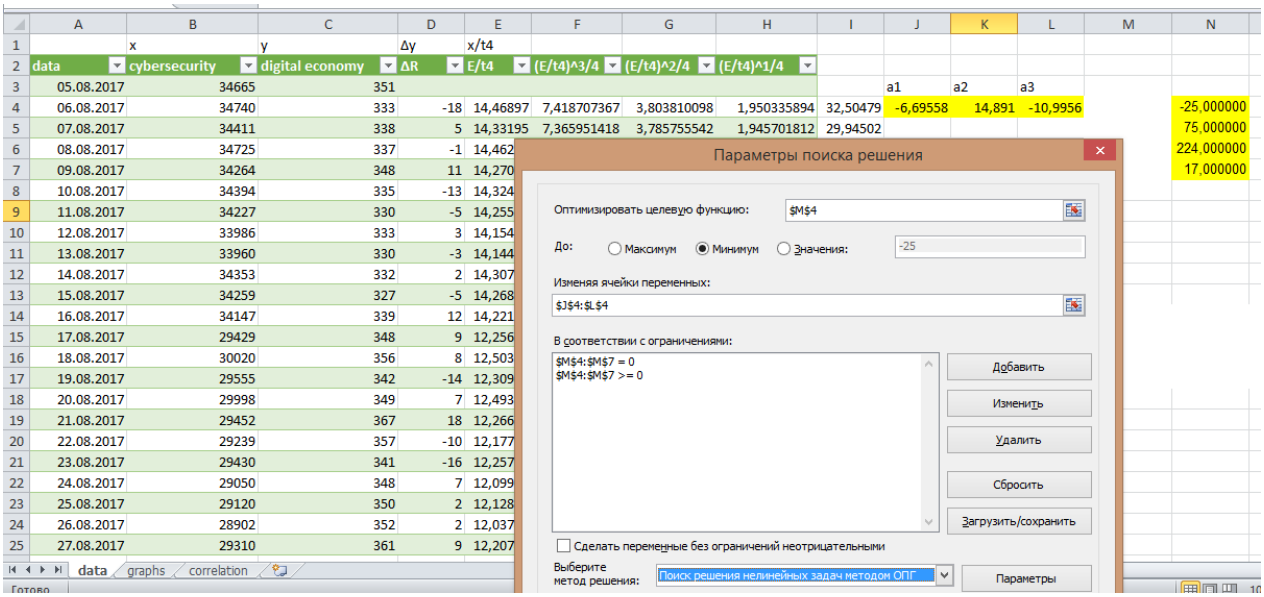


Рисунок 3.32 – Вікно «Пошук рішення» MS Excel для вирішення оптимізаційної задачі пошуку коефіцієнтів Сєдова-Тейлора (складено авторкою)

Безпосереднє вирішення системи рівнянь (3.20) відбувалося за допомогою програмного додатку «Mathcad», що дозволило сформувати модель Сєдова-Тейлора для опису ударної хвилі розповсюдження наслідків інформаційних атак в ході дестабілізації процесів реального сектору цифрової економіки у вигляді рівняння (3.21):

$$y(x) := x + -1735.63859 \cdot x^{\frac{3}{4}} + 7526.0874 \cdot x^{\frac{2}{4}} + -8088.55 \cdot x^{\frac{1}{4}},$$

$$\Delta R(t) = \frac{E}{t^4} - 1735{,}64 \cdot \left(\frac{E}{t^4}\right)^{\frac{3}{4}} + 7526{,}09 \cdot \left(\frac{E}{t^4}\right)^{\frac{2}{4}} - 8088{,}55 \cdot \left(\frac{E}{t^4}\right)^{\frac{1}{4}}. \quad (3.21)$$

З метою візуалізації моделі розповсюдження ударної хвилі після розриву «інформаційної бульбашки» побудуємо рисунок 3.33 у програмному додатку «Mathcad». Аналіз даного рисунку свідчить про наявність точки розриву другого роду, що супроводжує розрив «інформаційної бульбашки» з подальшою

адаптацією системи і боротьбою з наслідками ударної хвилі, про що свідчить характер зростаючої кривої.

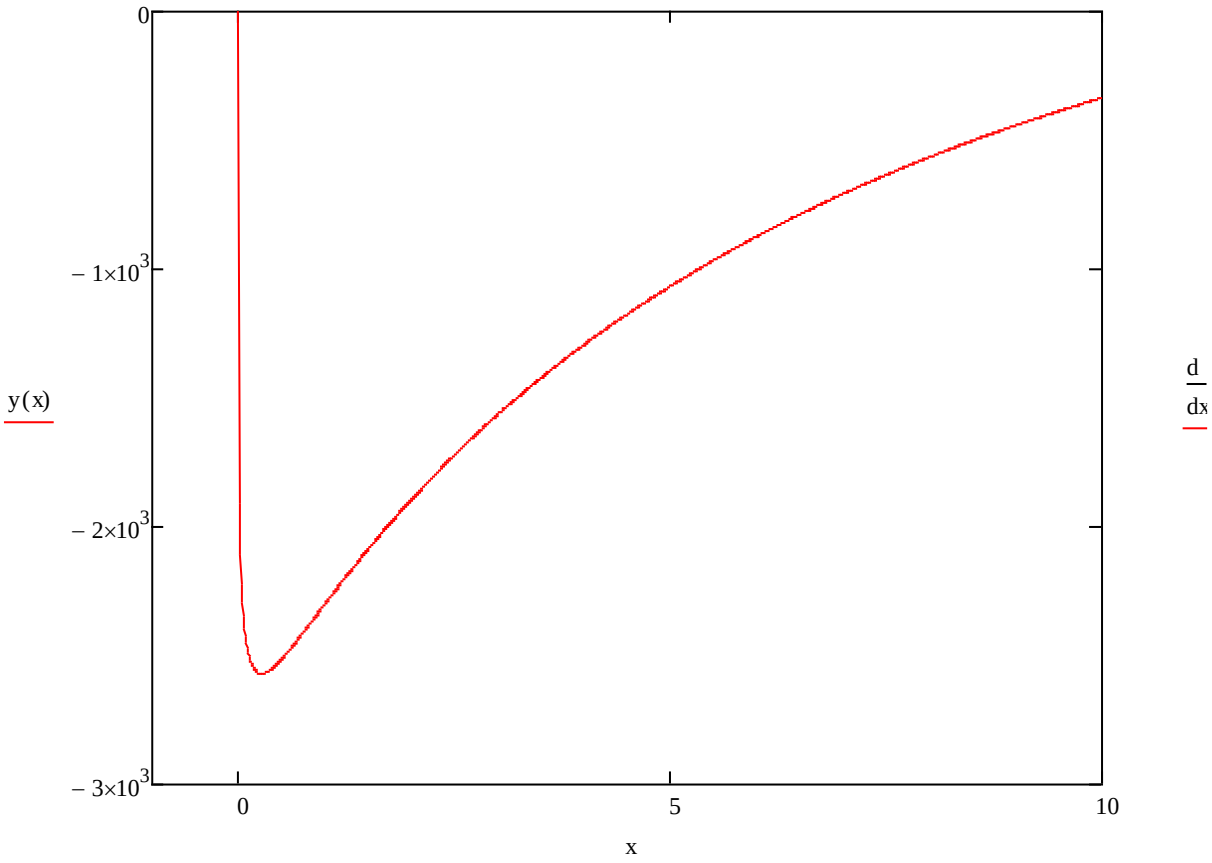


Рисунок 3.33 – Графічне представлення моделі Сєдова-Тейлора для опису ударної хвилі розповсюдження наслідків інформаційних атак в ході дестабілізації процесів реального сектору цифрової економіки країни (складено авторкою)

Прирівнюючи до нульового значення функцію (3.21), визначимо значення змінної $\frac{E}{t^4}$, за якого абсолютний приріст поточного рівня активностей щодо цифрової економіки до попереднього рівня буде набувати нульового. Результат представлений у вигляді матриці (3.22):

$$\begin{pmatrix} 2.845857250858869264 2e12 \\ 0.2588066593121824041 - 4.781365653050416083 6e-22i \\ 22.701480114635548483 + 4.478085629413948928 9e-21i \end{pmatrix} \quad (3.22)$$

Отримане значення $\frac{E}{t^4} = 2{,}82 \cdot 10^{12}$ свідчить про наявність постійної волатильності рівня активностей щодо цифрової економіки і майже неможливість досягнення нею нульового значення її абсолютного приросту.

Використовуючи апарат диференціального числення, необхідно провести додаткове дослідження: 1) точок перегину функції, тобто ідентифікувати рівні активностей щодо кіберзагроз, за яких буде змінюватися поведінка результативної ознаки (рівня цифрової економіки) при їх зростанні/зменшенні; 2) екстремальних точок функції, тобто знайти значення рівня активностей щодо кіберзагроз, за яких буде досягнуто максимально та мінімально можливі рівні активностей щодо цифрової економіки.

Для вирішення першої задачі визначимо першу похідну від функції (3.21) за відповідною змінною:

$$\frac{\mathrm{d}}{\mathrm{dx}}\mathrm{y(x)} \rightarrow \frac{3763.0437}{\sqrt{\mathrm{x}}} - \frac{1301.7289425}{\mathrm{x}^{\frac{1}{4}}} - \frac{2022.1375}{\mathrm{x}^{\frac{3}{4}}} + 1 \qquad (3.23)$$

Графічне представлення функції (3.23) наведемо на рисунку 3.34.

Аналіз рисунку 3.34 дозволяє зробити висновок про зростання рівня інформаційних активностей щодо цифрової економіки при зростанні рівня інформаційних активностей щодо кіберзагроз одразу після розриву «інформаційної бульбашки» до рівня 0,879 змінної $\frac{E}{t^4}$, при цьому рівень абсолютного приросту активностей щодо цифрової економіки складе 536 од. Це відбуватиметься на наступний після розриву «інформаційної бульбашки» день. Після даної точки зростання рівня інформаційних активностей щодо кіберзагроз буде супроводжуватися зниженням рівня інформаційних активностей щодо цифрової економіки.

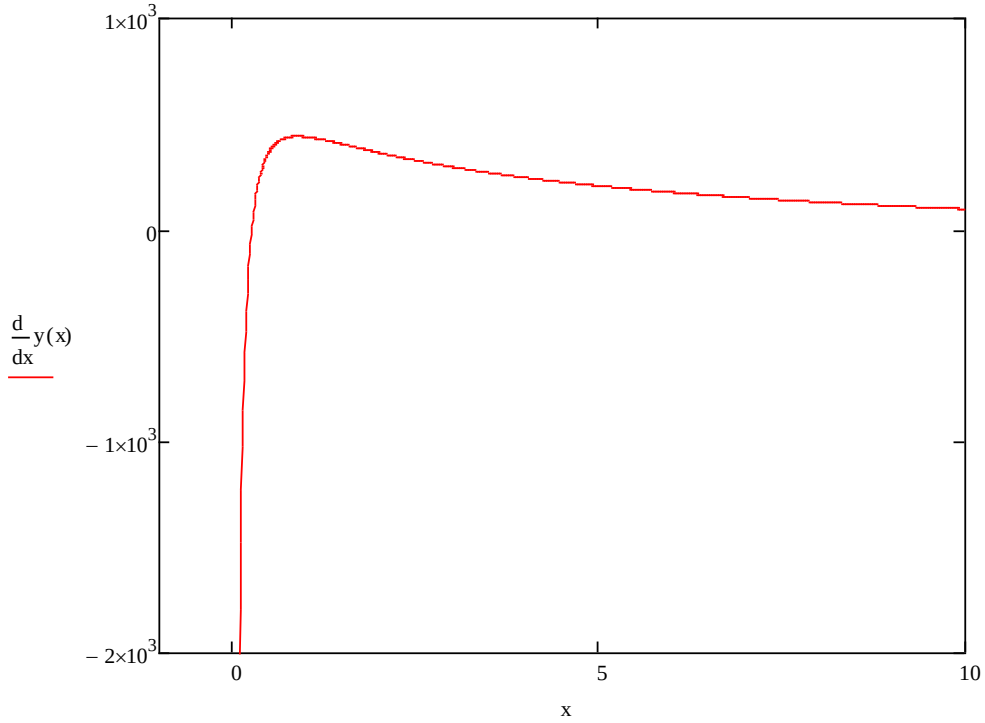


Рисунок 3.34 – Графічне представлення функції першої похідної моделі Сєдова-Тейлора для опису ударної хвилі розповсюдження наслідків інформаційних атак в ході дестабілізації процесів реального сектору цифрової економіки країни (складено авторкою)

Прирівнюючи до нуля функцію (3.23), отримаємо її розв'язок (3.24) із використанням програмного додатку «Mathcad»:

$$\frac{3763.0437}{\sqrt{x}} - \frac{1301.7289425}{x^{\frac{1}{4}}} - \frac{2022.1375}{x^{\frac{3}{4}}} + 1 = 0,$$

$$\begin{pmatrix} 0 \\ 8.984284529539317903 3e12 \\ 32.505056786866615254 + 8.233738853687931603e-21i \\ 14.657107438939712642 - 5.528986083971500360 7e-21i \end{pmatrix}. \quad (3.24)$$

Переходячи до вирішення другої задачі визначення екстремальних точок функції, тобто значень рівня активностей щодо кіберзагроз, за яких буде досягнуто

максимально та мінімально можливі рівні активностей щодо цифрової економіки, візьмемо другу похідну функції Сєдова-Тейлора (3.21), яка набуває вигляду (3.25):

$$\frac{d^2}{dx^2}y(x) \to \frac{325.432235625}{x^{\frac{5}{4}}} + \frac{1516.603125}{x^{\frac{7}{4}}} - \frac{1881.52185}{x^{\frac{3}{2}}} \tag{3.25}$$

Прирівнюючи до нуля функцію (3.25), отримаємо розв'язок (3.26):

$$\frac{325.432235625}{x^{\frac{5}{4}}} + \frac{1516.603125}{x^{\frac{7}{4}}} - \frac{1881.52185}{x^{\frac{3}{2}}} = 0$$

$$\begin{pmatrix} 0.8786745740009670 8478 \\ 536.8061068772862 5341 \end{pmatrix} \tag{3.26}$$

Графічне представлення функції другої похідної моделі Сєдова-Тейлора для опису ударної хвилі розповсюдження наслідків інформаційних атак в ході дестабілізації процесів реального сектору цифрової економіки країни (рисунок 3.35) дозволяє визначити екстремальне мінімально можливе значення абсолютного приросту рівня активностей щодо цифрової економіки в районі -80 од. при рівні змінної $\frac{E}{t^4}$, в районі 1,5 од. При цьому стабілізація рівня інформаційних активностей цифрової економіки почнеться після 10 дня.

Таким чином, було запропоновано застосування ударно-хвильової моделі Сєдова-Тейлора для моделювання розповсюдження наслідків інформаційних атак як фактору дестабілізації процесів реального сектору цифрової економіки країни. Дану модель було адаптовано під умови розповсюдження наслідків для каналів, які представлені у сфері цифрової економіки. Її реалізація дозволила визначити кількість бульбашок у світі в трирічній ретроспективі, середню тривалість періоду поширення дезінформації внаслідок глобальних кіберінцидентів, середній період дестабілізації цифрових економічних операцій після розриву бульбашки, відповідні значення інформаційних активностей.

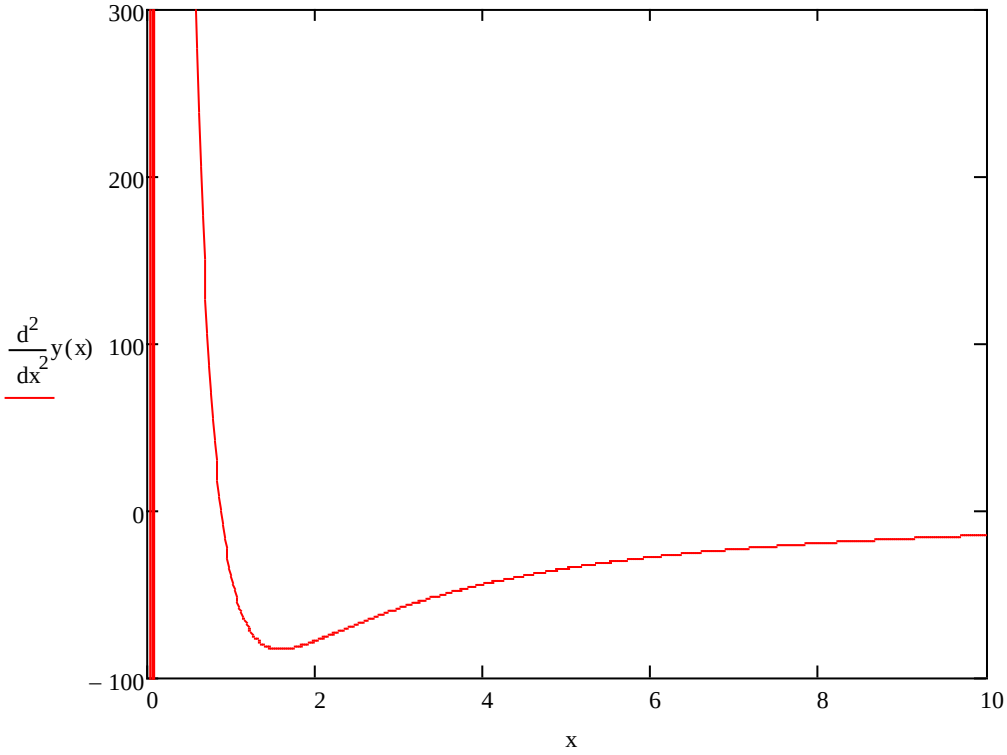


Рисунок 3.35 – Графічне представлення функції другої похідної моделі Сєдова-Тейлора для опису ударної хвилі розповсюдження наслідків інформаційних атак в ході дестабілізації процесів реального сектору цифрової економіки країни (складено авторкою)

Подібні моделі є формою інформаційною зброї, що здатна надати максимальний ефект, оскільки допомагає виявити ряд загрозливих чинників дестабілізації держави, встановити найбільш вразливі ділянки системи інформаційної безпеки, та спрогнозувати потенційні варіанти розвитку подій, щоб мати можливість завчасно передбачити можливі негативні наслідки інформаційних війн. Тому пропонується її використання для прогнозування появи можливих «інформаційних бульбашок», згенерованих інформаційними активностями у глобальному цифровому просторі, а також для передбачення кількісних та часових характеристик розповсюдження наслідків їх розриву. Це дозволить державним органам запровадити систему попереджувальних заходів, що сприятимуть максимальному нівелюванню впливу інформаційних атак на реальний сектор. Застосування даної моделі є доцільним для груп реагування на кіберінциденти та інформаційні війни.

Висновки до розділу 3

1. У підрозділі 3.1 дисертаційної роботи було висунуто гіпотезу, що заходи забезпечення персональної інформаційної безпеки, яким надає перевагу населення тієї чи іншої країни, істотно залежать від рівня його добробуту, а також національних суспільних традицій, ментальних і культурних особливостей, що формують ставлення населення до організації власної інформаційної безпеки та обізнаність щодо можливих наслідків її порушення. Для емпіричної перевірки цієї гіпотези використано результати моніторингу громадської думки в країнах-членах ЄС, що здійснювався в межах програми Євробарометр у 2014 та 2019 рр. Інструментарієм дослідження став кластерний аналіз за методом k-means, проведений із використанням аналітичної платформи «Deductor Academic».

2. Розрахунки дозволили підтвердити висунуту гіпотезу, а саме було: виділено 7 кластерів країн ЄС за домінуючими заходами персональної інформаційної безпеки та наслідками її порушення; проведено порівняльний аналіз кластерів країн на основі їх рівня ВВП на душу населення; здійснено візуалізацію результатів шляхом побудови карти країн. Так, було доведено, що більшість країн є близькими як за рівнем ВВП на душу населення, так і за географічним розміщенням, для яких характерним є близькість історично сформованих суспільних традицій.

3. У підрозділі 3.2 дисертаційної роботи досліджено зв’язок між рівнем кібербезпеки країни та ймовірністю її використання як потенційного об’єкта в процесах легалізації кримінальних доходів і відмивання брудних коштів. Інструментарієм дослідження стало системне поєднання гравітаційного моделювання та методу експертного оцінювання, об’єктами – 70 країн світу, періодом для розрахунків обраний 2018 р. Результати засвідчили, що врахування національного індексу кібербезпеки як додаткової змінної в гравітаційній моделі для досліджуваних країн змінює рівень їх привабливості для операцій, пов’язаних із відмиванням коштів.

4. Визначено перелік країн світу, які з урахуванням рівня їх кібербезпеки сформували свою привабливість для українських контрагентів з огляду на здійснення операцій з легалізації незаконно отриманих доходів: 1) п'ятірка найбільш привабливих країн (із середнім рівнем кібербезпеки 40,52) – Болівія, Індія, Гватемала, Гана, Туреччина; 2) п'ятірка найменш привабливих країн (із середнім рівнем кібербезпеки 65,71) – Данія, Норвегія, Фінляндія, Нова Зеландія та Ісландія. Отримані результати засвідчили, що низький рівень кібербезпеки є одним із факторів, який сприяє збільшенню незаконних операцій у країні. З іншого боку, зростання його рівня забезпечує формування більш потужного інструментарію щодо виявлення таких операцій. Водночас Україна є привабливою для легалізації незаконних доходів контрагентами з Кенії, Індії, Гватемали, Гани, Болівії та ін. та менш привабливою для Данії, Естонії, Ісландії, Норвегії, Нової Зеландії та ін. Одержані результати формують наукове підґрунтя розроблення рекомендацій щодо посилення контролю за операціями, які здійснюють контрагенти визначених країн.

5. У підрозділі 3.3 дисертаційної роботи зазначено, що інструментами ведення інформаційних війн є інформаційні атаки, хакерські кібератаки, кібершпигунство, пропаганда та інші, мета застосування яких пов'язана із викраденням, викривленням, знищенням інформації «потенційного» противника. Також було проаналізовано ряд показників, які характеризують інформаційні війни. Їх статистичні значення свідчать про зростання даної проблеми у всьому світі, що говорить про можливості виникнення озброєних конфліктів між країнами як наслідки ведення інформаційних війн між ними. У роботі було проаналізовано також й основні фінансові наслідки, отримані в результаті кібервійн у світі. Їх прогнозні значення свідчать не тільки про зростання втрат в майбутньому, а також й про збільшення витрат на забезпечення системи інформаційної безпеки. Тобто при відсутності дієвих заходів захисту та зростаючих можливостях для кіберзлочинців прогнозується в цілому несприятлива ситуація у світі, яка буде пов'язана із дестабілізацією різних сфер життєдіяльності, особливо економічної.

6. Було встановлено, що одним із проявів впливу кіберінцидентів на розвиток національної економіки є формування так званих «інформаційних бульбашок» (паразитарних інформаційних вкидів, несанкціонованих витоків інформації, масштабних хакерських атак тощо), що можуть перетворюватися на каталізатори «інформаційних війн» і завдавати істотних збитків реальному та фінансовому секторам національної економіки. Із застосуванням інструментарію «Global Web Statistics» було проведено аналітичне порівняння інформаційних активностей у глобальному цифровому просторі за період із 05.08.2017 до 20.10.2020, пов'язаних, з одного боку, з кіберінцидентами, а з іншого – з відповідною реакцією на це економічних агентів, діяльність яких пов'язана з цифровою економікою: криптовалютами, Інтернетом речей, онлайн-сервісами та банкінгом, електронною комерцією (лінійний коефіцієнт кореляції становить 0,52, що засвідчує наявність істотного зв'язку). Аналіз засвідчив, що у світі впродовж досліджуваного періоду чотири рази було зафіксовано масштабне інформаційне перевантаження внаслідок кібератак, яке призвело до розриву «інформаційних бульбашок». На основі побудованих автокореляційних функцій зроблено висновок, що період, упродовж якого відбувалося масове кумулятивне поширення дезінформації, в середньому дорівнює 7 дням. З використанням моделі Сєдова – Тейлора (для розрахунків використано аналітичні пакети «Mathcad», «STATISTICA», «MS Excel») визначено, що стабілізація глобального цифрового економічного простору розпочинається після десятого дня від розриву бульбашки. Отримані результати можуть стати методологічним підґрунтям для державних органів, які займаються питанням інформаційної безпеки, використовуватися для побудови прогнозів «інформаційних бульбашок» та вживання заходів їх попередження.

Основні положення третього розділу дисертаційної роботи опубліковано авторкою в роботах [169, 388, 394].

РОЗДІЛ 4 НАПРЯМКИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

4.1 Удосконалення методологічних засад обґрунтування таргетів та напрямків реформування системи забезпечення інформаційної безпеки в Україні

Запорукою ефективного функціонування будь-якої системи є всебічне забезпечення функціонування та розвитку її компонентів. Система інформаційної безпеки в цьому випадку також не є виключенням. В процесі її побудови на державному рівні необхідно відповісти на наступні запитання: яким чином відбуватиметься її вплив на національну економіку; які її цільові таргети повинні бути забезпечені у першу чергу; які проблеми можуть виникати в процесі її забезпечення на всіх рівнях національної економіки; які інструменти її забезпечення є найбільш дієвими для попередження потенційних інформаційних загроз. Саме тому існує необхідність у розробці комплексу заходів, реалізація яких дозволить вибудовати систему інформаційної безпеки у відповідності із поставленими завданнями, сформованими з урахуванням відповідей на поставлені запитання.

Одним з таких комплексних заходів є формування ефективної стратегії кібербезпеки країни, яка повинна включати систему заходів, пов’язаних із організацією відповідних інститутів та органів, діяльність яких спрямована на забезпечення кіберзахисту. Стратегія повинна також охоплювати напрямки: формування політики кібербезпеки, розробки відповідної законодавчої бази, освітніх програм, системи відповідальності за кіберзлочини, інвестування у наукові дослідження з питань кіберзахисту, розробки потужних кіберфізичних комплексів, програмного забезпечення для моніторингу, попередження та виявлення кіберзлочинів, тощо. В процесі розробки стратегії важливо розуміти, які аспекти кібербезпеки країни потребують покращення та посилення, а які вже мають потужний базис та вимагають підтримки. Це можливо оцінити в процесі визначення рейтингу країн, який формується за рівнем кібербезпеки.

На тлі зростання в останні десятиліття кількості наукових досліджень, присвячених проблемам кібербезпеки, можна виділити ряд з них, які акцентують увагу саме на формуванні стратегії безпеки на рівні країни. Так, С. Герноуті-Елі [100] досліджує деякі питання, пов'язані із розгортанням національної стратегії кібербезпеки для країни в умовах її взаємодії з іншими країнами. Галинець Д., Мозник Д. та Губеріна Б. [94] на прикладі Національної стратегії кібербезпеки Республіки Хорватія та Плану дій намагаються виявити організаційні проблеми в процесі їх формування та надають рекомендації щодо їх вирішення. Теох С. та Махмуд А. [232] розглядають взаємозв'язок національних стратегій кібербезпеки із цифровою економікою та проводять їх аналіз на предмет впливу на успіх цифрової економіки. Кшетрі Н. та Муругесан С. [155] виділяють ключові елементи національних стратегій кібербезпеки та проводять оцінку їх впливу на місцевому, національному та глобальному рівнях. Костюк Н. [152] досліджує проблеми, які постають перед країнами в умовах створення ефективної національної системи кібербезпеки, та наголошує на необхідності розвитку приватно-державного партнерства у цій сфері. Цей аспект також розглядають Штітіліс Д., Пакутінскас П. та Малінаускайте І. [225], які проводять аналіз національних стратегій кібербезпеки на предмет їх відповідності політиці кібербезпеки та стратегічним напрямкам ЄС та НАТО. П. Якобс, Б. Фон Солмс та М. Гроблер [133] пропонують в рамках забезпечення стратегії кібербезпеки країни створення моделі моніторингу кіберзахисту та реагування на інциденти, яка базується на інтеграції військового потенціалу країни та операційних моделей кібербезпеки.

Існує ряд показників, що застосовуються для рейтингування країн, серед яких виділяється «Національний індекс кібербезпеки», який дозволяє оцінити рівень готовності країн протидіяти кіберзагрозам. Його структура чітко відображає ті складові, які повинна мати будь-яка система національної інформаційної безпеки, оскільки для його розрахунку використовується ряд індикаторів, які стосуються різних аспектів кібербезпеки: правової, організаційної, технічної, освітньої, тощо. Після отримання їх оцінок

відбувається розрахунок узагальненого показника, що здійснюється шляхом знаходження долі сумарної оцінки для країни від сумарної максимальної оцінки. Але даний підхід не враховує важливості показників в процесі формування загального рейтингу, не реагує на випадки, коли вони мають різну амплітуду значень, а також не передбачає використання додаткових характеристик, які б допомогли чітко бачити відхилення від фактичних максимальних оцінок. Тому застосування різних підходів, таких як, наприклад, багатокритеріальний аналіз рішень, дозволить проводити оцінку рейтингів більш зважено, оскільки вони нівелюють згадані недоліки. Хоча дані методи застосовуються в процесі вибору та прийняття рішень, але вони дозволяють ефективно оцінити об’єкти дослідження. Вибір методу оцінки може значно вплинути на формування стратегії інформаційної безпеки для країни, тому треба врахувати результативність методу та його додаткові можливості.

Важливим напрямком у розвитку інформаційної безпеки країни є використання сучасних методів та інструментів, які спрямовані на підвищення її ефективності. Так, Коліні Ф. та Янчевський Л. [147] досліджують можливості використання математичних методів для підвищення ефективності формування стратегій захисту інформації, а саме вони виділяють кластерний аналіз та тематичне моделювання. Н. Фентон та М. Фейл [88] вивчають напрямки використання байєсівських причинно-наслідкових моделей ризику в процесі його оцінки для забезпечення більш ефективного управління та процесу прийняття рішень щодо кіберзахисту. Ноель С., Харлі Е., Там К.Х., Лімієро М. та Шейр М. [189] розглядають систему CyGraph, яка представляє собою уніфіковану графічну модель кібербезпеки, мета якої – забезпечення реакції на потенційні та реальні кібератаки. Чжан Р., Сюе Р. та Лю Л. [268] досліджують можливості блокчейн-технології для забезпечення безпеки та конфіденційності в криптовалютних системах. Деякі дослідники приділяють увагу питанням розробки спеціалізованих інформаційних систем, які передбачають автоматизацію поточних бізнес-процесів, що попереджує зовнішнє втручання в їх здійснення [383].

Що стосується методів багатоатрибутного прийняття рішень (multi-attribute decision-making), то даний інструментарій застосовується для рішення різного роду завдань. Так, Акрам С.М., Аль-Кенані А.Н. та Алкантуд Дж.С.Р. [9] приділили увагу VIKOR-методології щодо її можливостей оцінки для вибору методів поводження з відходами та місць для встановлення ТЕЦ. Галеб А. М., Каїд Х., Альсамхан А., Міан С. Х. та Хідрі Л. [99] провели порівняльний аналіз MCDM підходів для вибору виробничих процесів. Мардані А., Завадскас Е.К., Говіндан К., Амат Сенін А. і Джусох А. [173] дослідили можливості застосування VIKOR-технік у таких галузях, як стійкість та відновлювальна енергія. Суніантара І. К. П. та Путт І. Г. В. Е. [228] провели порівняльну характеристику VIKOR та TOPSIS методів з метою вибору значущих змінних процесу щодо мінливості реакцій яскравості та болючості у процесі виготовлення конвертів. Чатерджея П. та Чакраборті С. [44] провели оцінку ефективності абразивних матеріалів на основі семи критеріїв, в ході чого було застосовано метод VIKOR та його різні модифікації. Тобто методи багатоатрибутного прийняття рішень є широко уживаними не залежно від об’єкту дослідження, тому їх можна використовувати для рейтингування країн щодо рівня їх інформаційної безпеки.

Не зважаючи на значний науковий доробок для вирішення проблематики інформаційної безпеки, є важливе питання, яке досить слабко представлене науковими працями фахівців. Це стосується обґрунтування таргетів інформаційної безпеки для подальшого вироблення напрямків реформування системи її забезпечення. Тому для проведення дослідження було узято 12 показників-таргетів, які характеризують різні аспекти кібербезпеки та використовуються для визначення національного індексу кібербезпеки та відповідного рейтингу країни. Базу емпіричних даних сформували (e-Governance Academy Foundation, 2020):

1) розробка політики кібербезпеки (Cyber Security Policy Development) характеризує загальний рівень політики кібербезпеки у країні, що проявляється у створенні відповідних груп та союзів з цього питання, забезпеченні їх координації, розробці стратегії та плану реалізації кібербезпеки;

2) аналіз та інформація про кіберзагрози (Cyber Threat Analysis and Information) відображає напрямки, пов’язані із формуванням інформаційного забезпечення з питань кібербезпеки, куди входить щорічне звітування про кіберзагрози у світі та розробка спеціальних веб-ресурсів, а також напрямки щодо створення та розвитку спеціалізованих аналітичних груп, які регулярно здійснюють аналіз стану кібербезпеки у світі;

3) освіта та підвищення кваліфікації (Education and Professional Development) характеризує рівень освіти у галузі кібербезпеки, що проявляється у визначенні компетенцій з цього напрямку для різних рівнів освіти: початкової, середньої, бакалаврату, магістра, PhD, а також передбачає створення професійної асоціації кібербезпеки, яка охоплює провідних фахівців з вирішення даної проблеми;

4) внесок у глобальну кібербезпеку (Contribution to global cyber security) відображає напрямки, пов’язані із діяльністю країни на глобальному рівні щодо формування її внеску у розробку Конвенції про кіберзлочинність, міжнародних представництв, організацій з кібербезпеки, а також щодо формування можливостей нарощування потенціалу кібербезпеки для інших країн;

5) захист цифрових послуг (Protection of digital services) передбачає оцінку дій країни щодо забезпечення відповідальності для постачальників цифрових послуг, розробки стандартів кібербезпеки для державного сектору та формування спеціальних компетентних наглядових органів;

6) захист основних послуг (Protection of essential services) характеризує заходи країни щодо визначення операторів основних служб, розробки вимог до них, створення компетентного наглядового органу у цій сфері, здійснення регулярного моніторингу заходів безпеки в процесі здійснення основних послуг;

7) послуги електронної ідентифікації та довіри (E-identification and trust services) відображає дії держави щодо створення унікальних ідентифікаторів, компетентних наглядових органів, розробки вимог до криптосистем, електронної ідентифікації та підпису;

8) захист персональних даних (Protection of personal data) стосується напрямків, пов’язаних із формуванням ефективного законодавства в частині захисту персональних даних та створенням відповідних органів;

9) відповідь на кіберінциденти (Cyber incidents response) передбачає дії країни щодо формування спеціальних підрозділів реагування на кіберінциденти, єдиної контактної точки для міжнародної координації, розробки системи відповідальності за звітування щодо випадків кіберзлочинів;

10) менеджмент кіберкриз (Cyber crisis management) включає питання, пов’язані із формуванням плану управління кіберкризисними ситуаціями на національному рівні; участю у міжнародних навчаннях з кіберкриз; оперативною підтримкою волонтерів під час кіберкризи;

11) боротьба проти кіберзлочинів (Fight against cybercrime) характеризує аспекти діяльності спеціалізованих підрозділів з питань кіберзлочинності, цифрової криміналістики, контактної точки з питань міжнародної кіберзлочинності;

12) військові кібероперації (Military cyber operations) стосується напрямків щодо здійснення спеціалізованих кібероперацій та участі країни у міжнародних кібернетичних навчаннях.

Дані показників-таргетів було узято для 160 країн світу за 2018 рік [86]. Всі значення вимірюються у однакових величинах від 0 до 10 та представляють собою оцінки, які надаються кожній країні на основі наданої нею інформації.

Для проведення дослідження було обрано техніку упорядкування переваги за подібністю до ідеального рішення (Technique for Order of Preference by Similarity to Ideal Solution – TOPSIS), яка відноситься до класу розв’язання багатокритеріальних задач та яку було розроблено Хванг К.Л. та Йун К. у 1981 р. [122]. В подальшому дана методика набула розвитку та удосконалення. Її основна ідея полягає у визначенні двох альтернатив, одна з яких має найменшу геометричну відстань до позитивного ідеального рішення, а інша має найбільшу геометричну відстань до від’ємного ідеального рішення. Як результат, методика дозволяє визначити відносну відстань до ідеального рішення, що сприяє

отриманню загальної оцінки для кожної альтернативи, яка може виступити у якості її рейтингу. TOPSIS передбачає виконання наступних етапів.

На *першому етапі* створюється матриця з m-альтернатив та n-критеріїв. У якості альтернативи обираємо країни, для яких необхідно визначити рейтинг. У якості показників виступатимуть складові національного індексу кібербезпеки.

На *другому етапі* визначаються нормалізовані значення показників-таргетів кібербезпеки. Початкові дані приводяться до безрозмірних величин, тобто нормалізуються, оскільки їх значення можуть бути неспівставними. Для цього кроку використовується формула (4.1):

$$u_{ij} = \frac{a_{ij}}{\sqrt{\sum_{j=1}^{n} a_{ij}^2}}, \tag{4.1}$$

де u_{ij} – нормалізовані значення окремих j-их показників-таргетів кібербезпеки для i-ої країни ($i = 1 \div m;\ j = 1 \div n$);

m – кількість альтернатив, у нашому випадку дорівнює кількості країн ($m = 160$);

n – кількість цільових функцій, які дорівнюють кількості показників-таргетів кібербезпеки ($n = 12$);

a_{ij} – фактичне значення окремого j-ого показника-таргету кібербезпеки для i-ої країни.

На *третьому етапі* визначається зважена нормалізована матриця рішень, в якій враховується вага окремого показника для прийняття рішення щодо рейтингу країни, за формулою (4.2):

$$x_{ij} = w_j \cdot u_{ij}, \tag{4.2}$$

де x_{ij} – зважені нормалізовані значення окремих j-их показників-таргетів кібербезпеки для i-ої країни ($i = 1 \div m;\ j = 1 \div n$);

w_j – вага кожної j-ої цільової функції, яка відображає значимість показника-таргету кібербезпеки для загального рейтингу країни, при чому $\sum_{j=1}^{n} w_j = 1$. У нашому випадку вагу було визначено як долю нормативного значення j-го показника у їх сумарній оцінці за формулою (4.3):

$$w_j = \frac{w_j^*}{\sum_{j=1}^{n} w_j^*}, \tag{4.3}$$

де w_j^* – нормативна оцінка j-го показника-таргету кібербезпеки.

На *четвертому етапі* визначається позитивне та від'ємне ідеальне рішення, тобто визначається за формулами (4.4) та (4.5) країна, яка має найвищий рівень кібербезпеки, та країна з найгіршими показниками-таргетами:

$$A^+ = \{x_1^+, \dots, x_n^+\},$$
$$x_j^+ = \left\{\max_i x_{ij} | j \in C_j(max); \min_i x_{ij} | j \in C_j(min)\right\}, \tag{4.4}$$

$$A^- = \{x_1^-, \dots, x_n^-\},$$
$$x_j^- = \left\{\min_i x_{ij} | j \in C_j(min); \max_i x_{ij} | j \in C_j(max)\right\}, \tag{4.5}$$

де A^+ та A^- – відповідно найкраща та найгірша альтернативи або позитивне та від'ємне ідеальне рішення, які представлені набором показників кібербезпеки;

x_j^+ – розраховані максимальні значення для тих критеріїв, які позитивно впливають на формування найкращої альтернативи, або мінімальні значення, які також здійснюють позитивний вплив;

x_j^- – розраховані мінімальні значення для тих критеріїв, які негативно впливають на формування найгіршої альтернативи, або максимальні значення, які також здійснюють негативний вплив;

C_j – сукупність значень для j-ого показника-таргету кібербезпеки.

На *п'ятому етапі* проводиться оцінка відстаней для кожної країни до ідеальної альтернативи. Відстань до найкращої (позитивної) альтернативи розраховується за формулою (4.6) та її значення для конкретної *i*-ої країни показує, що чим воно менше, тим ближче дана країна до ідеальних значень показників-таргетів безпеки, а її рейтинг буде вищим. Відстань до найгіршої (від'ємної) альтернативи визначається за формулою (4.7) та її значення свідчить, що чим воно менше, тим ближче країна знаходиться до найгіршого варіанту, тобто вона матиме низький рейтинг за рівнем кібербезпеки:

$$S_i^+ = \sqrt{\sum_{j=1}^{n} \left(x_{ij} - x_j^+\right)^2}, \tag{4.6}$$

$$S_i^- = \sqrt{\sum_{j=1}^{n} \left(x_{ij} - x_j^-\right)^2}, \tag{4.7}$$

де S_i^+ – відстань показників країни до найкращої (позитивної) альтернативи;

S_i^- – відстань показників країни до найгіршої (від'ємної) альтернативи.

На *шостому етапі* здійснюється розрахунок за формулою (4.8) відносної відстані до ідеальної альтернативи, що передбачає визначення подібності значень критеріїв для кожної *i*-ої країни із найгіршим станом:

$$Q_i = \frac{S_i^-}{S_i^+ + S_i^-} \tag{4.8}$$

Якщо отримане значення Q_i наближається до 1, то це говорить про те, що *i*-та країна має найкращу комбінацію показників-таргетів кібербезпеки, яка є близькою до ідеальної комбінації. Якщо значення Q_i наближається до 0, то це свідчить про найгіршу комбінацію показників-таргетів кібербезпеки та дана країна буде мати досить низький рейтинг.

На *сьомому етапі* проводиться оцінка рейтингу шляхом визначення рангу для розрахованих значень. З цією метою проводиться ранжування країн за отриманим показником-таргетом Q_i у порядку його убування. Далі їм надається порядковий номер у ряді. Якщо значення Q_i однакові, то розраховується стандартизований ранг як середньоарифметичне значення порядкових номерів для однакових Q_i. Для перевірки правильності отриманих рангів необхідно знайти їх суму для всього ряду та дане значення порівняти із $N \cdot (N + 1)/2$, де N – це кількість країн у ряді, тобто 160.

Наступний метод, який було обрано для проведення розрахунків, це original VIKOR (Vlse Kriterijumska Optimizacija Kompromisno Resenje, in Serbian), який означає багатокритеріальну оптимізацію та компромісне рішення. Він був запропонований у 1979 році сербським вченим Оприцович С., але міжнародного визнання його класичний варіант набув у публікації [192]. Суть методу полягає у знаходженні багатокритеріальної оцінки, яка знаходиться як міра відносної близькості до ідеального компромісного рішення. VIKOR має декілька модифікацій, а саме comprehensive VIKOR, fuzzy VIKOR, regret theory-based VIKOR, modified VIKOR та interval VIKOR, але для типових задач найкращим є оригінальний VIKOR, що доведено Чатерією П. та Чакраборті С. [44]. Реалізація даного методу передбачає виконання наступних етапів.

На *першому етапі* створюється матриця альтернатив та критеріїв, яка є аналогічною матриці, створеною за методом TOPSIS.

На *другому етапі* проводиться нормалізація початкових показників-таргетів кібербезпеки, представлених у вигляді матриці. Але при цьому враховується факт впливу показника. Якщо його значення здійснює позитивний вплив, тобто є стимулятором, то нормалізація проводиться за формулою (4.9), якщо показник впливає негативно (є дестимулятором), то нормалізація відбувається за формулою (4.10):

$$x_{ij} = w_j \cdot \frac{a_j^{max} - a_{ij}}{a_j^{max} - a_j^{min}}, \tag{4.9}$$

$$x_{ij} = w_j \cdot \frac{a_{ij} - a_j^{min}}{a_j^{max} - a_j^{min}}, \quad (4.10)$$

де x_{ij} – нормалізоване значення j-ого показника-таргету кібербезпеки для i-ої країни ($i = 1 \div m$; $j = 1 \div n$);

w_j – вага кожного j-ого показника-таргету кібербезпеки, яка відображає його значимість для загального рейтингу країни, при чому $\sum_{j=1}^{n} w_j = 1$;

a_{ij} – фактичне значення j-ого показника-таргету кібербезпеки для i-ої країни;

a_j^{max} – максимальне значення j-ого показника-таргету кібербезпеки;

a_j^{min} – мінімальне значення j-ого показника-таргету кібербезпеки.

Оскільки всі показники кібербезпеки є стимуляторами, то для їх нормалізації використовуємо формулу 4.9. Підхід до визначення вагів використовуємо аналогічно до того, який застосовувався у методі TOPSIS.

На *третьому етапі* розраховуємо зважену та нормовану відстань Манхеттена (S_i) за формулою (4.11), а також зважену та нормовану відстань Чебишева (R_i) за формулою (4.12):

$$S_i = \sum_{j=1}^{n} x_{ij}, \quad (4.11)$$

$$R_i = \max_i x_{ij}. \quad (4.12)$$

На *четвертому кроці* обчислюється за формулою (4.13) оцінка відстані для i-ої країни до ідеального рішення, тобто оптимальної комбінації показників-таргетів кібербезпеки:

$$Q_i = v \cdot \frac{S_i - S^-}{S^+ - S^-} + (1 - v) \cdot \frac{R_i - R^-}{R^+ - R^-}, \quad (4.13)$$

де Q_i – оцінка відстані для i-ої країни до ідеального рішення, значення якої знаходиться в межах від 0 до 1. Чим ближче вона до 0, тим ближче відстань для i-ої країни до ідеального рішення. Якщо оцінка наближається до 1, то параметри країни значно віддаляються від ідеального рішення;

S^-, S^+ – розраховуються за формулою (4.14):

$$S^- = \min_i S_i, S^+ = \max_i S_i ; \tag{4.14}$$

R^-, R^+ – розраховуються за формулою (4.15):

$$R^- = \min_i R_i, R^+ = \max_i R_i; \tag{4.15}$$

v – це вага стратегії більшості атрибутів або групової корисності, значення якої знаходиться в межах від 0 до 1. Найбільша перевага надається значенню 0,5, яке показує збалансованість при прийнятті рішення. Якщо воно дорівнює 1, то мова йде про стратегію максимізації групової корисності, якщо 0, то про стратегію мінімізації індивідуального співчуття, тобто знаходиться мінімальне значення критерію для кожної альтернативи серед максимальних індивідуальних відхилень від ідеального значення.

На *п'ятому етапі* здійснюється ранжування для отриманих оцінок з метою визначення рейтингу країни аналогічно до процесу ранжування, описаному в методі TOPSIS.

Третій метод, який використовується у дослідженні, це багатоатрибутна модель ставлення (Multi-attribute Attitude Model – MAAM), яка базується на моделі Фішбейна та запропонована Міллером К. у 1963 році [176]. Її суть полягає у визначенні відношень споживачів до конкретного продукту в залежності від оцінок його атрибутів. Відповідно до умов даного дослідження відбуватиметься оцінка показників кібербезпеки для кожної країни з метою виділення найслабших та найсильніших країн щодо створених ними умов забезпечення

відповідного рівня безпеки. Метод є дуже простим у реалізації й передбачає здійснення наступних кроків.

Перший етап здійснюється аналогічно, як й за методами TOPSIS та VIKOR.

На *другому етапі* визначається оцінка загального рівня кібербезпеки за допомогою формули (4.16):

$$Q_i = \sum_{j=1}^{n} w_j \cdot a_{ij}, \tag{4.16}$$

де Q_i – оцінка загального рівня кібербезпеки для i-ої країни;

w_j – вага кожного j-ого показника-таргету кібербезпеки, яка відображає його значимість ($\sum_{j=1}^{n} w_j = 1$);

a_{ij} – фактичне значення j-ого таргету кібербезпеки для i-ої країни.

Третій етап присвячується розрахунку рейтингу для i-ої країни, який здійснюється аналогічно до методів TOPSIS та VIKOR.

Розрахунки здійснювалися за допомогою програми «MS Excel». Результати представлено в таблиці Ж.1 додатку Ж. Розрахунок за методом VIKOR відбувався з урахуванням ваги групової корисності 1 та 0,5. При v=0 результати рейтингів виявилися неадекватними.

Для отримання адекватної оцінки було проведено порівняння отриманих рейтингів із фактичним значенням, сформованого за існуючим результатом національного індексу кібербезпеки, результати розрахунків яких наводяться у таблиці Ж.1 додатку Ж. Для проведення аналізу було знайдено різницю між фактичним значенням рейтингу та розрахованим. На рисунку 4.1 представлено візуалізацію різниці, отриманої в результаті порівняння рейтингу за методом TOPSIS та фактичним.

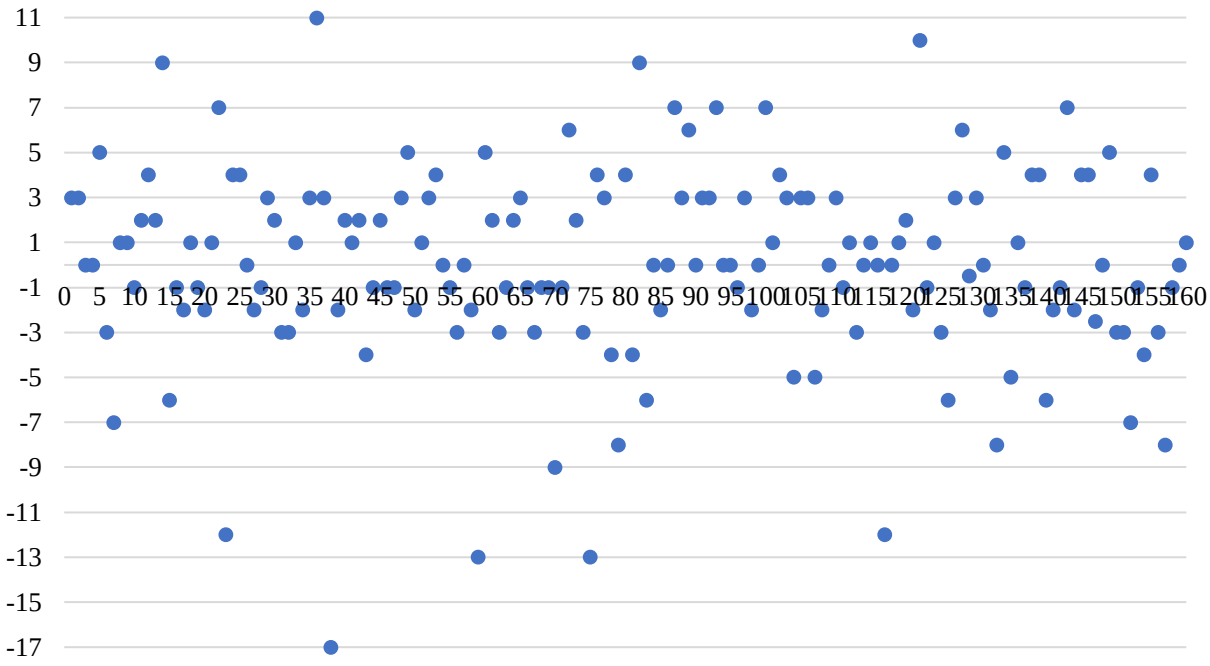


Рисунок 4.1 – Різниця, отримана в результаті порівняння рейтингу за методом TOPSIS та його фактичного значення (складено авторкою)

На рисунку 4.1 можна побачити, що відхилення між фактичним значенням та розрахованим за методом TOPSIS знаходиться від -17 до 11 позицій, що свідчить про значний розкид у значеннях. Тільки для 18 країн рейтинги співпали, що складає тільки 11,25% від загального обсягу країн. Оскільки існуючий підхід до визначення фактичного рейтингу не враховує таких аспектів, як важливість показників кібербезпеки, оцінка відхилення значень для країни по різних показниках, визначення кращої або гіршої альтернативи, то можна сказати, що отримані результати рейтингу за методом TOPSIS доцільно використовувати з позиції розробки стратегії знаходження сильних та слабких місць в кібербезпеці країни, що дозволить визначити напрямки реформування системи інформаційної безпеки країни. З цією метою побудуємо пелюсткову діаграму, яка дозволить провести такий аналіз (рисунок 4.2).

На рисунку 4.2 представлена найкраща альтернатива, яка відповідає еталонній моделі (максимальні значення таргетів), альтернативне рішення для Естонії (зайняла 1-е місце в отриманому рейтингу), альтернатива для України – країни із середнім рейтингом. Для наочності можна було б ще винести значення

найгіршої альтернативи, тобто рішення для Південного Судану – країни, що займає останнє місце в рейтингу. Але оскільки усі її значення наближаються до 0, то візуально на графіку вона відображатиметься у вигляді крапки.

Рисунок 4.2 – Результати аналізу напрямків реформування національної системи інформаційної безпеки (за таргетами методу TOPSIS) (складено авторкою)

Аналізуючи таргети для Естонії, можна побачити, що даній країні слід приділити більшу увагу розробці політики кібербезпеки, питанням розвитку освіти та підвищення кваліфікації, електронної ідентифікації та трастовим послугам, а також боротьбі із кіберзлочинністю, оскільки їх значення відхиляються від найкращої (позитивної) альтернативи. Це говорить про існування певних проблем, які потребують удосконалення законодавчої бази, впровадження нових спеціальностей, пов’язаних із захистом інформації та кіберзахистом, модернізації технологій в галузі електронної ідентифікації, створення більш дієвих організацій, направлених на боротьбу з кіберзлочинами.

Результати для України представляють значний контраст (рисунок 4.2), оскільки частина таргетів відповідають найкращій альтернативі або наближаються до неї, а частина інших прямують до значень найгіршої. Тобто спостерігаються дисбаланс у забезпеченні системи інформаційної безпеки

держави, викликаний існуванням ряду проблем, пов’язаних із аналізом та інформацією про кіберзагрози, внеском у глобальну кібербезпеку, захистом цифрових послуг, захистом основних послуг, електронною ідентифікацією та трастовими послугами, реакцією на кіберінциденти, менеджментом кіберкриз, кібервійськовими операціями. При чому показник-таргет менеджменту кіберкриз взагалі дорівнює 0, що свідчить про відсутність відповідних планів управління кібербезпекою, кіберкризами на національному рівні, оперативної підтримки волонтерів під час кіберкризи, участі у міжнародних навчаннях з питань кібербезпеки.

За методом TOPSIS найнижчим в рейтингу виявився Південний Судан, тобто фактично дана країна не забезпечує кібербезпеку для своїх громадян, підприємств та держави в цілому. Це пов’язано із історією становлення даної держави та постійними військовими конфліктами в її середині. Відповідно, сьогодні проблема кібербезпеки не є пріоритетною для неї.

Візуалізуємо результати, отримані за іншими методами. Представимо різницю, отриману в результаті порівняння фактичного рейтингу країни та рейтингу за методом VIKOR, на рисунках 4.3 та 4.4.

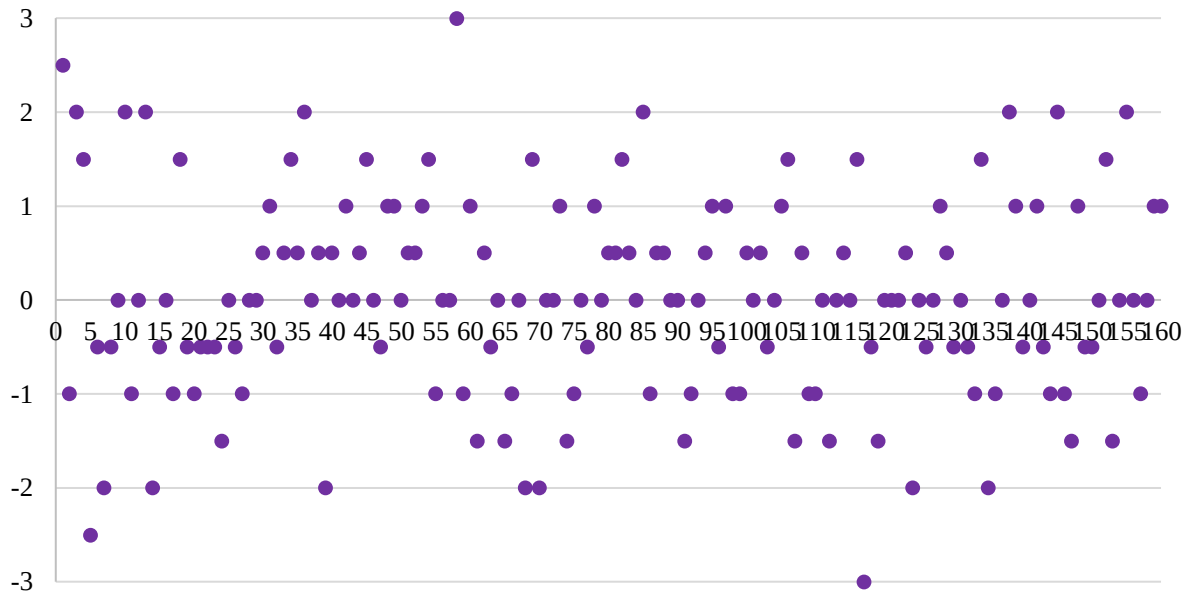


Рисунок 4.3 – Різниця, отримана в результаті порівняння рейтингу за методом VIKOR та його фактичним значенням (v=1,0) (складено авторкою)

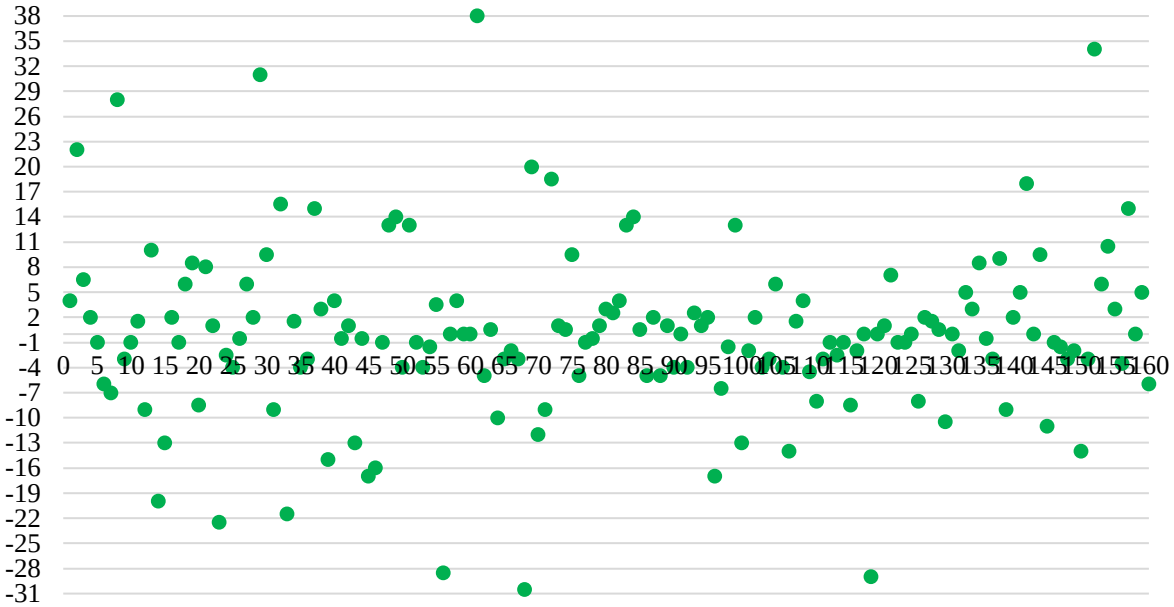


Рисунок 4.4 – Різниця, отримана в результаті порівняння рейтингу за методом VIKOR та його фактичним значенням (v=0,5) (складено авторкою)

Так, на рисунку 4.3 можна побачити розкид значень у межах від -3 до 3, що говорить про подібність результатів розрахункової оцінки рейтингів до фактичної. 40 країн мають оцінки, аналогічні до оцінок фактичного рейтингу, що складає 25% від загальної кількості. Оскільки для розрахунків використовувалося значення ваги групової корисності v = 1,0, коли відбувається його максимізація, то дані результати свідчать про позитивний погляд до сумарних оцінок рейтингу для країни. Результати розрахунків за збалансованим підходом, коли v = 0,5, представлені на рисунку 4.4, який показує різницю між оцінками з розкидом від -30,5 до +38. Кількість країн, які мають схожі оцінки, дорівнює 10, що складає 6,25%.

Рейтингування за методом VIKOR за умови, коли *v = 0,5*, доцільно у випадку знаходження компромісу за умовою використання суперечливих критеріїв. У випадку проведеного дослідження даний метод доцільно було б використати, якщо показники кібербезпеки мали б протилежні значення або здійснювали протилежний вплив на формування загальної оцінки.

Що стосується порівняння рейтингу, розрахованого за методом MAAM, із фактичним рейтингом, то отримані різниці представлені на рисунку 4.5.

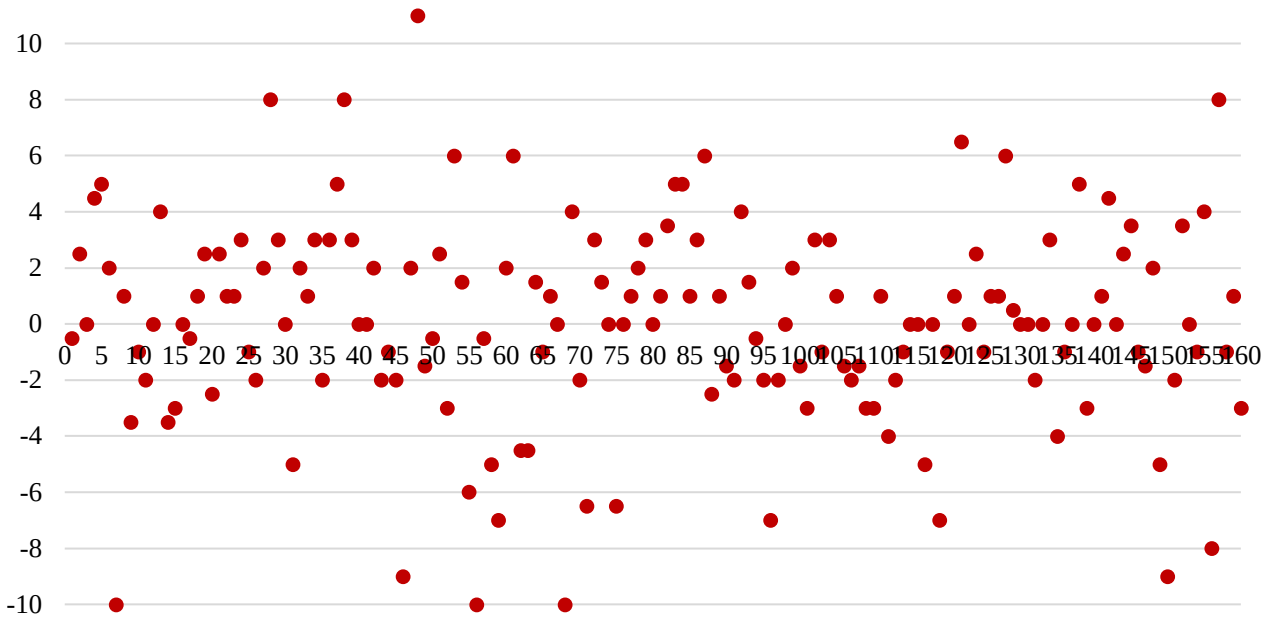


Рисунок 4.5 – Різниця, отримана в результаті порівняння рейтингу за методом MAAM та його фактичним значенням (складено авторкою)

Результати порівняння, відображені на рисунку 4.5, показують, що різниця між оцінками коливається від -10 до +11, тобто результати є однаковими для 22 країн, що складає приблизно 13,75%. Також дані розбіжності близькі до тих, які були отримані при порівнянні фактичного рейтингу та оцінки за методом TOPSIS. Але даний метод не передбачає застосування нормалізації даних, що робить його не придатним для застосування у випадках, коли критерії мають різну розмірність.

На рисунку 4.6 представлені порівняння отриманих рейтингів для країн, які мають найнижчий рівень за 3-ма методами (Південний Судан), найвищий (Чеська республіка та Естонія) та помірний (Україна).

У випадку із Південним Суданом за всіма методами було отримано однакову рейтингову оцінку, яка також співпадає із фактичним рейтингом. Для України результати значно відрізняються, при чому за методом TOPSIS країну було оцінено більш критично, а за іншими методами вона отримала оцінки вищі, ніж реальний рейтинг.

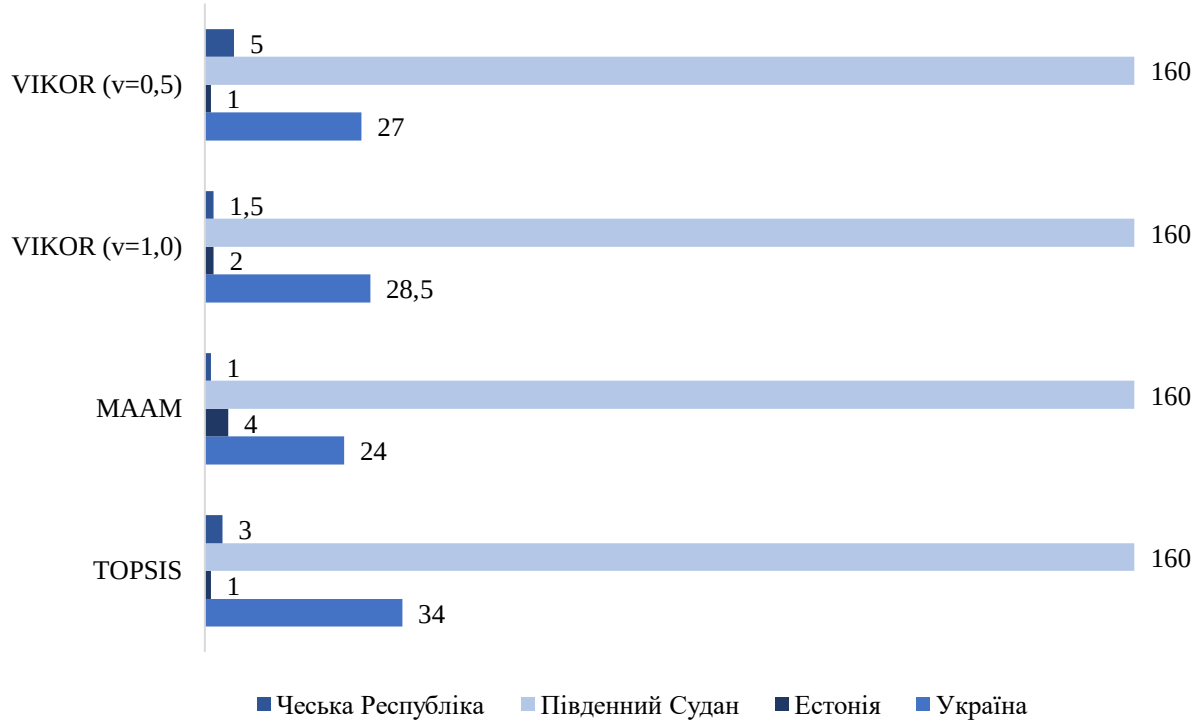


Рисунок 4.6 – Порівняння результатів рейтингових оцінок (складено авторкою)

Що стосується Естонії та Чеської Республіки, то вони є лідерами за різними методами, при чому їх оцінки коливаються в межах від 1 до 5 для Чеської республіки, та від 1 до 4 для Естонії. Можна прийти до висновку, що в залежності від стратегії рейтингування, можна обирати будь-який із приведених методів, але у випадку нерівномірного коливання значень критеріїв їх результати будуть кардинально відрізнятися.

Проведемо перевірку ефективності застосовуваних методів шляхом розрахунку коефіцієнту рангової кореляції Спірмена за формулою (4.17), результати якого наведені у таблиці 4.1:

$$r = 1 - 6 \cdot \frac{\sum (d_x - d_y)^2}{n^3 - n}, \tag{4.17}$$

де r – коефіцієнт рангової кореляції Спірмена;

n – кількість спостережень;

d_x та d_y – пари співставних значень рангів.

Таблиця 4.1 – Розраховані значення коефіцієнта рангової кореляції Спірмена

Назва методу	Фактичний рейтинг	TOPSIS	MAAM	VIKOR (v=1,0)	VIKOR (v=0,5)
Фактичний рейтинг	1	0,9956	0,9969	0,9997	0,9759
TOPSIS	–	1	0,9940	0,9958	0,9723
MAAM	–	–	1	0,9971	0,9817
VIKOR (v=1,0)	–	–	–	1	0,9764
VIKOR(v=0,5)	–	–	–	–	1

Отримані значення коефіцієнта кореляції наближаються до 1, що свідчить про високу ефективність отриманих результатів ранжування. Але метод VIKOR (v=0,5) надає нижчі результати ефективності у порівнянні із іншими методами. Інші методи мають досить рівнозначні оцінки, що говорить про високий рівень довіри до отриманих даних.

Таким чином, реалізовані методи TOPSIS, VIKOR та MAAM було застосовано для визначення ефективного рейтингу країн на основі оцінок показників-таргетів кібербезпеки. Отримано, що результати за методом VIKOR (v=1,0) мають близько 25% подібності із оцінками реального рейтингу країн, що свідчить про низькі його можливості, пов’язані із існуванням недоліків, відповідних оцінці реального рейтингу. Вибір такого значення ваги є доцільним у випадку вибору альтернатив, але у випадку тільки оцінки рейтингу цей фактор може значно впливати на результати, що є неприпустимим для здійснення оцінок окремої країни. Метод VIKOR (v=0,5) виявив нижчу ефективність у порівнянні з іншими методами, про що свідчать отримані результати коефіцієнта рангової кореляції Спірмена.

Найкращі результати продемонстрували методи TOPSIS та MAAM. Отримані оцінки є збалансованими, що говорить про їх гарні можливості для застосування в процесі визначення ефективного рейтингу країн щодо рівня їх кібербезпеки. Але метод TOPSIS є найбільш прийнятним для проведення рейтингування країн за рівнем кібербезпеки, оскільки він має високі показники ефективності, нівелює перелічені недоліки методів реальної оцінки, а також, що

саме головне, дозволяє визначати альтернативні стратегії для показників-таргетів на відміну від інших методів, що було зроблено для України та країн з найкращими та найгіршими альтернативами. Тому вважаємо, що в умовах вирішення проблематики дослідження, даний метод дозволить не тільки отримати ефективні оцінки рейтингу, але допоможе визначити критичні значення таргетів для окремої країни, виявити держави з ідеальними альтернативами, що сприятиме вивченню їх досвіду щодо розробки стратегії кібербезпеки.

В процесі порівняння оцінок, розрахованих за різними методами, було виявлено, що країни Естонія та Чеська Республіка мають найвищі рейтинги та значення їх показників найбільше наближається до ідеальних. Тобто, доцільно звернути увагу на їх практику щодо формування стратегії кібербезпеки в Україні, особливо в частині тих показників, які значно відхиляються від ідеальних та мають критичні значення. Країною із самим низьким рейтингом, що було підтверджено розрахунками за всіма методами, є Південний Судан. Оскільки вона має проблеми політичного, військового, соціально-економічного характеру, то це підтверджує відсутність пріоритету забезпечення її кіберзахисту.

Що стосується напрямів реформування національної системи інформаційної безпеки для України, то пропонуємо в рамках визначених таргетів наступні заходи для підвищення її рівня:

1) розробити та впровадити на загальнодержавному рівні статистичну систему збору та аналізу інформації щодо випадків кіберінцидентів для різних суб’єктів інформаційної безпеки, що дозволить мати деталізовану інформацію та розробляти рекомендації щодо попередження різного роду інформаційних інцидентів, які базуються на досвіді та практиці тих суб’єктів економіки, які у своїй діяльності зіткнулися з подібними викликами;

2) реформувати національну систему стандартів інформаційного захисту шляхом впровадження міжнародної практики та міжнародних стандартів захисту цифрових послуг, а також забезпечити контроль за обов’язковістю їх дотримання особливо тими компаніями, які здійснюють сервісні та онлайн-послуги;

3) сформувати спеціальну державну комісію по роботі із міжнародними організаціями, які займаються питаннями глобальної кібербезпеки, а також надати пропозиції щодо включення України у різного роду опитування з питань формування та забезпечення інформаційної безпеки на різних рівнях національної економіки держави, які проводять міжнародні консалтингові та ІТ-компанії (наприклад, IBM та Deloitte);

4) посилити діяльність урядових організацій у напрямку формування та реформування спеціальних груп реагування на здійснення масштабних кібератак, а також спеціальних груп контролю за проведенням кібервійськових операцій, що є актуальним в умовах ведення бойових дій на Сході України. В цьому напрямку доцільно сформувати групи, які б також відслідковували загрози, пов'язані із здійсненням хактивізму та недоброчинної поведінки у соціальних мережах, засобах масової інформації;

5) провести консультативну роботу на рівні державних органів та економічних агентів щодо формування та впровадження у їх діяльність менеджменту кіберкриз, що є досить актуальним для попередження інформаційного кібершпигунства та кібератак. Паралельно для вирішення даної проблеми рекомендується впровадити в освітній процес спеціальність, яка б дозволила готувати висококваліфікованих фахівців з кіберменеджменту, а також запровадити курси підвищення кваліфікації з даного напрямку для представників бізнесу та державного управління;

6) сприяти розробці систем попередження кіберінцидентів, які дозволять не тільки виявляти факти їх здійснення, але й забезпечувати на ранніх етапах діагностику процесів захисту, виявляти слабкі місця та визначати напрями потенційних кіберзлочинів;

7) сприяти розвитку трастових компаній, які дозволять суб'єктам інформаційної безпеки прийняти на себе частину ризиків, пов'язаних саме із перевіркою та контролем ідентифікації користувачів різних онлайн-систем: банківських, платіжних, електронної комерції, електронного уряду, електронних послуг, тощо.

4.2 Поглиблення методології обґрунтування пріоритетів формування державних секторальних та галузевих програм у напрямку забезпечення інформаційної безпеки національної економіки

Сьогодні тренди господарської діяльності вимагають від підприємств застосування автоматизованих інформаційних систем (далі АІС) будь-якого класу, які охопили практично усі сфери економічної діяльності. Це дозволяє підвищувати ефективність управління бізнес-процесами та сприяє прийняттю більш гнучких та зважених рішень. Також наявність АІС управління є гарантією того, що дана компанія забезпечує високу якість своєї продукції чи послуг у відповідності із міжнародними стандартами. Цей пункт є одним із важливих та прописаний у стандартах забезпечення якості продукції ISO 9000. Саме тому інформаційні системи стали невід'ємною частиною діяльності економічних агентів.

Із зростанням інцидентів та загроз, націлених на викрадення, знищення, порушення цілісності інформації, зросла необхідність у забезпеченні її захисту, для чого є потреба у організації системи інформаційної безпеки, яка повинна виконувати ці функції. У цьому напрямку активно розробляються стандарти із захисту інформації та інформаційної безпеки, створюються програмні та технічні інструменти для їх забезпечення, формуються цілі підрозділи на підприємствах, тощо.

З одного боку, є нагальна потреба у формуванні інформаційної безпеки на підприємствах, з іншого боку, це потребує значних фінансових вкладень. Саме тому необхідно оцінити потенційні можливості суб'єкта господарювання щодо здійснення обґрунтованого розміру витрат на систему інформаційного захисту, яка б дозволила ефективно протистояти загрозам та не призводити до невиправдано високих збитків. З цією метою доцільно провести оцінку ефективності системи інформаційної безпеки, але оскільки вона не може існувати окремо від автоматизованої інформаційної системи підприємства, то її

необхідно здійснювати у комплексі.

Перш за все, для оцінки ефективності системи захисту необхідно розглянути ті її функції, які стосуються безпосередньо самого захисту та АІС, яка буде підлягати захисту. Так, якщо реалізується функція захисту від проникнення вірусів, то у відповідності із нею необхідно впровадження антивірусної програми, з якою окрім витрат на придбання, будуть пов'язані витрати щодо щомісячної оплати за її функціонування та оновлення. Якщо існує потреба у попередженні дій інсайдерів, направлених на викрадення секретної інформації або порушення її цілісності, то для цього необхідно реалізувати систему аудиту дій персоналу, забезпечення функціонування якої потребує також відповідних витрат.

Витрати на заходи захисту значні і постійно збільшуються не залежно від галузі діяльності або розміру компанії. Але їх розмір не може бути необґрунтованим, оскільки в цьому випадку переваги від впровадження цих заходів не будуть перевищувати обсяги витрат, що може призвести до зниження прибутку компанії. Саме тому ефективність від систем захисту повинна досягатися тільки за рахунок мобілізації використання резервів підприємства, отриманих в наслідок прийняття обґрунтованих рішень в АІС управління.

Для визначення витратної складової будь-якої інформаційної системи, в тому числі й системи інформаційної безпеки, використовується ряд методик, серед яких є найбільш популярною та ефективною методика оцінки сукупної вартості володіння (далі СВВ), розроблена у 1987 р. компанією «Gartner Group». Сукупна вартість володіння визначається на 1 рік і може бути використана, як при вибору складових системи, так і для розрахунків між підрозділами підприємства, якщо їх взаєморозрахунки здійснюються за методом «держава в державі». Її суть полягає у тому, що окрім капітальних витрат на придбання технічних та програмних засобів АІС підприємства відбувається розрахунок всіх витрат, пов'язаних із експлуатацією даної системи. Їх перелік є стандартним та включає оцінку витрат на програмно-апаратне забезпечення, адміністрування, підтримку, розробку, комунікації, людський фактор та простої. Розрахунок СВВ

дозволяє оцінити, які з її компонентів є найбільш витратними та як їх можна оптимізувати, щоб знизити вартість.

СВВ АІС надає інформацію про рівень витрат на її придбання. Вона використовується для вибору оптимальної архітектури у відповідності із потребами підприємства шляхом порівняння СВВ декількох варіантів технічного та програмного забезпечення з урахуванням їх вартісних та функціональних характеристик. Також розрахунок СВВ окремих видів технічних засобів, програмних комплексів, технологічних операцій вводу даних постійної та змінної інформації, обробки даних дає змогу визначити вартість 1 години роботи системи у процесі її експлуатації.

Для організації інформаційного захисту аналогічним шляхом визначається СВВ підсистеми інформаційного захисту. Оскільки однією із основних її функцій є захист прикладної системи, то він також включатиме й захист від внутрішніх та зовнішніх загроз, які приводять до зниження ефективності самої АІС. Це потрібно враховувати в процесі оцінки економічної ефективності (доцільності) системи інформаційного захисту.

Окрім витратної частини, необхідно оцінити дохідну, що дозволить в подальшому визначити ефект від функціонування системи. В умовах, коли в компанії взаємовідносини між підрозділами будуються на основі підходу «держава в державі», то в цьому випадку дохід від АІС буде формуватися як грошові надходження за надані відділом ІТ послуги іншим підрозділам. З цією метою необхідно визначати вартість машино-години за формулою (4.18):

$$V_{AIS}^{h} = \frac{TVO}{H}, \tag{4.18}$$

де V_{AIS}^{h} – вартість машино-години, яка вимірюється у грошових одиницях за 1 годину роботи АІС;

TVO – сукупна вартість володіння АІС, розрахована на рік, як сума усіх витрат на систему у грошових одиницях;

H – річна сума годин роботи АІС.

Відповідно дохід, який генерує АІС компанії, буде визначатися за формулою (4.19):

$$R_{AIS} = \sum_{i=1}^{n} V_{ITS_i}, \tag{4.19}$$

де R_{AIS} – дохід від надання ІТ-підрозділом компанії ІТ-послуг іншим підрозділам, який визначається за місяць, квартал, рік та вимірюється у грошових одиницях;

V_{ITS_i} – вартість надання і-го виду ІТ-послуги, розрахована у грошових одиницях ($i = \overline{1,n}$, n – кількість ІТ-послуг), яка розраховується за формулою (4.20):

$$V_{ITS_i} = V_{AIS}^{h} \times h_i, \tag{4.20}$$

де h_i – загальний час на виконання i-ої ІТ-послуги.

Для інших компаній, які не практикують подібну систему взаєморозрахунків між підрозділами, в якості доходу, який генерує АІС, виступає результат, отриманий від змін, які відбуваються внаслідок функціонування інформаційної системи. Таким результатом, як правило, виступає річна економія, що представляє собою відносне або абсолютне зменшення витрат на виробництво в цілому, або за окремими елементами витрат (сировини, матеріалів, оплати праці, витрат на управління і обслуговування виробництва), а також відносне або абсолютне збільшення доходів. Тобто вона може включати в себе:

– річний приріст прибутку, отриманий в результаті збільшення обсягу господарської діяльності (виробництва, послуг або робіт) як наслідок впровадження АІС;

– річний приріст прибутку, отриманий за рахунок прискорення

освоєння нової продукції (послуг) в результаті розробки і впровадження АІС;

– додатковий прибуток, отриманий за рахунок скорочення невиробничих втрат (штрафів, пені, неустойок) в результаті впровадження АІС;

– річний приріст доходу від реалізації продукції за рахунок збільшення кількості клієнтів, залучених за допомогою АІС;

– додатковий прибуток за рахунок підвищення продуктивності праці;

– економію поточних витрат на виробництво продукції, послуг або робіт в умовах функціонування АІС;

– економію заробітної плати за рахунок збільшення кількості вивільнених працівників в результаті впровадження АІС;

– економію втрат від браку за рахунок підвищення якості продукції, що випускається;

– економію інших витрат, що не входять в собівартість виробництва чи робіт, що забезпечується функціонуванням АІС як безпосередньо на об'єкті впровадження, так і в пов’язаних сферах і галузях, тощо.

Літературні джерела однозначно не дають відповідей на те, яким чином потрібно визначати доходи, які генерує АІС підприємства. Увага акцентується тільки на витратну складову. Дослідження даної проблеми дозволило прийти до такого висновку, що дохід від АІС, або правильніше казати, річна економія, формується за рахунок різних напрямів економії грошових коштів компанії, які виникають від дій АІС, тобто джерел ефективності. Стандартна методологія їх визначення відсутня. Єдиним підходом є порівняння стану системи до впровадження АІС та після, або стан системи за попередній рік та стан системи за поточний. Але в цьому випадку треба враховувати, який стан система управління підприємства мала до і після, та на які аспекти діяльності компанії впливає саме інформаційна система.

Так, джерела ефективності в першу чергу залежатимуть від функціональних підсистем АІС. Тому спочатку треба визначити та виявити ті функції і задачі, які система автоматизує. Далі необхідно виділити ті джерела ефективності, завдяки яким підприємство отримує ефект. Для компаній, які

займаються схожими видами діяльності, функціонують в одній галузі, джерела ефективності є однаковими, але їх розмір буде різним. Тому це буде набір загальних джерел, завдяки яким підприємство або отримає, або не отримає ефект. Потім необхідно встановити зв'язок між джерелами ефективності та даними бухгалтерського обліку, оскільки тільки в обліку можна реально виділити ті зміни, які відбуваються на підприємстві з фінансовими, матеріальними та трудовими потоками. Тобто, за мобілізацію джерел ефективності відповідає облікова підсистема у поєднанні з проблемами підприємства та даними бухгалтерського обліку. В цьому випадку дохід від АІС або розмір річної економії буде розраховуватися наступним чином:

$$R_{AIS} = EC_{AIS} = \sum_{i=1}^{n} (k_i \times VSE_i), \quad (4.21)$$

де EC_{AIS} – річна економія, яку генерує АІС та яка формується як наслідок зменшення витрат або збільшення доходів;

VSE_i – вартість i-го джерела ефективності, визначеного за даними бухгалтерського обліку та визначеного у грошовому вимірі ($i = \overline{1,n}$, n – кількість джерел ефективності);

k_i – коефіцієнт зміни джерела ефективності, який визначається шляхом порівняння стану об’єкту за попередній рік із станом об’єкту за поточний та коректується на стан об’єкту за попередній рік та розраховується у відсотках. На практиці його значення може варіюватися в залежності від природи джерела ефективності. Наприклад [279]:

– збільшення обсягу виручки від реалізації продукції, товарів, робіт, послуг – 5-25%;

– підвищення ефективності використання ресурсів – 15-40%;

– підвищення рівня обслуговування клієнтів компанії – 25-60%;

– підвищення оборотності грошових коштів – 25-55%;

– прискорення виведення нового товару на ринку – 25-75%;
– скорочення виробничого циклу – 35-65%;
– зменшення оборотності запасів – 25-55%;
– зниження витрат – 5-25%;
– зниження виробничого браку 35-65%;
– зниження виробничого циклу – 5-25%.

Таким чином, для визначення ефекту від функціонування АІС необхідно мати дві складові, а саме – значення сукупної вартості володіння АІС (витратна складова), та значення доходу або економії, які генеруються в результаті використання АІС підприємства (дохідна складова):

$$E_{AIS} = R_{AIS} - TVO_{AIS}, \quad (4.22)$$

де E_{AIS} – ефект від функціонування АІС компанії.

Що стосується системи інформаційної безпеки підприємства, то в організаційному плані вона є складовою АІС, її підсистемою. Впливу на збільшення доходу, який отримує компанія внаслідок функціонування АІС, вона немає, тому що система інформаційної безпеки не впливає на господарську діяльність, організацію бізнес-процесів, не сприяє скороченню операційних витрат, не забезпечує зростанню прибутків. Навпаки, її сукупна вартість володіння певною мірою знижує ефективність АІС, тобто:

$$E_{AIS} = R_{AIS} - TVO_{AIS} - TVO_{IS}, \quad (4.23)$$

де TVO_{IS} – сукупна вартість володіння системи інформаційної безпеки компанії, яка визначається аналогічно до сукупної вартості володіння АІС або будь-якої складової, тобто враховує всі витрати, пов’язані із її функціонуванням, а саме витрати на програмно-апаратне забезпечення системи захисту інформації, її адміністрування, підтримку, розробку певних компонентів, комунікації, людський фактор та можливі простої.

Оскільки система захисту не генерує жодних прибутків, то її ефективність не може бути визначеною з урахуванням доходу від неї, оскільки вона не впливає на нього. Тому відповідні витрати на неї повинні відноситися на той дохід, який генерує АІС підприємства, а не на дохід підприємства, що й пропонується у даній роботі. Якщо б всі можливі загрози можна було б повністю нейтралізувати системою інформаційної безпеки, то формула (4.23) мала б місце для розрахунку ефективності. Але на практиці це неможливо досягти за рахунок різноманітності інформаційних та кібернетичних загроз, виникнення яких за часту передбачити повністю дуже складно. Тоді потенційні втрати знижують автоматично дохід від діяльності АІС на їх величину. Як правило, в якості цих витрат виступатимуть:

– явні витрати на відновлення інформації, які включають: заробітну плату працівників, що займатимуться відновленням, матеріальні витрати на відновлення, заробітну плату працівників, які не працюють під час простою;

– неявні втрати, пов’язані із своєчасною відсутністю інформації на період її відновлення, а саме втрата іміджу, прибутку від втрати клієнтів, втрата вигід від застосування втрачених технологій, тощо.

Для визначення цих втрат можна скористатися формулою (4.24):

$$VL_{IS} = EX_{RI} \times K_{REX}, \tag{4.24}$$

де VL_{IS} – сума втрат від порушення цілісності, доступності та конфіденційності інформації, розрахована у грошовому вимірі;

EX_{RI} – сума витрат на відновлення інформації, яка включає явні та неявні витрати, визначені у грошовому вимірі;

K_{REX} – коефіцієнт збільшення витрат на відновлення інформації. Він буде представляти собою інтегральну оцінку зовнішніх факторів (потенційно можливого отримання доходу), внутрішніх факторів (потенційних витрат на управління), а також ймовірної цінності для злочинців. Можна заздалегідь зробити прогнозні оцінки, які будуть базуватися на попередньому досвіді чи статистики з інших підприємств, і в разі втрат тієї чи іншої інформації можна з

найменшими втратами провести їх оцінку, а також визначити вразливі види інформації, які потребують найбільше витрат на відновлення, розробити сценарії відновлення.

Таким чином, при розрахунку ефекту слід враховувати суму втрат від порушення цілісності, доступності та конфіденційності інформації, яка буде враховувати суму витрат на відновлення інформації, втраченої або порушеної в результаті здійснення кібератак або виникнення інформаційних інцидентів:

$$E_{AIS} = R_{AIS} - TVO_{AIS} - TVO_{IS} - VL_{IS}. \quad (4.25)$$

Автоматизована інформаційна система в цілому та з урахуванням її компонента інформаційної безпеки буде ефективною тільки тоді, коли відбуватиметься зростання доходу, який вона генерує, або зниження витрат, пов'язаних з її функціонуванням. Найбільш результативним для компанії є забезпечення відповідного доходу шляхом оптимізації витрат. Тому для визначення їх оптимального значення необхідно знайти коефіцієнт економічної ефективності витрат на систему. Він визначатиметься за формулою (4.26):

$$KE_{AIS} = \frac{R_{AIS}}{TVO_{AIS} + TVO_{IS} + VL_{IS}}, \quad (4.26)$$

де KE_{AIS} – коефіцієнт економічної ефективності витрат на АІС. Якщо $KE_{AIS} > 1$, то система функціонує ефективно, якщо $KE_{AIS} < 1$, то система функціонує неефективно, якщо $KE_{AIS} = 1$, то дохід від функціонування системи покриває витрати на неї.

Якщо сума СВВ системи інформаційної безпеки та втрат від порушення цілісності, доступності та конфіденційності інформації буде дорівнювати 0, то в цьому випадку коефіцієнт економічної ефективності витрат на АІС буде визначатися за формулою (4.27):

$$KE_{AIS} = \frac{R_{AIS}}{TVO_{AIS}}. \quad (4.27)$$

Рівняння (4.27) можливе тільки у випадку, коли компанія не витрачає додаткові грошові кошти на інформаційну безпеку або АІС вже має вбудовану систему захисту, яка захищає підприємство на 100%. Але даний випадок є нереальним, оскільки різноманіття загроз та інцидентів потребує додаткових засобів захисту та попередження. Саме тому ці витрати впливають на розмір доходу, який генерує АІС підприємства. Тобто, оскільки захист потрібен у будь-якому випадку, то ці витрати будуть фінансуватися саме за рахунок неї, але це відбуватиметься за умови, якщо функціонування АІС є ефективним. В протилежному випадку, дані витрати будуть погашені за рахунок прибутку компанії. Тобто коефіцієнт економічної ефективності витрат на АІС буде визначатися як:

$$KE_{AIS} = \frac{R_{AIS} - (TVO_{IS} + VL_{IS})}{TVO_{AIS} + TVO_{IS} + VL_{IS}}. \quad (4.28)$$

У даному випадку коефіцієнт, розрахований за формулою (4.28), дозволить визначити суму допустимих витрат для створення системи інформаційного захисту, тобто їх значення, враховане у формулі, є найбільш прийнятним та відповідає поточному рівню доходу від функціонування АІС та поточному рівню СВВ АІС. Але також можна спланувати, який максимальний рівень витрат на інформаційну безпеку може дозволити собі компанія, щоб хоча б забезпечити значення коефіцієнту економічної ефективності витрат на АІС на рівні 1, тобто:

$$1 = \frac{R_{AIS} - (TVO_{IS} + VL_{IS})}{TVO_{AIS} + TVO_{IS} + VL_{IS}} \Rightarrow TVO_{IS} + VL_{IS} = \frac{1}{2} \times (R_{AIS} - TVO_{AIS}). \quad (4.29)$$

Для реалізації запропонованого підходу визначення витрат на інформаційну безпеку та можливих резервів на їх збільшення проведено

розрахунки на основі емпіричних даних щодо різних компаній, які відрізняються розмірами та видами діяльності. Для цього було використано дані звіту компанії IBM, в якому було надано інформацію щодо загальних розмірів вартості втрат компаній в результаті дій інсайдерів, тобто представлені наслідки внутрішніх загроз [58]. Цю інформацію використаємо для знаходження середнього значення втрат на 1 працівника в залежності від розміру підприємства, що представлено у таблиці 4.2. Оскільки не відомо конкретно, яка була чисельність кожного з підприємств, що сформували вибірку для розрахунку втрат, то використаємо імітовану їх кількість, щоб визначити середню чисельність.

Таблиця 4.2 – Результати визначення середнього значення втрат від дій інсайдерів на 1-го працівника компанії

Чисельність компаній, особи [58]	% компаній [58]	Кількість компаній, одиниць*	Загальні втрати від порушення даних, долари США [58]	Імітована середня чисельність 1 підприємст-ва, особи*	Загальна чисель-ність, особи*	Середні втрати на 1-го працівника, долари США*
До 500	14	29	7680000	277	8033	956,06
501 - 1000	15	31	6920000	763	23653	292,56
1001 - 5000	21	43	9650000	3057	131451	73,41
5001 - 10000	18	37	12640000	7645	282865	44,69
10001 - 25000	16	33	13950000	17739	585387	23,83
25001 - 75000	10	20	17920000	50935	1018700	17,59
>75000	6	11	16650000	81381	895191	18,60
Підсумок	100	204	85410000	–	2945280	29,00

* – розраховано авторкою

Також необхідно визначити втрати компаній на 1 працівника від зовнішніх загроз. З цією метою було використано дані звіту компанії IBM про вартість витоку інформації за 2020 рік, звідки було узято інформацію щодо розміру вибірки компаній та загального розміру втрат [57]. Результати розрахунків представлені у таблиці 4.3.

Таблиця 4.3 – Результати визначення середнього значення втрат від витоку інформації завдяки зовнішнім загрозам на 1-го працівника компанії

Чисельність компаній, особи [57]	% компаній [57]	Кількість компаній, одиниць*	Загальні втрати від витоку даних, долари США [57]	Імітована середня чисельність 1 підприємства, особи*	Загальна чисельність, особи*	Середні втрати на 1-го працівника, долари США*
До 500	13	68	2350000	265	18020	130,41
501 - 1000	12	63	2530000	773	48699	51,95
1001 - 5000	21	110	3780000	2905	319550	11,83
5001 - 10000	23	121	4720000	7469	903749	5,22
10001 - 25000	14	73	4610000	17722	1293706	3,56
>25000	17	89	4250000	51791	4609399	0,92
Підсумок	100	524	22240000	–	7193123	3,09

* – розраховано авторкою

Сума середніх втрат від дій інсайдерів на 1-го працівника (див. табл. 4.2) та середніх втрат від витоку інформації завдяки зовнішнім загрозам на 1-го працівника (див. табл. 4.3) – це сума втрат від порушення цілісності, доступності та конфіденційності інформації (VL_{IS}) (див. табл. 4.4). Використовуючи неусереднені, а реальні дані підприємств, можна більш точніше визначити ці значення, враховуючи, як внутрішні, так й зовнішні загрози.

Таблиця 4.4 – Сума втрат від порушення цілісності, доступності та конфіденційності інформації (VL_{IS})

Назва показника	Розмір компаній					
	До 500	501-1000	1001-5000	5001-10000	10001-25000	>25000
Середні втрати від дій інсайдерів на 1-го працівника, долари США	956,06	292,56	73,41	44,69	23,83	17,59
Середні втрати від витоку інформації завдяки зовнішнім загрозам на 1-го працівника, долари США	130,41	51,95	11,83	5,22	3,56	0,92
VL_{IS}, долари США	1086,47	344,52	85,24	49,91	27,39	18,51

Результати розрахунків, наведені у таблиці 4.4, представимо на графіку 4.7.

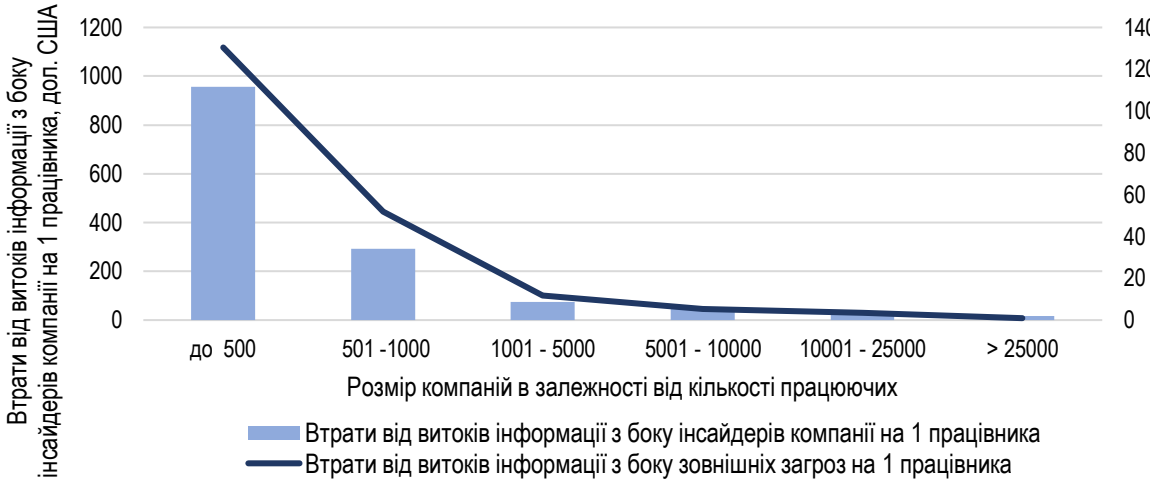


Рисунок 4.7 – Втрати компаній від кіберінцидентів на одного працівника в залежності від їх розмірів (складено авторкою)

Тобто можна зробити висновок, що компанії, які відносяться до малих і середніх, у найбільшій мірі потерпають від кіберзагроз, оскільки на одного працюючого припадає великий обсяг фінансових втрат у порівнянні із великими підприємствами (рисунок 4.7). Це можна обґрунтувати рядом факторів, таких як:

1) великі компанії мають більшу кількість досвідчених фахівців в галузі інформаційної безпеки, оскільки рівень заробітних плат, встановлений ними, є значно вищим у порівнянні із компаніями малого та середнього бізнесу, що у більшій мірі приваблює висококваліфікованих працівників до роботи саме на підприємствах такого рівня;

2) великі компанії мають розгалужену структуру та за часту їх материнська компанія засновується в країнах із високим рівнем економічного розвитку (США, Німеччина, Великобританія, тощо). Відповідно рівень контролю за процесами захисту інформації є підвищеним, ніж для малих та середніх компаній, оскільки відповідальність за процесами безпеки розповсюджується на всю велику структуру компанії;

3) для великих компаній характерний розподіл рівня відповідальності між фахівцями, що зменшує кількість втручань працівників у будь-які процеси,

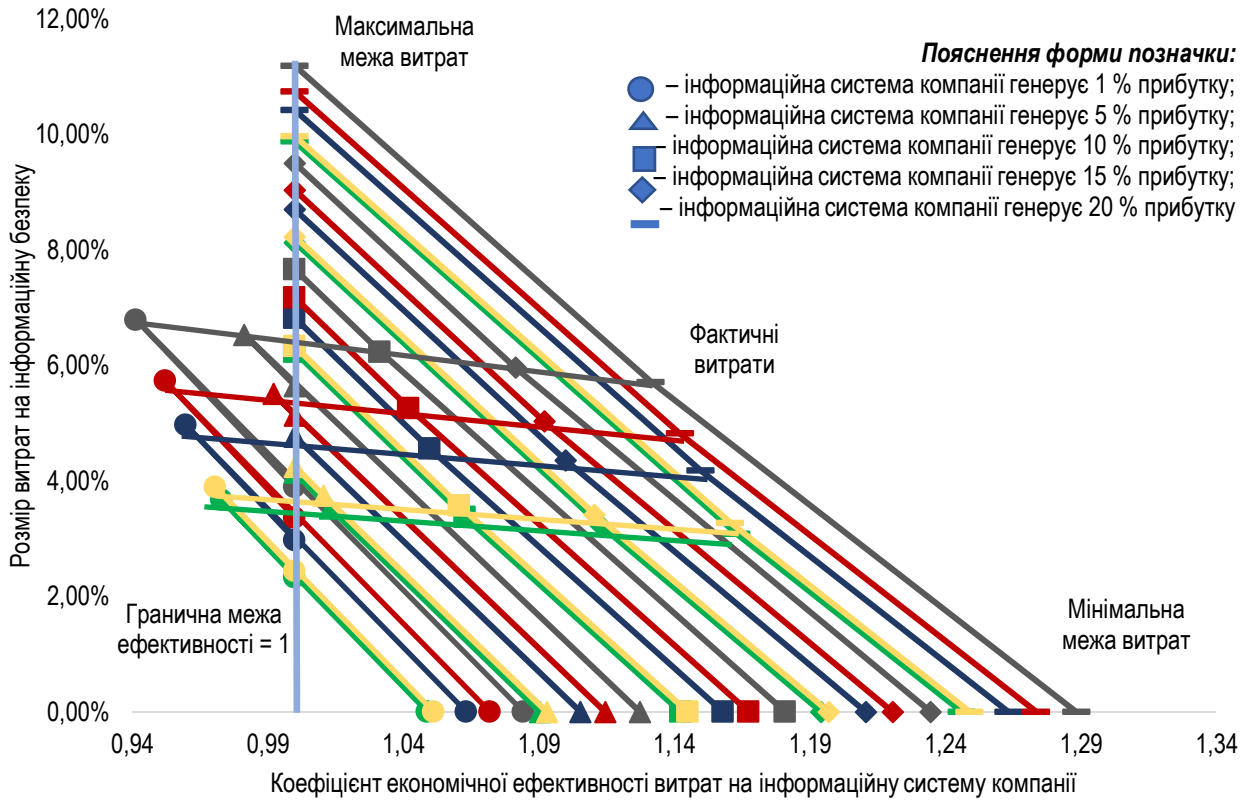
знижує можливості формування злочинних зговорів, а також не дозволяє окремим особам мати надмірні функціональні повноваження, що призводить до зловживання ними службового становища;

4) великі компанії дотримуються виконання міжнародних стандартів, які регламентують процеси безпеки. Це знов таки пов'язано із міжнародним рівнем їх функціонування. Що стосується малих та середніх компаній, то їх більшість орієнтується на нормативно-правову базу тієї країни, де вони здійснюють свою діяльність. Відповідно недоліки правового забезпечення процесів інформаційної безпеки можуть призводити до існування слабких місць.

Хоча рівень втрат від дій інсайдерів та зловмисників є більшим у абсолютному виразі для великих компаній, оскільки масштаби їх діяльності приваблюють злочинців зі всього світу, але саме показник у відносному виразі дозволяє зробити висновок щодо більшої чутливості малих та середніх компаній чисельністю до 500 осіб до наслідків інформаційних загроз.

Для визначення ССВ AIC та ССВ інформаційної безпеки було використано дані звіту компанії Deloitte. Для розрахунків було узято усереднені значення витрат IT-безпеки на 1 людину та витрати на IT-безпеку у відсотках від загального бюджету на IT по галузям [23]. Дані значення дозволили обчислити ССВ AIC та ССВ інформаційної безпеки. Використовуючи формули (4.27)-(4.29), було розраховано показники ефективності та граничні значення витрат на інформаційну безпеку. В якості значення прибутку, який генерує AIC, було узято різні його варіанти, тобто 1%, 5%, 10%, 15% та 20% перевищення від загальної суми витрат на систему ($TVO_{AIS} + TVO_{IS} + VL_{IS}$). Дані значення було обрано з метою обґрунтування меж витрат, виходячи із результатів функціонування інформаційної системи підприємства.

На рисунку 4.8 представлено максимальне, дійсне та мінімальне значення суми TVO_{IS} та VL_{IS}, які відповідають різним значенням коефіцієнта ефективності функціонування автоматизованої інформаційної системи, а також різним варіантам прибутку для підприємств із кількістю працюючих до 500 осіб різних галузей діяльності.



Пояснення кольору лінії: **синій** – підприємства галузі роздрібної торгівлі / корпоративного банкінгу; **червоний** – споживання / небанківських фінансових послуг; **сірий** – страхування; **зелений** – постачальники послуг; **жовтий** – компанії – фінансові утиліти (бізнес-консалтингові компанії)

Рисунок 4.8 – Співвідношення розміру витрат на інформаційну безпеку та коефіцієнта економічної ефективності витрат на інформаційну систему для підприємств різних галузей із кількістю до 500 осіб (складено авторкою)

На рисунку 4.8 можна побачити, що у випадку, коли АІС генерує дохід, який перевищує витрати на 1%, то дійсний рівень витрат на інформаційну безпеку не покривається за рахунок існуючого рівня прибутку. У цьому випадку функціонування АІС є неефективним, оскільки коефіцієнт ефективності буде знаходитися від 0,94 для страхових компаній до 0,97 для постачальників послуг. Це може бути причиною: здійснення необґрунтовано високих витрат на інформаційну безпеку; недостатньої ефективності АІС компанії за рахунок недовикористання її потенційних можливостей, або за рахунок її низької програмно-технічної здатності для надання інформаційних послуг підрозділам підприємства. При цьому максимальний рівень витрат на інформаційну безпеку

у цих умовах може бути забезпечений від 2,33% для постачальників послуг до 3,89% для страхових компаній.

На рисунку 4.8 можна побачити, що для страхових компаній та підприємств споживання / небанківських фінансових послуг 5% прибутку AIC також не забезпечують необхідний рівень витрат на інформаційну безпеку. Для компаній інших галузей цей рівень прибутку забезпечує витрати, але при цьому коефіцієнт ефективності дорівнює 1. Максимальний рівень витрат на інформаційну безпеку у цих умовах може бути забезпечений від 4,15% для постачальників послуг до 5,65% для страхових компаній.

У випадку розміру прибутку 10% граничні межі витрат на інформаційну безпеку можуть дорівнювати від 6,23% до 7,66%, для прибутку 15% – від 8,13% до 9,50%, для прибутку 20% – від 9,88% до 11,19%.

Аналогічно проведемо розрахунки для підприємств із кількістю працюючих від 501 до 1000 осіб, від 1001 до 5000 осіб, від 5001 до 10000 осіб, від 10001 до 25000 осіб та більше 25000 осіб. При цьому врахуємо різні варіанти прибутку від AIC, а також той факт, що підприємства відносяться до різних галузей діяльності. Результати розрахунків представлено на графіках И.1 – И.5 в додатку И.

Так, 1% перевищення доходу від AIC над витратами не забезпечить в повному обсязі витрат на інформаційну безпеку підприємства із чисельністю від 501 до 1000 осіб (рисунок И.1 додатку И), хоча розмір такого перевищення є нижчим, ніж для малих та середніх підприємств. Для підприємств із чисельністю 1001 особа і вище (рисунки И.2 – И.5 додатку И), 1% доходу може забезпечити фактичний обсяг витрат на інформаційну безпеку, та при цьому зберегти значення коефіцієнту ефективності вище 1.

Для підприємств із чисельністю 501 особа та вище 5% перевищення доходу від AIC буде достатньо для покриття витрат, пов’язаних із інформаційним захистом (рисунки И.2 – И.5 додатку И). При зростанні відсотку прибутку спостерігатиметься збільшення граничної межи витрат для підприємств всіх галузей. Але для компаній із кількістю працюючих більше, ніж 500 осіб,

зростання прибутку призводить до того, що межа для підприємств різних галузей стає близькою за значенням та не залежить від галузевої спрямованості діяльності (рисунки И.2 – И.5 додатку И). При цьому для підприємств із чисельністю від 501 до 1000 осіб можуть забезпечуватися такі граничні витрати: 1,02% – 1,40% (для рівня прибутку 1%), 2,88% – 3,25% (5% прибутку), 5,02% – 5,38% (10 % прибутку), 6,98% – 7,32% (15% прибутку), 8,77% – 9,10% (20% прибутку); від 1001 до 5000 осіб забезпечується: 0,64% – 0,74% (для рівня прибутку 1%), 2,52% – 2,62% (5% прибутку), 4,68% – 4,77% (10 % прибутку), 6,65% – 6,74% (15% прибутку), 8,46% – 8,54% (20% прибутку); від 5001 до 10000 осіб забезпечується: 0,54% – 0,58% (для рівня прибутку 1%), 2,43% – 2,46% (5% прибутку), 4,59% – 4,62% (10 % прибутку), 6,56% – 6,59% (15% прибутку), 8,37% – 8,40% (20% прибутку); від 10001 до 25000 осіб забезпечується: 0,52% – 0,53% (для рівня прибутку 1%), 2,40% – 2,41% (5% прибутку), 4,56% – 4,58% (10 % прибутку), 6,54% – 6,55% (15% прибутку), 8,35% – 8,36% (20% прибутку); вище 25000 осіб забезпечується: 0,50% – 0,51% (для рівня прибутку 1%), 2,39% (5% прибутку), 4,55% – 4,56% (10 % прибутку), 6,53% (15% прибутку), 8,34% (20% прибутку).

За економічною моделлю Гордона–Лоєба, яка дозволяє аналізувати оптимальний розмір інвестування в інформаційну безпеку, встановлено, що максимально ефективно інвестувати у захист інформації можна тільки на рівні 37% від сум прогнозованих втрат [107]. Дану модель широко застосовують у наукових колах та для потреб практики. Використаємо запропонований підхід до визначення обґрунтованих меж витрат на інформаційну безпеку з урахуванням того, що компаніям необхідно забезпечити 37% витрат на інформаційну безпеку, тобто прогнозованих втрат. Розрахуємо рівень прибутку AIC, який повинні генерувати компанії у такому випадку (рисунок 4.9).

Розрахунки свідчать, що забезпечення 37% витрат на інформаційну безпеку можливе за умови отримання прибутку від функціонування AIC на рівні від 359% до 370% для підприємств із чисельністю до 500 осіб та від 382% до 384% для підприємств із чисельністю більше ніж 25000 працюючих.

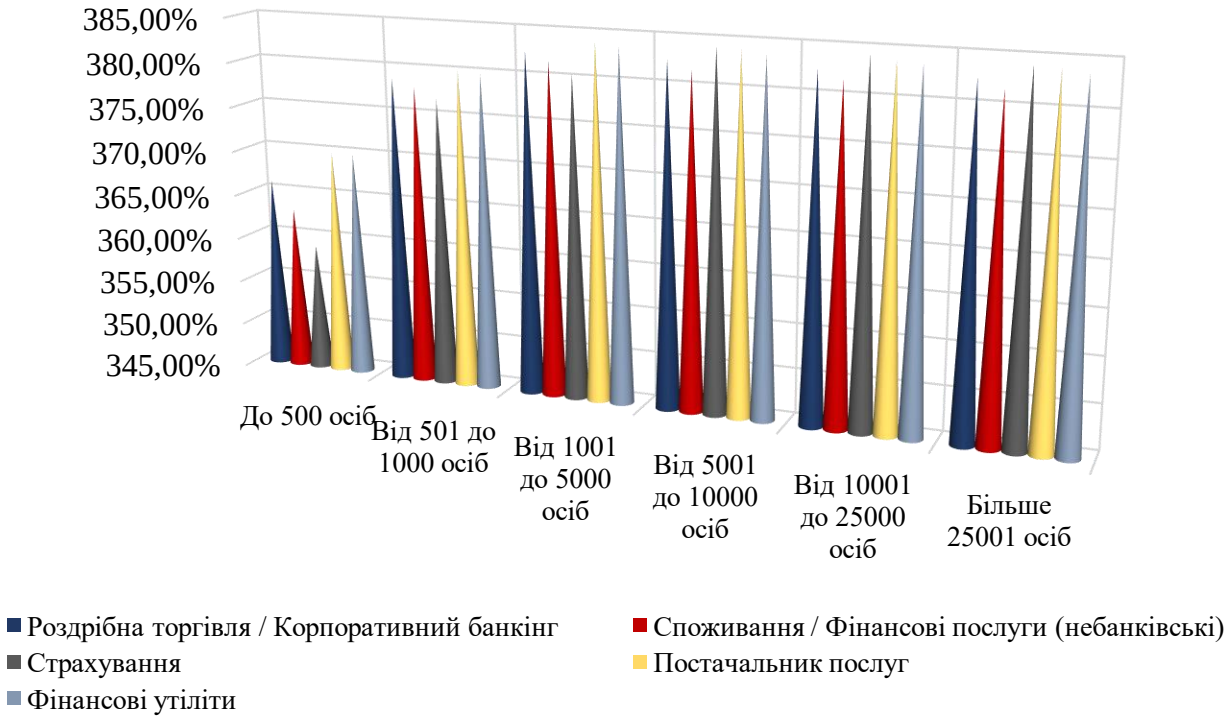


Рисунок 4.9 – Значення прибутку від AIC за умови, якщо рівень витрат на інформаційну безпеку складатиме 37% (складено авторкою)

Отримані результати є дуже суперечливими, оскільки такий рівень прибутку не зможе забезпечити жодна AIC. Це тільки ймовірно можливо для тих компаній, де IT-підрозділ функціонує за принципом «держава у державі». Також, на нашу думку, на отриманий результат вплинув рівень витрат на інформаційну безпеку в обсязі 37%, який за моделлю Гордона-Лоєба було визначено, виходячи з загального прибутку компанії, а не прибутку AIC, що використано у даному дослідженні. Тому запропонована у роботі методологія відповідає підходу обґрунтування витрат за рахунок саме прибутків від AIC компанії.

Отримані результати дослідження дозволяють сформувати наступні орієнтири для реалізації заходів державних програм інформаційної безпеки. Головним напрямом є формування орієнтирів для підприємств малого та середнього бізнесу, які схильні до найбільших витрат у випадках масових кіберзагроз. Так, рекомендується:

1) організувати забезпечення якісної підготовки фахівців у сфері інформаційної безпеки не тільки на рівні отримання вищої освіти, але й на рівні

організації спеціалізованих курсів підвищення кваліфікації для представників малого та середнього бізнесу;

2) забезпечити можливості сертифікації професійних IT-аудиторів та фахівців внутрішнього контролю, що дозволить їм здійснювати моніторинг IT-систем та завчасно виявляти порушення. Особливо цей напрям є актуальним для державних підприємств, наприклад, галузі охорони здоров'я, оскільки саме ця галузь є лідером за фактами кіберзлочинів, направлених проти них (за 2020 рік втрати від витоків інформації з боку зовнішніх кіберзлочинців для підприємств охорони здоров'я склали 7,13 млн. дол. [57]);

3) розробити та впровадити систему централізованого збору інформації щодо випадків витоків інформації та кіберзлочинів, яка повинна охоплювати дані щодо якісних та кількісних характеристик таких інцидентів. Це можливо за рахунок створення форми статистичної звітності, яку компанії можуть надавати поряд із фінансовою звітністю. Цей захід дозволить сформувати базу даних щодо рівня втрат, цінності інформації, періоду виявлення витоків, періоду відновлення, тощо. Використовуючи цю інформацію та запропонований в роботі підхід, можливо визначити обґрунтовані межі витрат для більшої кількості галузей, а також для підприємств із різною чисельністю працюючих, та запропонувати рекомендації щодо розробки планів інвестування в IT-безпеку;

4) створити систему забезпечення створення державних програм підтримки малого та середнього бізнесу щодо проведення їх консультування з боку високо кваліфікованих фахівців з питань ефективності інформаційної безпеки;

5) розробити стратегії розвитку підприємств різних галузей народного господарства в частині залучення іноземних інвестицій для підтримки компаній малого та середнього бізнесу сфери сервісних послуг, які у порівнянні із іншими галузями мають найнижчий рівень інвестування у розвиток систем інформаційної безпеки;

6) сприяти розповсюдженню методики обґрунтування витрат на інформаційну безпеку на державному рівні.

4.3 Розробка методології визначення ролі цифрової спроможності та кібербезпеки країни у забезпеченні збалансованості розвитку національної економіки

Стійкість розвитку національної економіки будь-якої країни забезпечується за рахунок збалансованої взаємодії ряду факторів. Так, це підтверджується дослідженнями таких науковців як: Бойко А. [278], Загорський В., Борощук Є., Жолобчук І. [291], Кулініч О. [322], Лопатинський Ю.М. Меглей В.І. [324], Міхальова К. [330], Філіпішина Л. [368], Ходжаян А. [370], Цанько О. [371] та інші. З аналізу їх наукових праць можна виділити, що найбільший вплив на розвиток економіки країни здійснюють саме соціальні, політичні та суто економічні фактори, хоча можна виділити ряд й інших, таких як екологічні, демографічні, технологічні. Але з результатів, отриманих у підрозділі 2.1 даної роботи також встановлено, що фактори, пов’язані із інформаційною безпекою також здійснюють вплив на розвиток національної економіки. Відповідно за рахунок збалансованої взаємодії цих чотирьох сфер відбувається або розвиток національної економіки країни, або його гальмування, що викликається їх дисбалансом. Тому дуже важливо розуміти, що сприяє нестабільності та які чинники необхідно прийняти до уваги, щоб змінити вектор розвитку у напрямок його зростання або забезпечення стійкості.

Обґрунтований у підрозділі 2.2 взаємовплив між рядом показників дозволив сформувати інтегральний індекс інформаційної безпеки національної економіки. Оскільки для визначення рівня збалансованості її сфер до уваги слід приймати комплексні показники, а не первинні, які стосуються тільки одного параметра економіки, то це потрібно прийняти до уваги в подальших розрахунках.

Так, в даній роботі пропонується науково-методичний підхід, який дозволить побудувати багатополюсну (у цьому випадку чотириполюсну)

барицентричну модель збалансованості розвитку держави, що інтегрує композитні таргети економічного, соціального, політичного вимірів та виміру інформаційної безпеки, що сприятиме визначенню рівня збалансованості розвитку країни, виявити ті сфери, де відбувається його дестабілізація. В якості виміру інформаційної безпеки будемо використовувати групу показників цифрової спроможності та кібербезпеки, які дозволяють її ідентифікувати та вимірювати з різних аспектів.

Ідея підходу базується на визначенні центру мас багатокутника, де забезпечується стійкість геометричної фігури. Її вершинами можуть виступати різні показники або виміри, які інтегрують їх набір. Їх кількість може бути обумовлена набором тих сфер, які впливають на рівень збалансованого розвитку країни. При цьому формування сфери обумовлюється за рахунок різного набору показників, які за своєю сутністю повинні бути комплексними. Так, застосування даного підходу знайшло практичне використання для ринку страхування та перестрахування в роботах Кузьменко О. (Меренкової О.), Козьменко О., Бойко А. [312], де розробляється модель стійкості на основі трикутника. Також загальний підхід без практичної реалізації було запропоновано для аналізу ділової активності компаній в роботі Берзіна П., Шишкіної О., Кузьменко О., Яровенко Г. [24].

Оскільки в роботі було обрано чотири виміри, то в якості багатокутника повинен виступати чотирикутник. Відповідно метою реалізації буде знаходження центру його мас.

На *першому етапі* обираємо базу показників-факторів, які характеризують рівень розвитку кожного з чотирьох вимірів. Деякі з них здійснюють позитивний вплив, в результаті чого відбувається підвищення стабільності. Такі чинники є стимуляторами. Інші показники чинять негативний вплив та призводять до розбалансування чотирьох сфер, які, відповідно, називаються дестимуляторами. На основі аналізу та синтезу, індукції та дедукції наукової літератури оберемо фактори, що формують композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки (див. табл. 4.5).

Таблиця 4.5 – Фактори, що формують композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки

Назва виміру	Назва факторів, які формують композитні таргети	Зміст факторів
Економічний	Індекс економічної свободи – Economic freedom index (+)	Індекс, який вимірює людини контролювати власну працю та майно, рівень власного споживання та інвестування. Більш високе значення свідчить про високий рівень економічної свободи для людини [7]
	Індекс нерівномірного економічного розвитку – Uneven economic development index (-)	Показник враховує нерівність в економіці незалежно від показників економіки. Він розглядає структурну нерівність (расову, етнічну, регіональну, освітню, тощо), яка викликає економічну різницю між даними групами, що врешті решт впливає на економічний розвиток. Найбільше значення індексу відповідає найвищому рівню нерівномірності економічного розвитку [83]
	Індекс фінансового розвитку – Financial development index (+)	Індекс, який вимірює та аналізує фактори впливу розвитку фінансових систем на зростання, стабільність та нерівність різних економік. Найвище значення відповідає високому рівню розвитку фінансової системи країни [89]
	Індекс легкості ведення бізнесу – Ease of doing business (+)	Індекс дозволяє порівнювати умови ведення бізнесу у країні. Більш високий рейтинг (низьке числове значення) свідчить про простіші правила для бізнесу та посилений захист прав власності [74, с. 1]
	Індекс глобальної конкурентоспроможності – The Global Competitiveness Index (+)	Індекс оцінює спроможність країн забезпечити високий рівень добробуту громадян. Чим вище оцінка, тим більші можливості у країни щодо забезпечення добробуту своїх громадян [209, с. v-vii]
Політичний	Індекс політичної стабільності – Political stability index (+)	Індекс вимірює рівень ймовірності того, що уряд країни може бути дестабілізований або зруйнований засобами, які носять неконституційний та насильницький характер, в тому числі військові перевороти та тероризм. Найвище значення відповідає найбільш стабільному уряду країни [197]
	Індекс демократії – Democracy index (+)	Індекс вимірює якість демократії у країні на основі оцінок виборчого процесу та плюралізму, громадянської свободи, функціонування уряду, політичної участі та політичної культури, та дозволяє визначити тип режиму – «повна демократія», «вада», «гібридний режим» та «авторитарний режим». Шкала оцінки – від 0 до 100. Найвищі значення відповідають режиму повної демократії, найнижчі – авторитарному режиму [67, с.2]
	Індекс ефективності уряду – Government effectiveness index (+)	Індекс вимірює якість уряду країни, що полягає у оцінці якості державних послуг, державної служби, ступеня незалежності від політичного тиску, якості формування та реалізації політичних заходів, рівня

Продовження таблиці 4.5

Назва виміру	Назва факторів, які формують композитні таргети	Зміст факторів
		довіри до такого уряду та його рішень. Найвище значення оцінки відповідає найбільш якісному уряду країни [109, с.1]
	Індекс сприйняття корупції – Corruption Perceptions Index (+)	Індекс вимірює передбачуваний рівень корупції у державному секторі, що показує також й ступінь контролю державою корупційних процесів, здатних знижувати рівень демократії у суспільстві. Шкала оцінки – від 0 до 100. Найвища оцінка відповідає тим країнам, в яких відсутня корупція [55, с. 1]
Соціальний	Індекс щастя – Happiness Index (+)	Індекс вимірює якість поточного життя населення країн та є частиною Всесвітнього звіту про щастя. Оцінки здійснюються за шкалою від 0 до 10. Чим вище значення, тим вище якість життя [111]
	Індекс соціального прогресу – Social Progress Index (+)	Індекс вимірює рівень забезпечення країнами основних потреб людини, їх добробуту та можливостей для прогресу. Найвище значення, яке прямує до 1, свідчить про високий рівень соціального прогресу для країни [6]
	Індекс людського розвитку – Human Development Index (+)	Індекс вимірює рівень життя, грамотності, освіченості і довголіття, як основних характеристик людського потенціалу досліджуваної території. Найвище значення, яке наближається до 1, свідчить про високий рівень людського розвитку в країні [121]
Цифрової спроможності і кібербезпеки	Глобальний індекс кібербезпеки – Global Cybersecurity Index (+); Національний індекс кібербезпеки – National Cyber Security Index (+); Індекс розвитку ІКТ – ICT Development Index (+); Рівень цифрового розвитку – Digital Development Level (+); Індекс мережевої готовності – Networked Readiness Index (+) Зміст факторів розкрито в підрозділі 2.1 даної роботи	

* (+) – фактор стимулятор: збільшення його значення підвищує рівень стабільного розвитку країни; (–) – фактор дестимулятор: збільшення його значення знижує рівень стабільного розвитку країни.

Емпіричні дані можуть бути часовими, узятими тільки для однієї країни, а можуть бути просторовими, узятими для різних країн за один проміжок часу. У першому випадку виконується другий етап, у другому – за даною методикою виконується третій етап.

На *другому етапі* необхідно дослідити обрані фактори на аномальність. Спочатку представимо фактори у вигляді часових рядів, тобто ряду даних, які змінюються із часом. Можлива така ситуація, коли будь яке його значення

значно відхиляється від середнього, то в цьому випадку маємо справу з аномальним значенням або викидом. Їх також необхідно враховувати в процесі моделювання економічних явищ, оскільки аномальність може бути не типовим явищем, яке необхідно вміти виявляти та прогнозувати у майбутньому. Для цієї мети використовуються різні критерії, такі як критерій Ірвіна, модифікований критерій Ірвіна, критерій Діксона та інші. Наприклад, оберемо модифікований критерій Ірвіна, як найбільш простий та ефективний, який ґрунтується на порівнянні сусідніх рівнів ряду. Спочатку розраховується за формулою (4.30) середньоквадратичне відхилення по часовому ряду, але береться не уся сукупність спостережень, а тільки кожні три:

$$\hat{\sigma}_y = \sqrt{\frac{\sum_{t=1}^{n}((y_{t-1}-\bar{y}_t)^2+(y_{t+1}-\bar{y}_t)^2)}{2}}, \tag{4.30}$$

де $\hat{\sigma}_y$ – це середньоквадратичне відхилення за трьома спостереженнями;

y_{t-1} – попередній рівень ряду;

y_{t+1} – наступний рівень ряду;

n – довжина ряду, в даному випадку буде дорівнювати 3;

$\bar{y}_t$ – середнє значення для двох сусідніх значень, яке розраховується як:

$$\bar{y}_t = \frac{y_{t-1}+y_{t+1}}{2},\ t = 2,3,\dots,n-1, \tag{4.31}$$

Для знаходження аномальних значень розраховуються за формулою (4.32) характеристики λ_t, отримані значення яких порівнюються з критичним значенням λ_α. Якщо розраховані значення λ_t не перевищують критичні, то це говорить про відсутність аномального значення для заданого рівня ряду, в протилежному випадку існує викид.

$$\lambda_t = \frac{|y_t-y_{t-1}|}{\hat{\sigma}_y},\ t = 2,3,\dots,n. \tag{4.32}$$

Якщо було виявлено аномальне значення, то деякі методики пропонують позбутися його та продовжувати розрахунки без його значення. В інших методиках рекомендується замінити його усередненим значенням. Для моделювання економічних явищ та процесів важливо розуміти, що є ситуації, які можуть генерувати викид, тому їх доцільно враховувати. Для цього пропонується використання додаткової фіктивної змінної, значення якої буде дорівнювати «0» для тих рівнів ряду, в яких не спостерігається аномалія, та «1» для тих, де виявлено викид.

На *третьому етапі* проводиться нормалізація значень факторів. Це пов'язано із різною їх природою, що проявляється у відмінностях їх абсолютних величин. Застосування нормалізації до вирішення даної проблеми дозволить звести їх від 0 до 1, що в подальшому сприятиме їх згортці та визначенню композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності та кібербезпеки.

Для просторових даних доцільно використовувати лінійну нормалізацію, що проводиться за формулою (4.33), оскільки спостереження є незалежними один від одного та не підпорядковані законам розподілу:

$$\widetilde{x_{ik}} = \frac{x_{ik} - x_{min_i}}{x_{max_i} - x_{min_i}}, \tag{4.33}$$

де $\widetilde{x_{ik}}$ – нормалізоване вхідне значення фактору економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки;

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

x_{min_i} та x_{max_i} – відповідно мінімальне та максимальне значення фактору економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки серед усіх спостережень.

Формула (4.33) застосовується для змінних-стимуляторів. Для дестимуляторів слід використати її модифікацію (4.34):

$$\widetilde{x_{ik}} = 1 - \frac{x_{ik} - x_{min_i}}{x_{max_i} - x_{min_i}}. \quad (4.34)$$

Для часових даних можна також використовувати лінійну нормалізацію, але за умови перевірки даних на нормальний розподіл. У іншому випадку краще використати нелінійну нормалізацію, наприклад, сигмоїдну логістичну функцію (4.35):

$$\widetilde{x_{ik}} = \frac{1}{e^{-a(x_{ik} - x_{ci})} + 1}, \quad (4.35)$$

де a – це параметр, який впливає на ступінь зміни нелінійності змінної в інтервалі, що нормалізується, та знаходиться в інтервалі від 0 до 1;

x_{ci} – центр інтервалів змін вхідних значень факторів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки, що підлягають нормалізації, та які розраховуються за формулою (4.36):

$$x_{ci} = \left(x_{min_i} + x_{max_i}\right)/2. \quad (4.36)$$

На *четвертому етапі* відбувається розрахунок інтегральних показників, тобто композитних таргетів для кожного виміру – економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки. За умови використання просторових даних пропонується його розрахунок із використанням середньогеометричної функції (4.37), оскільки вона дозволяє визначати середнє пропорційне значення, яке відноситься до одного числа так само, як і інше число до середньогеометричного:

$$G(\widetilde{x_1}, \widetilde{x_2}, \dots, \widetilde{x_n}) = \left(\prod_{i=1}^{n} \widetilde{x_i} \right)^{1/n}, \quad (4.37)$$

де $G(\widetilde{x_1}, \widetilde{x_2}, \dots, \widetilde{x_n})$ – середньогеометричне значення нормалізованих вхідних значень факторів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки, яке виступає композитним таргетом;

n – кількість факторів у кожному із вимірів.

Для формування інтегральних показників для часових даних краще скористатися формулою метрик Мінковського (4.38):

$$R(x_i) = 1 - \sqrt{\sum_{j=1}^{k} \omega_j \left| 1 - \frac{x_{ij}}{x_{max_j}} \right|^2 + \sum_{j=k+1}^{n} \omega_j \left| 1 - \frac{x_{min_j}}{x_{ij}} \right|^2}, \quad (4.38)$$

де $R(x_i)$ – інтегральний показник – композитний таргет економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки;

ω_j – вага кожного фактору, з якою він впливає на загальну функцію. У якості таких вагів можна використати стандартизовані коефіцієнти множинної регресії. Умовою для формування вагів є $\sum_{j=1}^{n} \omega_j = 1$, яка виконується, якщо визначити суму стандартизованих коефіцієнтів.

Також формулу (4.38) необхідно застосувати в умовах дослідження просторових даних для тих спостережень, які після нормалізації будуть мати нульове значення. У випадку використання середньогеометричної функції це дозволить уникнути отримання значення таргету рівним 0.

Не залежно від виду даних отримуємо чотири композитні таргети факторів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки. Значення інтегрального показника, яке

наближатиметься до 1, буде говорити про досягнення максимального рівня розвитку даної сфери.

На *п'ятому етапі* будується чотириполюсна барицентрична модель збалансованості розвитку держави, що інтегрує композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки (рисунок 4.10).

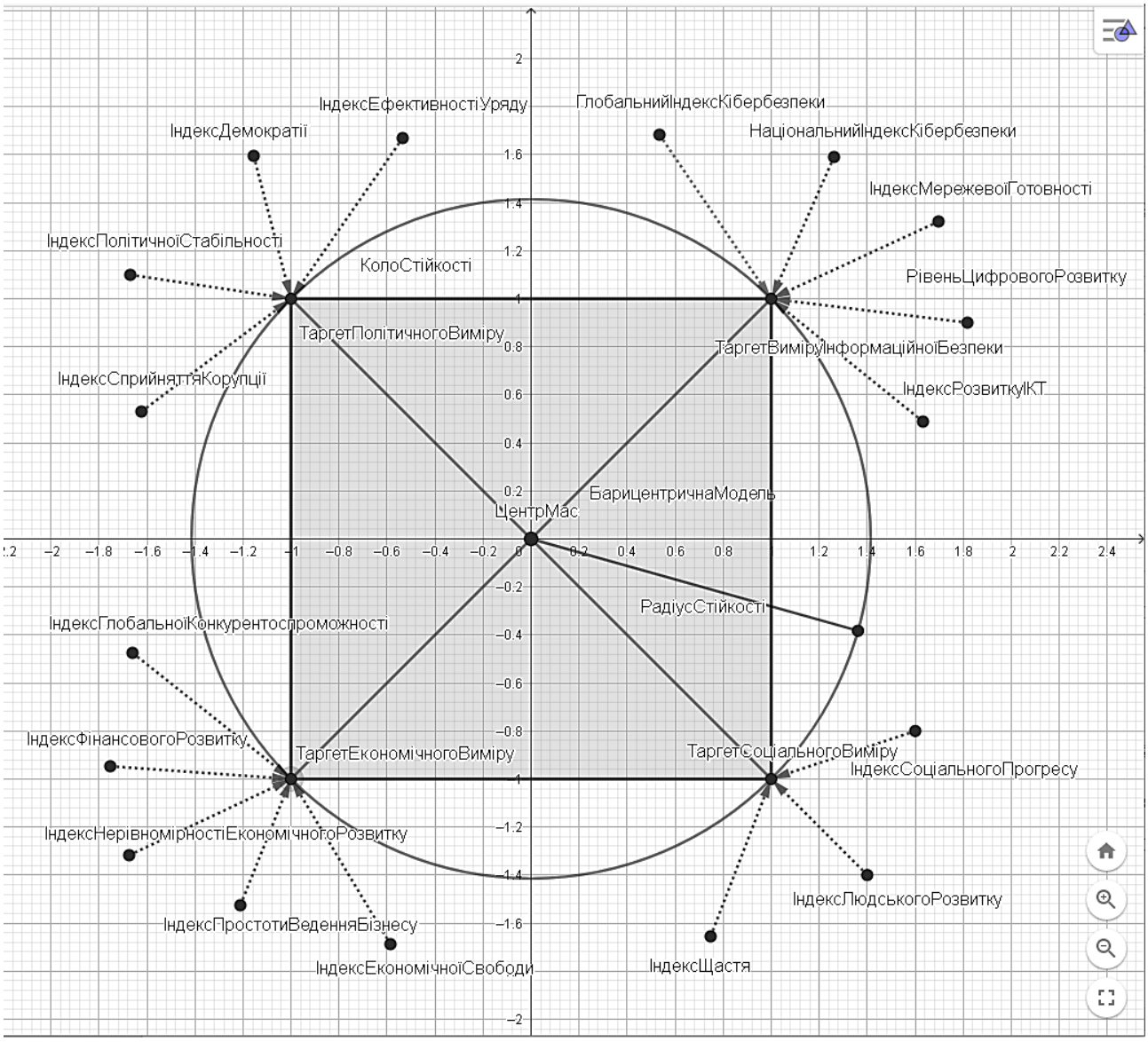


Рисунок 4.10 – Еталонна чотириполюсна барицентрична модель збалансованості розвитку країни (складено авторкою)

На рисунку 4.10 представлена еталонна модель чотирикутника – квадрату, вершини якого виступають інтегральними показниками, що визначаються на

четвертому етапі, та які формуються з набору факторів. Її було побудовано із використанням програмного забезпечення GeoGebra. У даному випадку квадрат виступає еталоном, центроїд (центр мас) якого знаходиться у точці перетину його діагоналей (“ЦентрМас”) із координатами (0;0), яка також співпадає з центром описаного кола. Вершини квадрату знаходяться у точках із координатами (1;1) для виміру цифрової спроможності і кібербезпеки, (1;-1) для соціального виміру, (-1;-1) для економічного виміру, (-1;0) для політичного виміру. Значення цих координат відповідають максимальному значенню композитних таргетів, які може досягнути країна за умов потужного розвитку.

На практиці отримати ідеальний квадрат буде практично неможливо, оскільки за таких умов країна, яка має таку модель, є по суті супер-країною із максимально розвинутими економічною, соціальною, політичною сферами та сферою інформаційної безпеки. Тому по факту співвідношення чотирьох груп факторів буде генерувати різні форми чотирикутників – опуклі, увігнуті та складні, з різними довжинами боків та різними кутами.

Можливо буде встановлено, що за обраними параметрами виявиться незначна кількість країн, які будуть відповідати еталонній чотириполюсній барицентричній моделі збалансованості розвитку держави, тому сформуємо правила, за якими можна інтерпретувати чотирикутники для різних країн:

1) координати чотирьох точок – вершин чотирикутника повинні бути в межах від 0 до1. Чим ближче значення до 1, тим вищий рівень розвитку забезпечує даний вимір. Чим ближче воно до 0, тим рівень розвитку виміру є нижчим;

2) навколо чотирикутника можна описати коло, якщо сума його протилежних кутів дорівнює 180^{o}. Маємо справу з опуклими чотирикутниками, хоча є окремі випадки чотирикутників, які самоперетинаються та навколо яких можна описати коло. У випадках, якщо коло не можливо описати, це говоритиме про існування певного дисбалансу між чотирма вимірами;

3) у випадку, якщо навколо чотирикутника можливо описати коло, то центр даного кола повинен бути якомога ближчим до центра мас. В цьому

випадку буде забезпечуватися баланс вимірів. Якщо центр кола, описаного навколо чотирикутника, співпадає з центром мас, то маємо справу із квадратом – еталонною моделлю стійкості розвитку країни;

4) центр мас барицентричної моделі повинен співпадати із центром мас еталонної моделі. У протилежному випадку необхідно визначити довжину відрізку, який буде показувати ступінь нестійкості розвитку країни.

Чотириполюсна барицентрична модель збалансованості розвитку країни будується наступним чином: на координатній площині відкладаються вершини чотирикутника, в якості яких виступають значення розрахованих композитних таргетів, отриманих на етапі 4. Вони з'єднуються відрізками. Далі визначаються кути чотирикутника з метою визначення, чи можна описати коло навколо нього. Для цього необхідно його розбити на два трикутника та визначити довжину сторін та діагоналей як довжину відрізків за формулою (4.39):

$$AB = \sqrt{(x_b - x_a)^2 + (y_b - y_a)^2}, \tag{4.39}$$

де AB – це довжина відрізку між двома точками A та B, які є вершинами чотирикутника – композитними таргетами чотирьох вимірів;

$(x_a; y_a)$ – координати точки A;

$(x_b; y_b)$ – координати точки B.

Далі знаходимо косинуси кутів для кожного з двох трикутників за формулою (4.40):

$$\cos\alpha = \frac{b^2 + c^2 - a^2}{2 \cdot b \cdot c}, \tag{4.40}$$

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

Використовуючи формулу (4.40) визначаються косинуси трьох кутів кожного з двох трикутників. Далі отримані значення переводяться у градусну міру, або за допомогою таблиць, або за допомогою спеціальних калькуляторів.

Далі сумуємо два кути, які знаходяться біля основ одного трикутника, із кутами іншого. Перевіряємо суму отриманих кутів чотирикутника, чи дорівнює вона 360 градусів. Потів робимо перевірку із протилежними кутами, чи дорівнює їх сума 180 градусів. У випадку із їх рівністю робимо висновок, що навколо даного чотирикутника можна описати коло, значення радіусу якого розраховується за формулою (4.41):

$$R = \frac{1}{4}\sqrt{\frac{(ab+cd)(ad+bc)(ac+bd)}{(p-a)(p-b)(p-c)(p-d)}}, \tag{4.41}$$

де a, b, c, d – довжина боків чотирикутника, визначена за формулою (4.39);

p – напівпериметр чотирикутника, який розраховується як:

$$p = \frac{a+b+c+d}{2}. \tag{4.42}$$

Далі необхідно визначити центр мас чотирикутника, тобто його координати, які розраховуються за формулами (4.43)–(4.44):

$$F_x = \frac{1}{6A}\sum_{i=0}^{n-1}((x_i + x_{i+1})(x_i y_{i+1} - x_{i+1} y_i)); \tag{4.43}$$

$$F_y = \frac{1}{6A}\sum_{i=0}^{n-1}((y_i + y_{i+1})(x_i y_{i+1} - x_{i+1} y_i)); \tag{4.44}$$

де F_x та F_y – координати центру мас чотирикутника;

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

A – площа чотирикутника, яка визначається за формулою (4.45):

$$\mathrm{A} = \frac{1}{2}\sum_{i=0}^{n-1}(x_i y_{i+1} - x_{i+1} y_i). \quad (4.45)$$

На *шостому етапі* визначаємо різницю між центром мас, визначеним для конкретної країни, та центром мас для ідеальної моделі. Її розраховуємо, як довжину відрізку за формулою (4.39). Проводимо аналіз отриманих даних, щодо виконання основних правил та щодо відхилень у стійкості розвитку.

Для застосування даної методики сформуємо масив вхідних даних, які представляють собою значення факторів, перелік яких наведено у таблиці 4.5. Цю інформацію було узято для 127 країн із наступних джерел [6, 56, 68, 74, 84, 89, 108, 111, 120, 197, 209, 241]. Оскільки дані відповідають країнам світу та повний набір інформації сформовано тільки за 2018 рік (за інші періоди більшість інформації є відсутньою, особливо в частині показників інформаційної безпеки), то для подальшої реалізації запропонованої методики обираємо варіант із просторовими даними.

Після цього проводимо нормалізацію даних за формулами (4.34)–(4.35). Результат представлено у таблиці К.1 в додатку К. Далі за формулою (4.36) розраховуємо композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки, результати чого наведено у таблицях К.2–К.5 додатку К. Візуалізуємо отримані дані для більш ефективного наочного сприйняття інформації та проведення аналізу. Використаємо підхід до класифікації країн за рівнем їх розвитку, згідно із яким вони поділяються на розвинені, ті, що розвиваються, та найменш розвинені. А також виділимо серед країн, що розвиваються, групу тих, які вважаються новими індустріальними, оскільки вони мають рівень економічного зростання набагато вищий, ніж інші. Сюди відносяться Аргентина, Бразилія, Мексика, Індія, Малайзія, Тайланд, Чилі, Індонезія, Туреччина, Китай, Іран, Філіппіни [186], та перспективні індустріальні країни з Групи одинадцяти (Нігерія, Єгипет, Пакистан, Бангладеш, В’єтнам) [190]. На практиці цей підхід є доволі умовним

поділом країн, який характеризує так би мовити їх загальний розвиток. Також вживають інші види розподілу, наприклад, по типу економік: країни із доіндустріальною, індустріальною, постіндустріальною, інноваційною економікою, із змішаними укладами [373, с. 11]. Не залежно від виду класифікації більшість країн відносяться до одних й тих груп розвитку.

На рисунку 4.11 представлені композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки, для розвинутих країн або країн із високим рівнем економіки, перелік яких було означено у відповідністю із Міжнародним валютним фондом [258, с. 132].

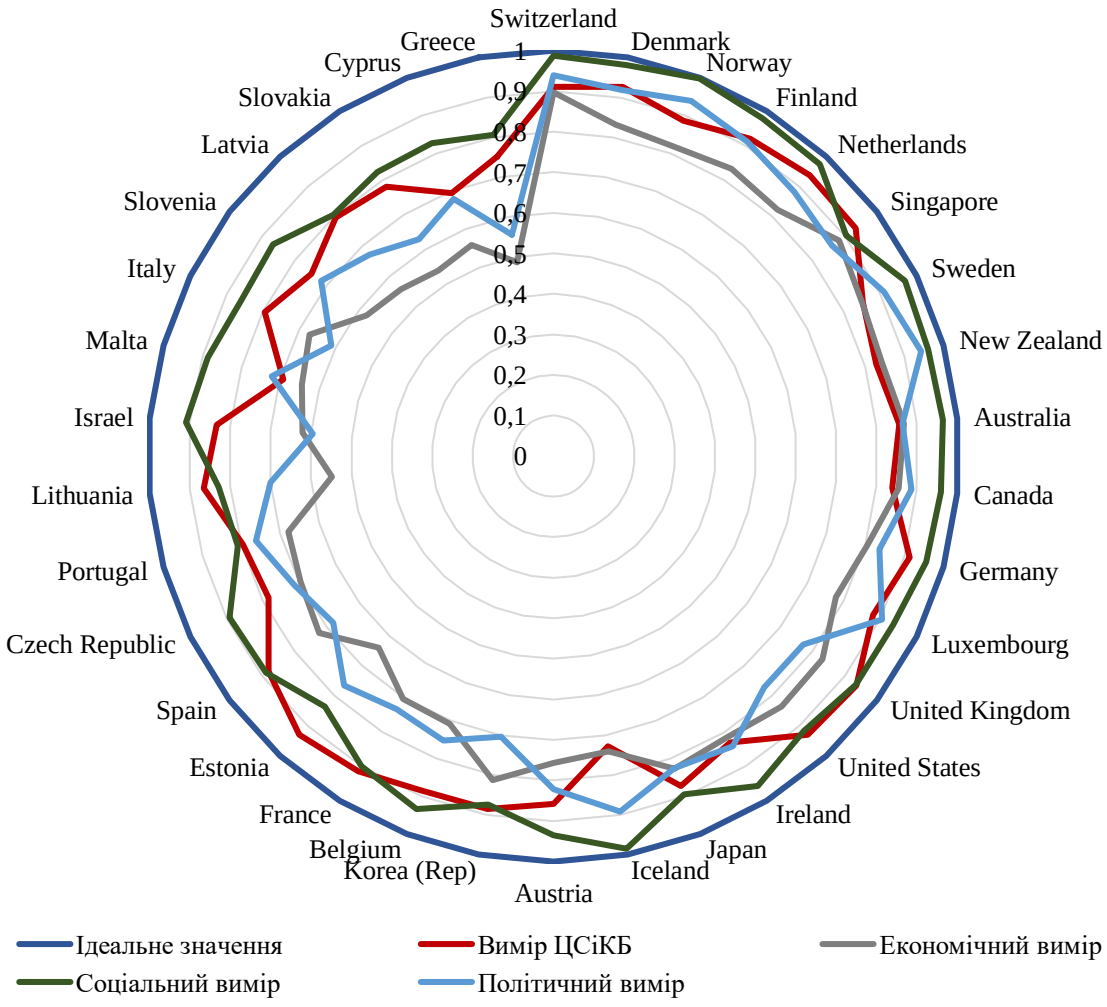


Рисунок 4.11 – Композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки (ЦСіКБ) для розвинутих країн (складено авторкою)

На рисунку 4.11 можна побачити, що значення таргетів кожної країни відхиляються від ідеального значення. Але на практиці досягнення такого рівня є складною задачею, тому чим ближче розраховані значення прямують до нього, тим вищий рівень розвитку країни у даному вимірі. Можна відмітити, що найкращий результат демонструє Швейцарія, яка має найвище сумарне значення таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки, яке складає 3,735. Такі країни, як Данія, Фінляндія, Норвегія, Нідерланди, Сінгапур, Швеція, Нова Зеландія, Австралія, Канада, Німеччина, Люксембург, Великобританія, США, Ірландія, Японія та Австрія, отримали також найвищі оцінки, що свідчить про досить високий рівень розвитку кожного із визначених таргетів. Найнижчі показники демонструє Греція. Можна відмітити, що найвищий рівень розвитку належить соціальному виміру. Для більшості країн рівень розвитку виміру цифрової спроможності і кібербезпеки займає друге місце. Дещо відстає економічний вимір.

Можна зробити висновок, що практично для більшості розвинених країн характерний високий рівень розвитку таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності, але рівень економіки має нижчі тенденції розвитку у порівнянні із іншими, щоб забезпечити повну їх збалансованість.

На рисунку 4.12 представлені композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для країн, що розвиваються, перелік яких було визначено МВФ [258, с. 134-135].

У порівнянні із таргетами, отриманими для розвинутих країн, у даному випадку спостерігається значний дисбаланс, що виникає між соціо-інформаційним рівнями та економіко-політичним. При чому різниці є досить суттєвими. Наприклад, для Казахстану таргет соціального виміру дорівнює 0,7112, цифрової спроможності і кібербезпеки – 0,7053, економічний – 0,5659, політичний – 0,3108; для Алжиру – відповідно 0,6542, 0,3486, 0,1365, 0,3002.

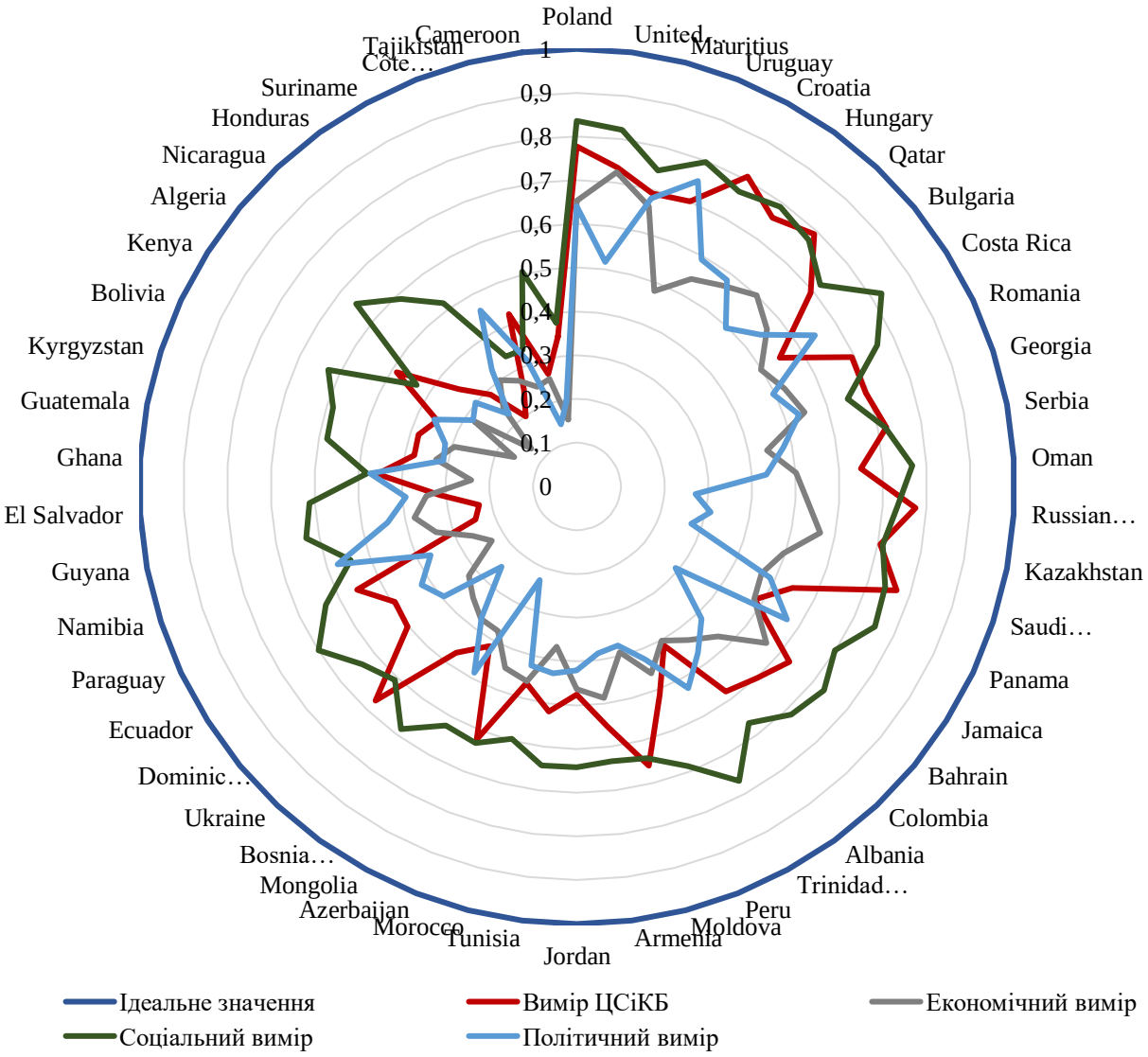


Рисунок 4.12 – Композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки (ЦСіКБ) для країн, що розвиваються (складено авторкою)

Найгірші результати було отримано для Камеруну: таргет соціального виміру – 0,3770, цифрової спроможності і кібербезпеки – 0,3461, економічний – 0,1549, політичний – 0,1961. Тобто для країн, що розвиваються, є важливим, в першу чергу, посилення політичного виміру шляхом трансформації законодавства, прийняття урядом більш ефективних рішень, спрямованих на розвиток економіки, проведення економічних реформ.

Що стосується композитних таргетів для окремої групи країн, що розвиваються, а саме нових індустріальних, то отримані їх значення представлені на рисунку 4.13.

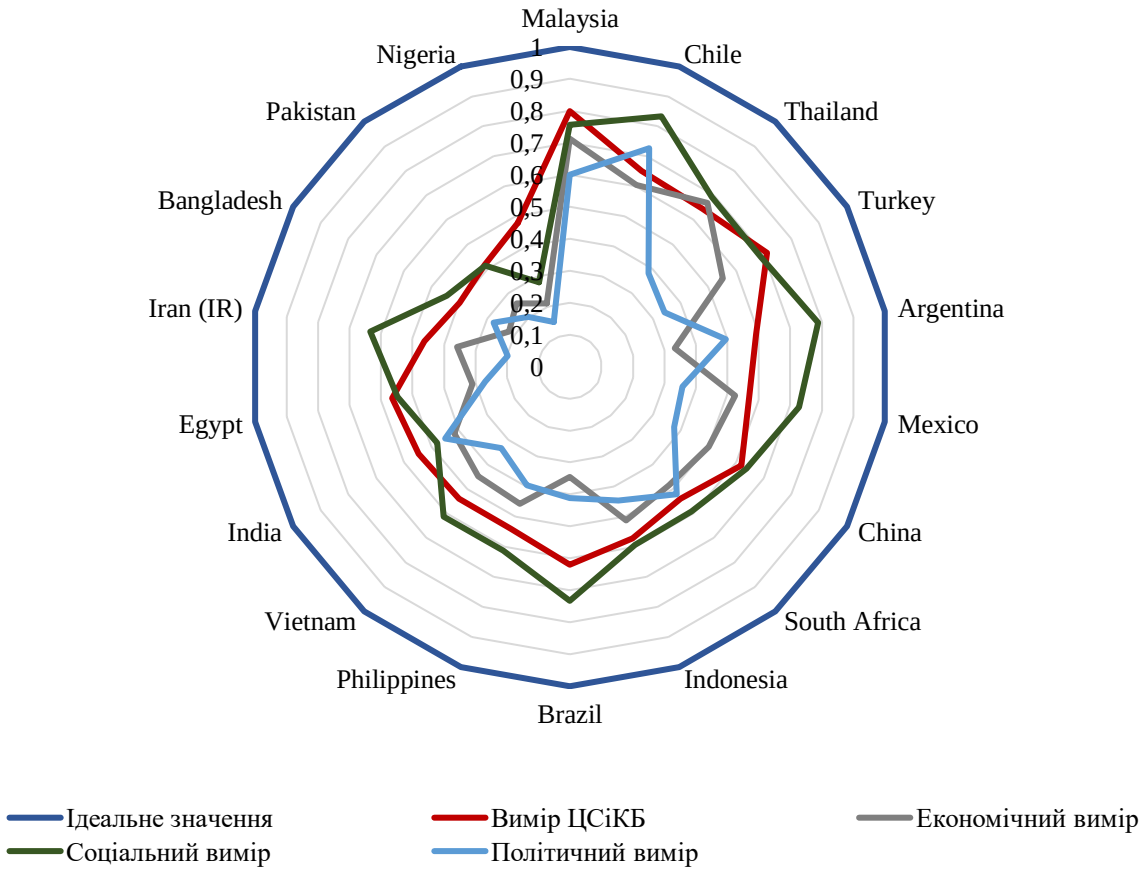


Рисунок 4.13 – Композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки (ЦСіКБ) для нових індустріальних країн (складено авторкою)

На рисунку 4.13 чітко видно, що присутній дисбаланс у розвитку країн, при цьому явно спостерігається однаковий напрям розвитку у соціально-цифровому вимірі та економіко-політичному. Хоча на відмінність від даних рисунку 4.12 можна відмітити той факт, що для даних країн характерний більш рівномірний розвиток, який не містить аномальних перепадів. Найвищі показники мають Малайзія, Чилі, Тайланд, Туреччина та Аргентина, найгірший результат характерний для Нігерії. Оскільки представлені країни вважаються такими, що пройшли певні етапи соціо-економічного розвитку та досягли успіхів, або мають всі шанси на індустріальний стрибок, то можна сказати, що для більшості із них,

а саме Туреччині, Тайланду, Аргентині, Нігерії, Пакістану, Чилі, Бразилії, Бангладешу, Мексиці та Ірану, слід звернути увагу на розвиток політичного та економічного вимірів для забезпечення розвитку соціо-цифрової сфер.

На рисунку 4.14 представлені побудовані композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки для найменш розвинутих країн, перелік яких визначено Організацією Об'єднаних Націй (далі ООН) [165, с. 1].

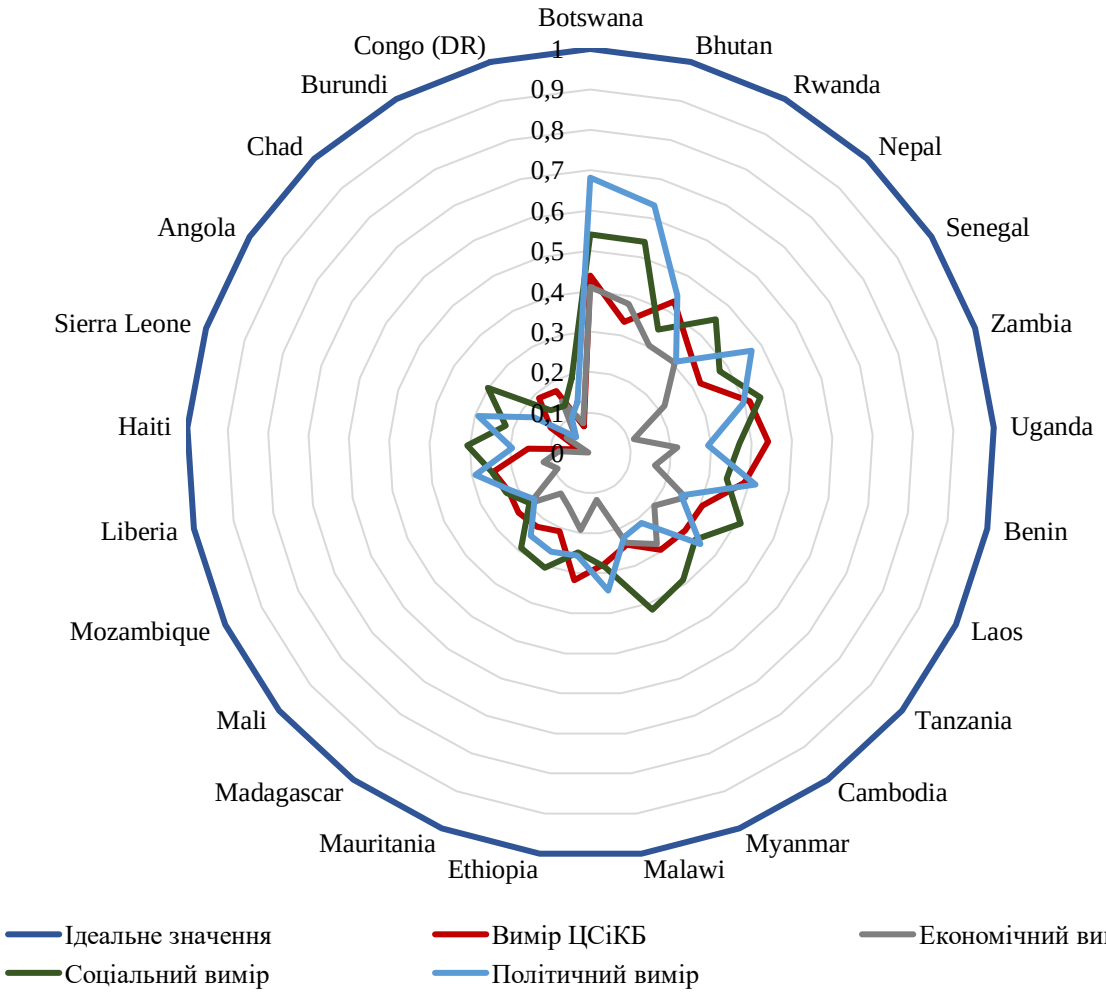


Рисунок 4.14 – Композитні таргети економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки (ЦСіКБ) для найменш розвинутих країн (складено авторкою)

Можна відмітити, що практично усі країни, окрім Ботсвани та Бутану, мають дуже низькі значення чотирьох таргетів (рисунок 4.14). При цьому можна

побачити значну розбалансованість усіх вимірів, особливо економічного. Отримані результати свідчать про існування реальних проблем, пов'язаних із економічним, соціальним, політичним та інформаційним розвитком даних країн, а також про необхідність у допомозі з боку міжнародних організацій.

Перед побудовою барицентричної моделі необхідно визначити суми протилежних кутів та перевірити, чи дорівнюють вони 180 градусів. Застосовуючи формулу (2.25), проведемо розрахунки. Візуалізуємо отриману інформацію для спрощення аналізу. Так, на рисунку 4.15 можна побачити співвідношення сум протилежних кутів чотирикутника, які дозволять зробити про збалансованість розвитку чотирьох вимірів – соціо-політичного та економіко-інформаційного (для скорочення назви виміру цифрової спроможності та кібербезпеки застосовуємо «інформаційний»).

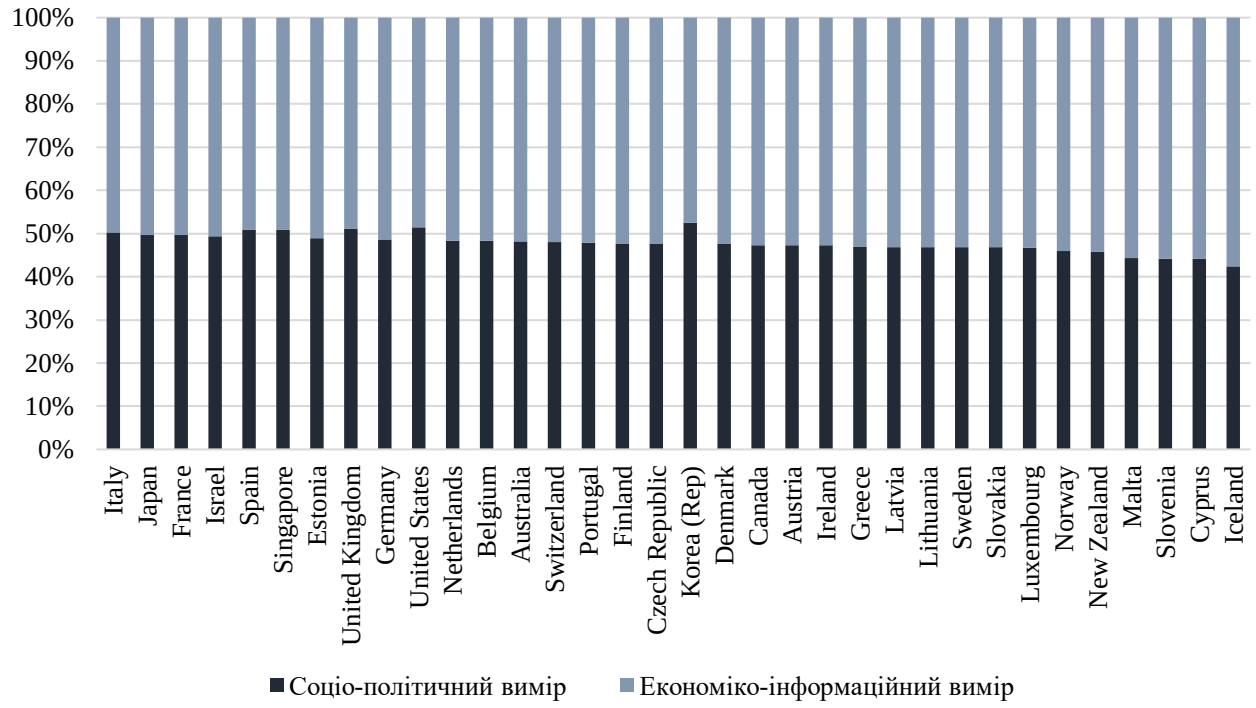


Рисунок 4.15 – Збалансованість пар соціально-політичного та економіко-інформаційного вимірів на основі суми протилежних кутів для розвинутих країн (складено авторкою)

Аналізуючи дані рисунку 4.15, можна зробити висновок про те, що для моделі жодної з країн не можливо накреслити коло навколо чотирикутника,

оскільки суми протилежних кутів не дорівнюють 180 градусів. Тільки одна країна (Італія) має значення цього показника приблизно рівним 180 градусів. Для Японії, Франції, Ізраїлю, Іспанії, Сінгапуру, Естонії, Великобританії, Німеччини та США сума кутів незначно відхиляється від необхідного значення. Для всіх інших розбіжність зростає. Можна зробити висновок, що для країн із меншим відхиленням значень сум протилежних кутів від 180 градусів є характерним ситуація, коли існуючі співвідношення чотирьох вимірів є сприятливим для забезпечення подальшого розвитку країни. В протилежному випадку, спостерігатиметься дисбаланс у розвитку окремих сфер.

Побудуємо чотириполюсну барицентричну модель збалансованості розвитку Італії, результат якої представлений на рисунку 4.16.

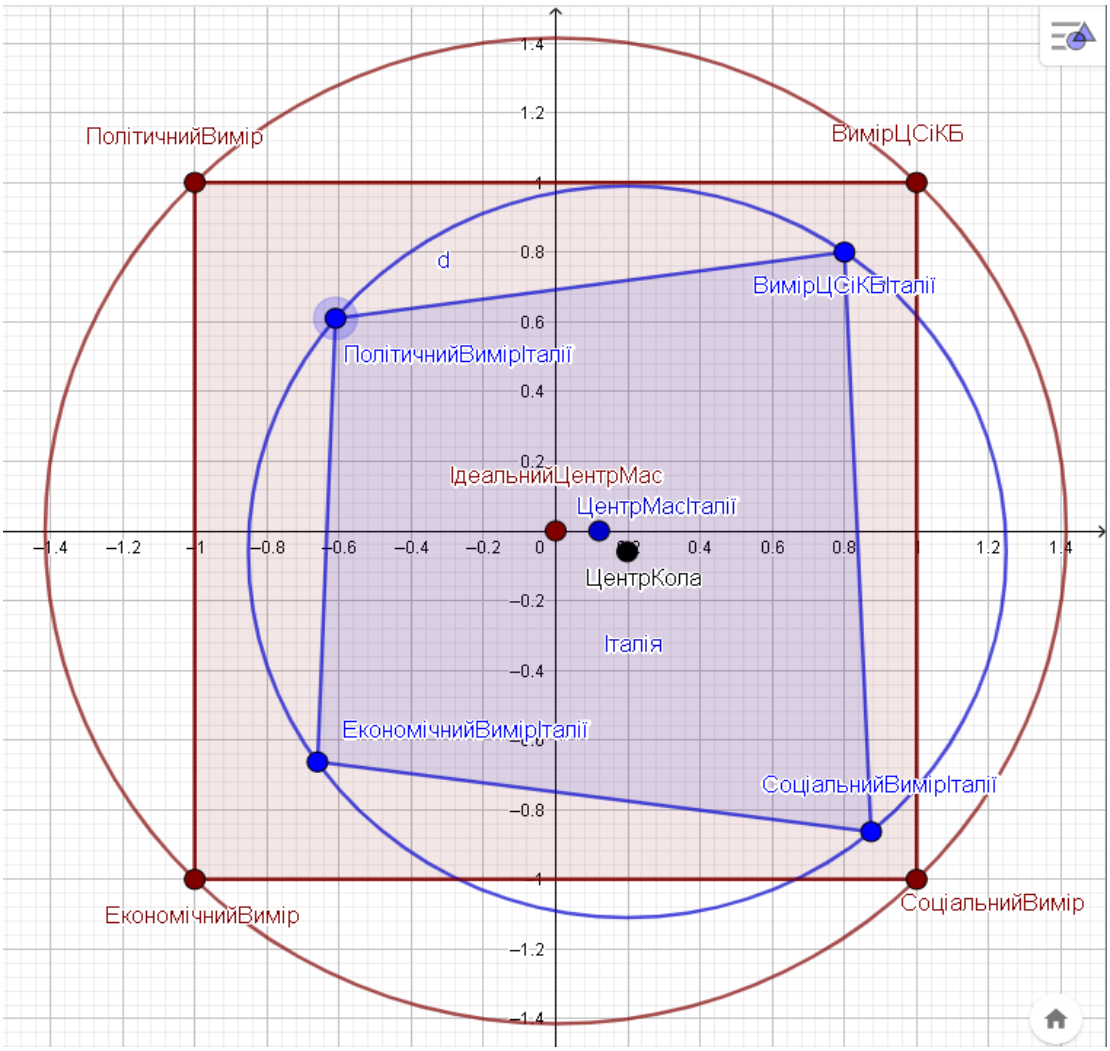


Рисунок 4.16 – Чотириполюсна барицентрична модель збалансованості розвитку Італії (складено авторкою)

Барицентрична модель (рисунок 4.16) показує стійкість розвитку Італії з урахуванням збалансованості чотирьох вимірів – економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки. На рисунку 4.16 відмічено центр мас чотирикутника, розрахунки координат якого наведено у таблиці К.6 додатку К, де також представлено результати для усіх країн. Також позначено відрізок, який є відстанню між значенням ідеального центру мас та центру мас Італії. Значення відстаней для усіх країн наведені у К.6 додатку К. За даною моделлю можна зробити наступний висновок: розвиток країни є не досить стійким, оскільки є відстань між центрами мас, але його значення не є критичним, то можна сказати, що розвиток відбувається, але він має певні коливання. Співвідношення між парами вимірів (економіко-цифровим та соціо-політичним) є збалансованим, що дозволяє компенсувати недоліки розвитку однієї сфери за рахунок іншої. Таргети політичного та економічного вимірів є слабкішими, тому країні треба змістити акцент у даний напрямок розвитку. При чому драйвером розвитку політичного напрямку може виступити соціальний, а для економічного – сфера інформаційної безпеки.

Результати розрахунків сум протилежних кутів для побудови барицентричної моделі країн, що розвиваються, представлені на рисунку 4.17. Тільки дві країни мають відповідні значення – це Ко-д'Івуар та Болгарія. Всі інші мають суму протилежних кутів, що не дорівнює 180 градусів, що говорить про не можливість описати коло навколо чотирикутника-моделі. Оман, Румунія, Хорватія та Колумбія мають близькі значення кутів до 180 градусів, для інших країн відхилення тільки зростають. Отримані результати свідчать про превалювання окремих пар таргетів над іншими, що потрібно враховувати при побудові програм розвитку країн. Для України однаково нерівномірними є обидві пари таргетів.

Побудуємо чотириполюсну барицентричну модель збалансованості розвитку України, результат якої представлений на рисунку 4.18. Отримана модель дозволяє зробити наступні висновки: розвиток країни є не стійким, оскільки відстань між центрами мас дорівнює 0,2216, що практично наближає його до максимального значення серед відстаней.

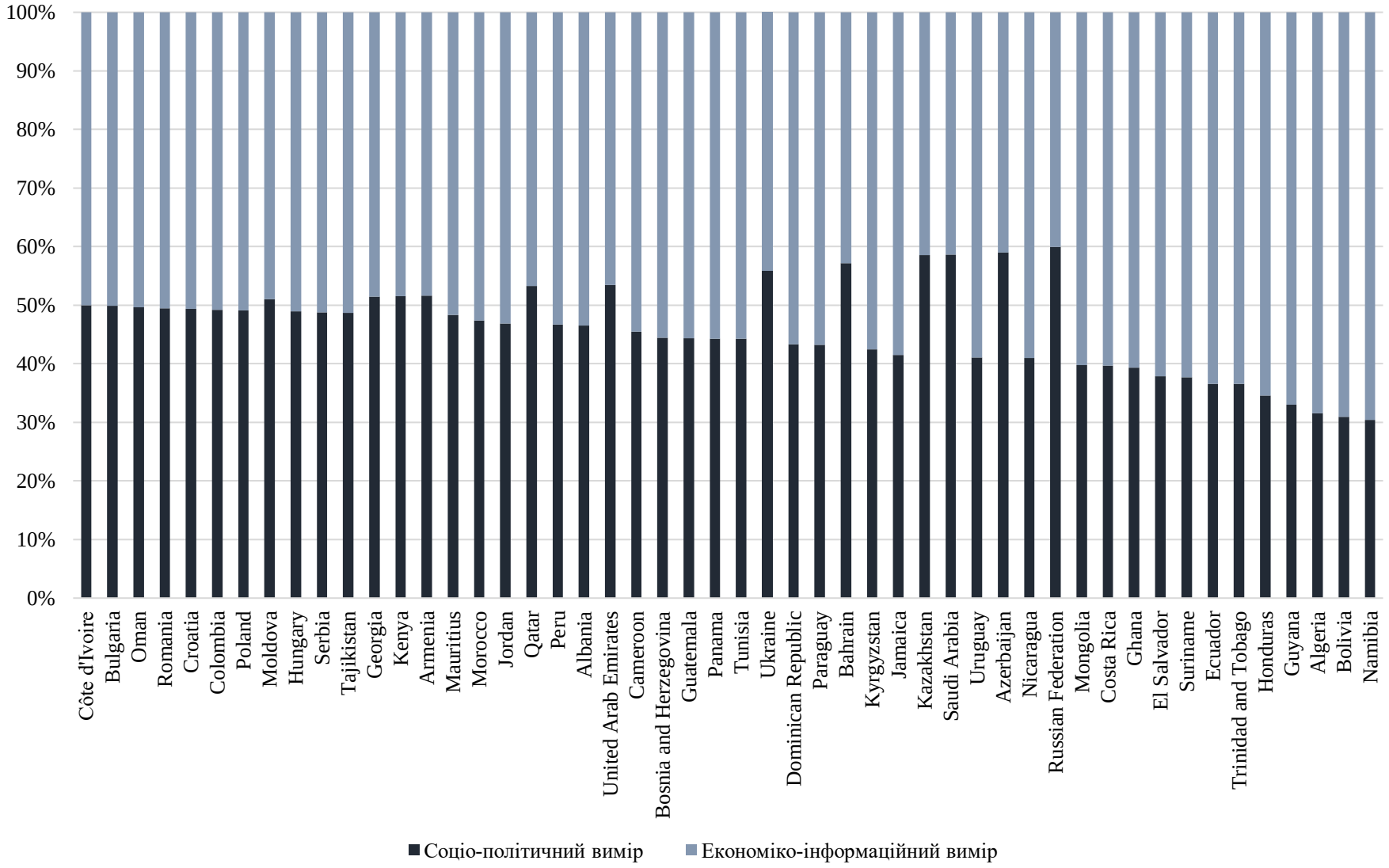


Рисунок 4.17 – Збалансованість пар соціально-політичного та економіко-інормаційного вимірів на основі суми протилежних кутів для країн, що розвиваються (складено авторкою)

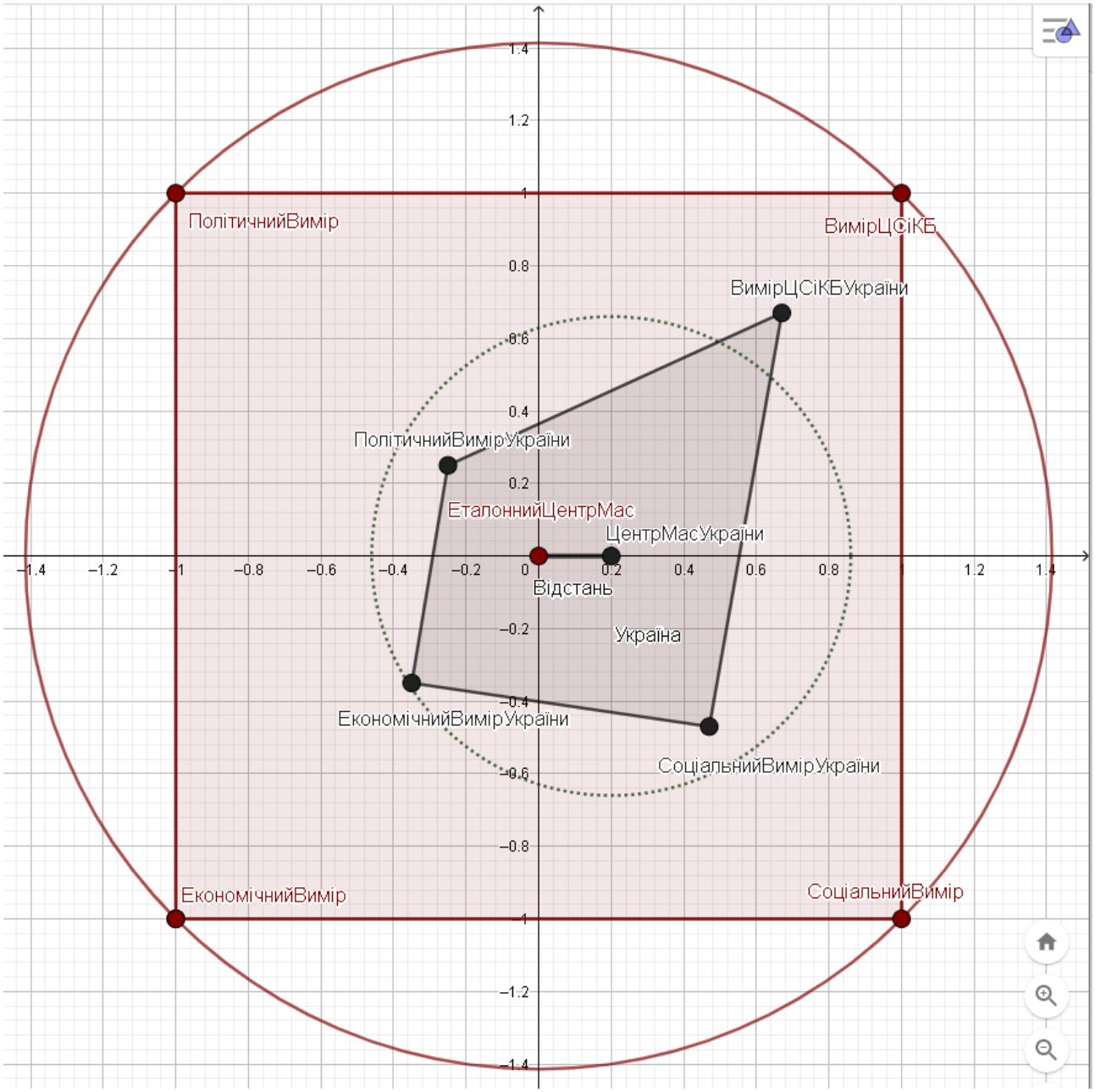


Рисунок 4.18 – Чотириполюсна барицентрична модель збалансованості розвитку України (складено авторкою)

Співвідношення між парами вимірів (економіко-інформаційним та соціо-політичним) не є збалансованим, оскільки суми протилежних кутів не дорівнюють 180 градусів, причому дисбаланс є найбільшим для соціального та політичного вимірів. Найбільш ефективним є таргет цифрової спроможності і кібербезпеки, що говорить про посилення її заходів в останні роки та формування нових інститутів. Але за умови слабких економічного, політичного та соціального вимірів, розвиток тільки цифрової складової не сприятиме

повноцінному розвитку національної економіки країни в цілому. Тому у першу чергу слід звернути увагу на вирішення проблем економічного, соціального та політичного характеру.

Значення сум протилежних кутів для нових індустріальних країн представлено у вигляді гістограми на рисунку 4.19.

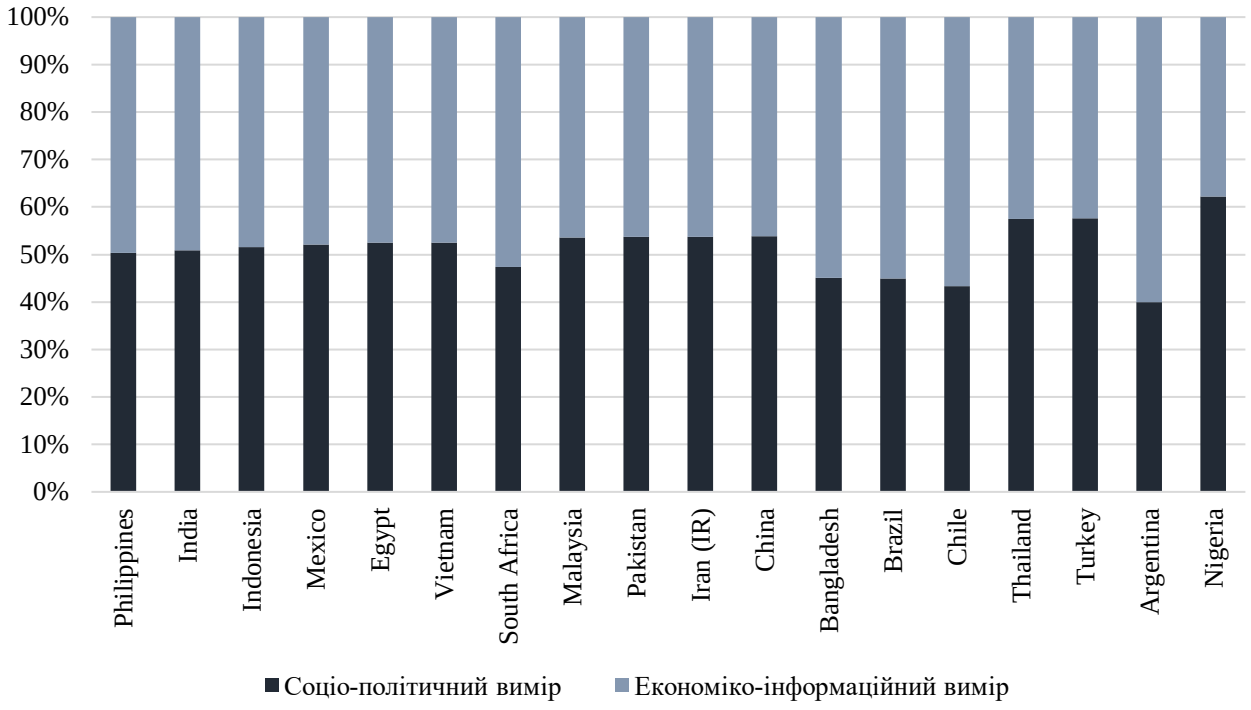


Рисунок 4.19 – Збалансованість пар соціально-політичного та економіко-інформаційного вимірів на основі суми протилежних кутів для нових індустріальних країн (складено авторкою)

З рисунку 4.19 видно, що тільки модель Філіппін має значення сум протилежних кутів чотирикутника, які приблизно дорівнюють 180 градусів. Інші країни мають незбалансовані пари вимірів, причому для одних є характерним превалювання збалансованості економіко-інформаційного виміру (Індія, Індонезія, Мексика, Єгипет, В’єтнам, Малайзія, Пакистан, Іран, Китай, Тайланд, Туреччина, Нігерія), для інших – соціально-політичного (Південна Африка, Аргентина, Бангладеш, Бразилія, Чилі).

Побудуємо чотириполюсну барицентричну модель збалансованості

розвитку однієї із нових індустріальних країн, а саме Китаю, результат якої представлений на рисунку 4.20.

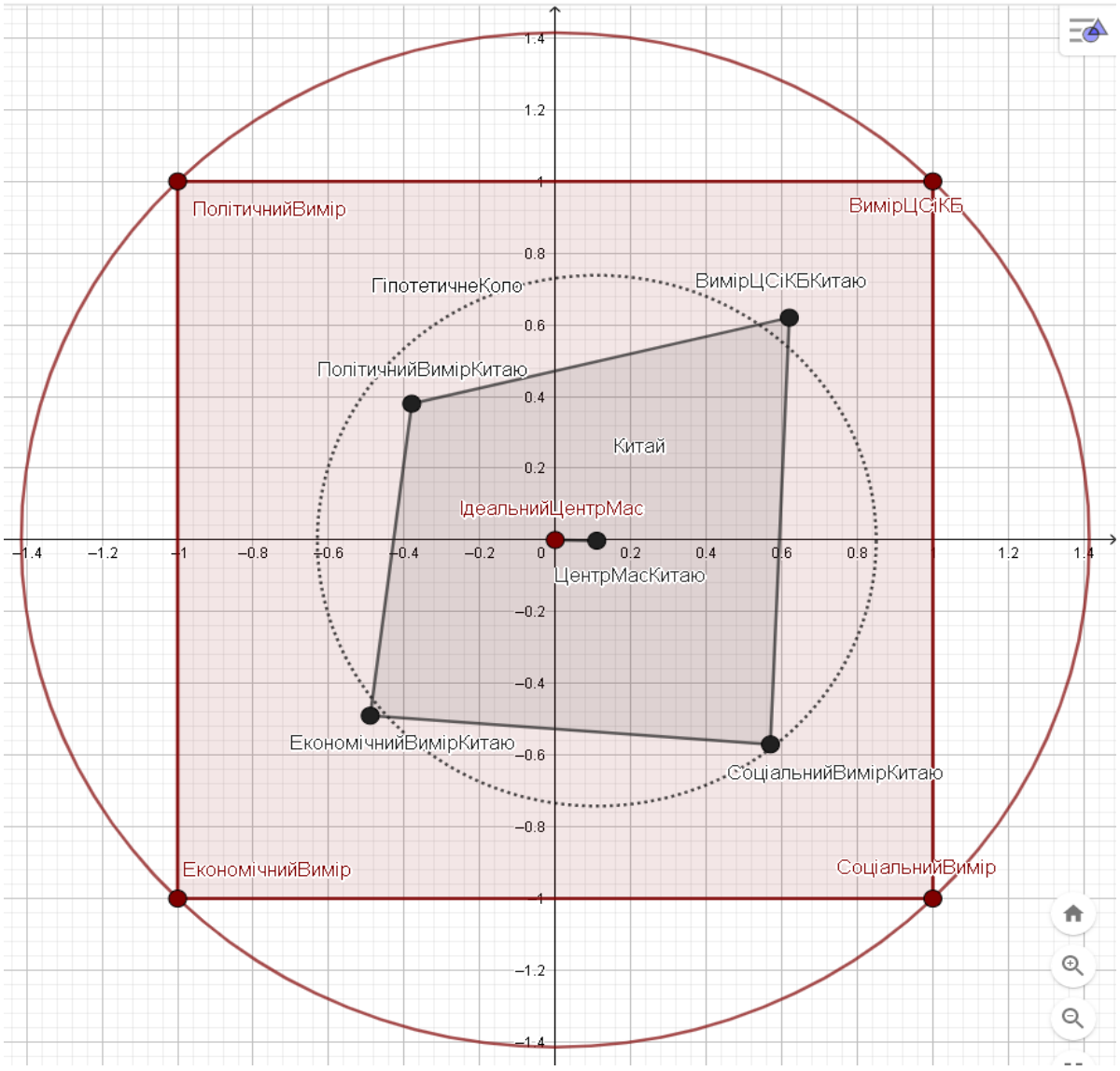


Рисунок 4.20 – Чотириполюсна барицентрична модель збалансованості розвитку Китаю (складено авторкою)

За результатами моделі (рисунок 4.20) можна зробити наступні висновки: розвиток країни є досить не стійким, оскільки відстань між центрами мас дорівнює 0,1226, але його значення наближене до середнього серед інших країн. Тобто розвиток відбувається, але він є нестабільним. Співвідношення між парами вимірів (економіко-інформаційним та соціально-політичним) – незбалансоване, оскільки суми протилежних кутів не дорівнюють 180 градусів,

причому дисбаланс є найбільшим для соціального та політичного вимірів, ніж для економіко-інформаційного. Таргети інформаційної безпеки та економічний є ефективними, що говорить про існування потужного економічного та інформаційного потенціалів. Сьогодні Китай є країною, розвиток якої спрямований саме у ці сфери, але він має певні проблеми соціального та політичного характеру, що є також наслідком існування політичного режиму, наслідком чого відбувається зниження якості соціальних стандартів.

Розраховані значення сум протилежних кутів для найменш розвинених країн представлено на рисунку 4.21.

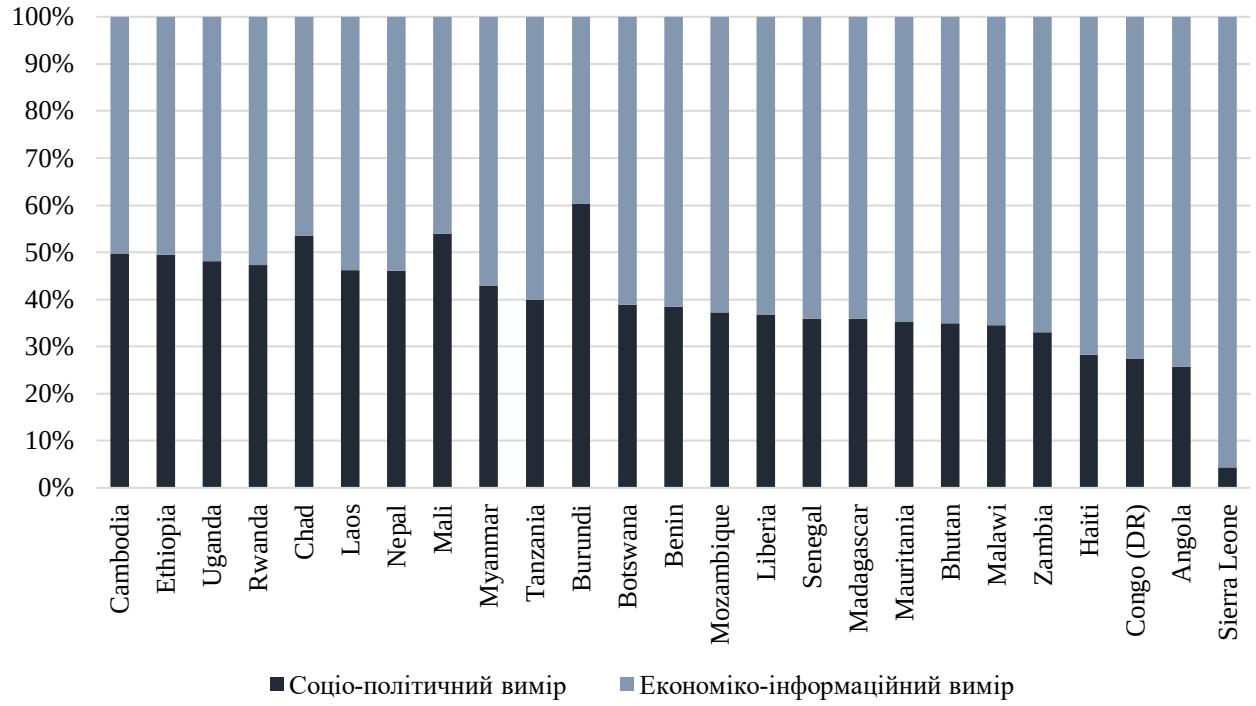


Рисунок 4.21 – Збалансованість пар соціально-політичного та економіко-цифрового вимірів на основі суми протилежних кутів для найменш розвинутих країн (складено авторкою)

На рисунку 4.21 можна побачити, що тільки для Камбоджі значення сум протилежних кутів чотирикутника дорівнюють 180 градусів, а для Ефіопії ці значення є близькими. Інші країни мають ярко виражену незбалансованість пар вимірів, причому для переважної більшості із них є характерним превалювання

соціально-політичного виміру та незбалансованість економіко-інформаційного. Для Чаду, Малі та Бурунді ситуація є зворотною.

Побудуємо чотириполюсну барицентричну модель збалансованості розвитку Камбоджі, оскільки вона має найбільш збалансовану пару вимірів. Результат представлений на рисунку 4.22.

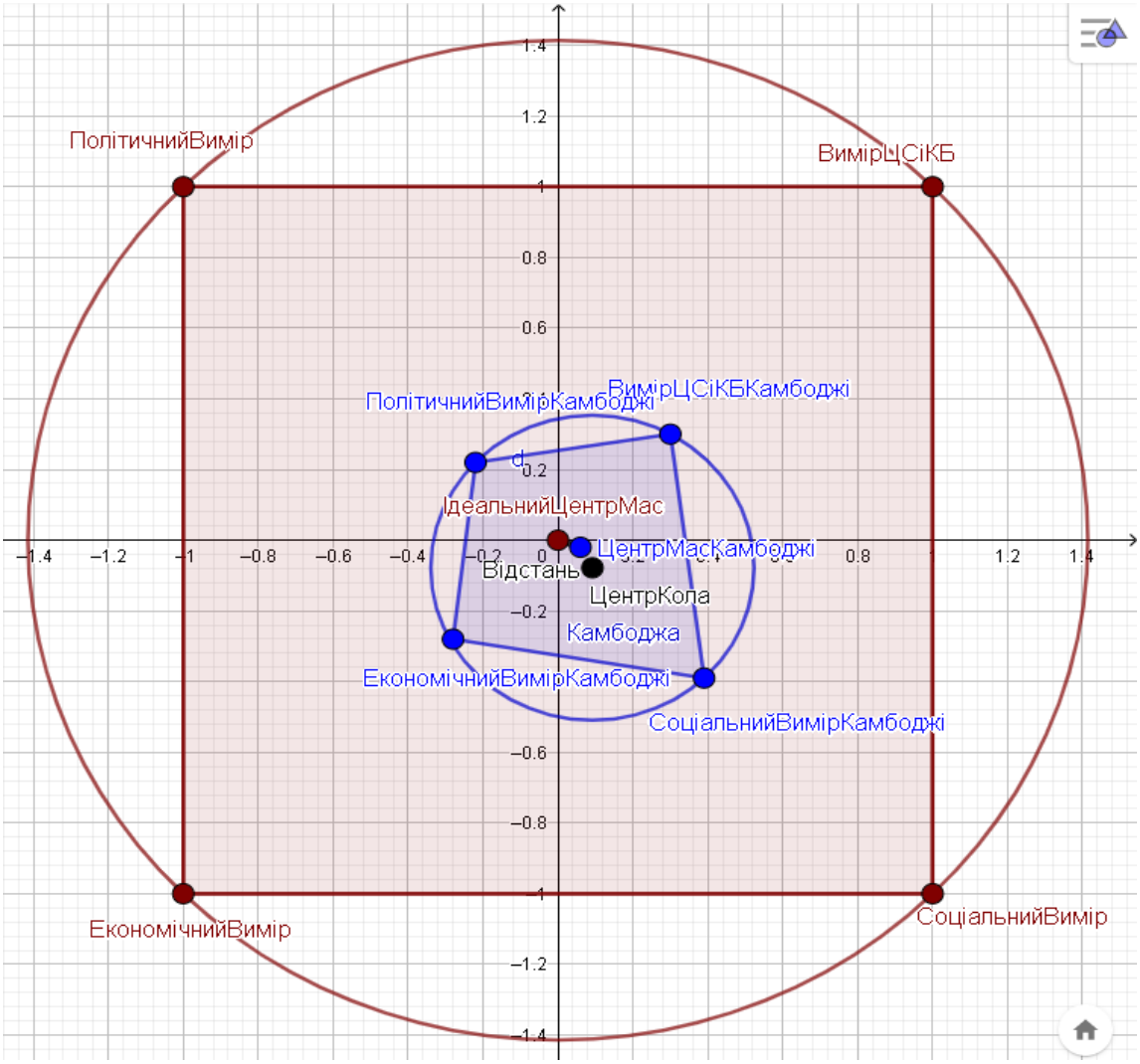


Рисунок 4.22 – Чотириполюсна барицентрична модель збалансованості розвитку Камбоджі (складено авторкою)

За результатами моделі (рисунок 4.22) можна зробити наступні висновки: розвиток країни є не стійким, оскільки відстань між центрами мас дорівнює 0,0603, але його значення наближається до 0 в більшій мірі, що говорить про правильність напрямів розвитку Камбоджі. Хоча є певна нестабільність, але вона

викликається за рахунок зростання таргетів соціального виміру, що є наслідком формування за останні 25 років демократичного уряду, який долає результати існування досить тривалого часу терористичних режимів. Співвідношення між парами вимірів (економіко-цифровим та соціально-політичним) – збалансоване, оскільки суми протилежних кутів дорівнюють 180 градусів. Значення таргетів є невеликими (0,2957 – для виміру цифрової спроможності та кібербезпеки; 0,2788 – для економічного; 0,3891 – для соціального; 0,2150 – для політичного), що говорить про доволі низькі рівні розвитку даних сфер. Але оскільки розвиток наближається до стійкого та існує збалансованість між парами вимірів, то можна сказати, що Камбоджі має всі можливості для забезпечення інтенсивного та динамічного подальшого розвитку за умови підтримки таких тенденцій.

На рисунку 4.23 представлено розраховане значення відстаней між центрами мас для всіх країн, тобто відхилень фактичних значень їх центрів мас від ідеального значення, що показує рівень збалансованості їх розвитку.

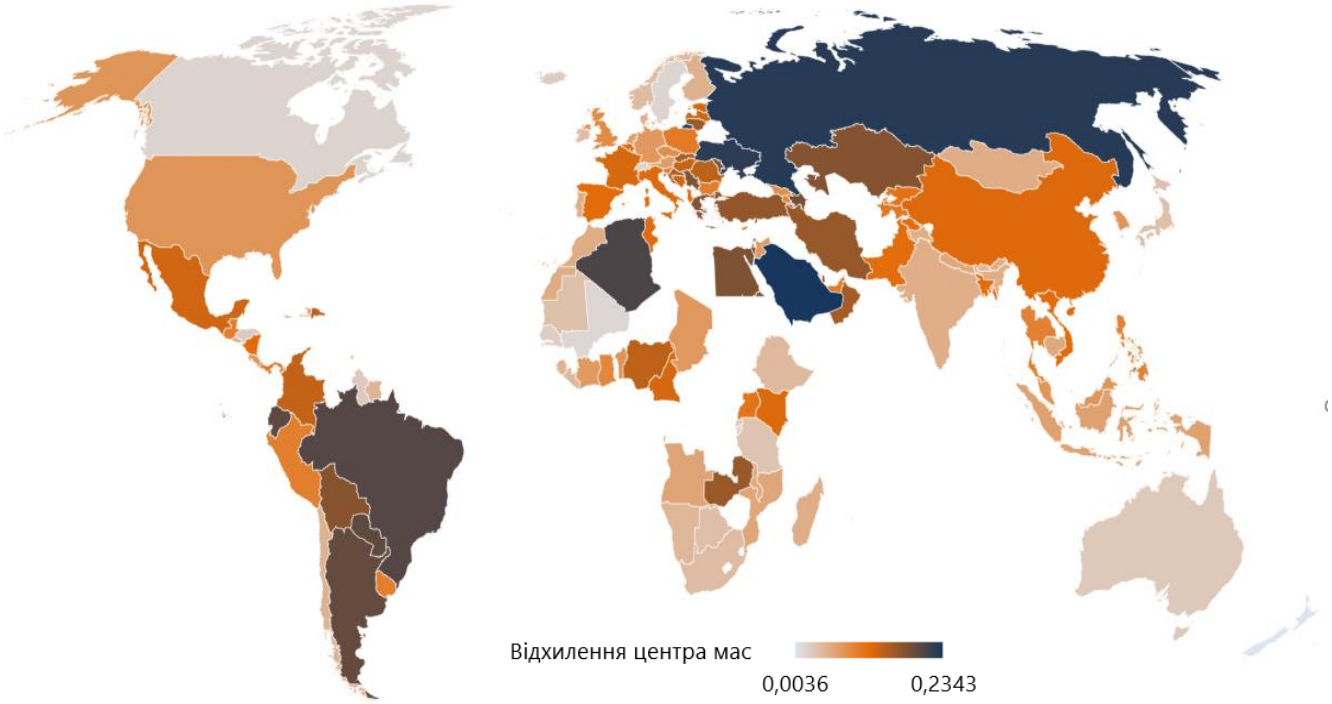


Рисунок 4.23 – Рівень збалансованості розвитку країн на основі відхилення центрів мас їх барицентричних моделей (складено авторкою)

Так, найбільш збалансованими є Нова Зеландія (0,0036), Малі (0,0185), Швеція (0,0201), Канада (0,0203), Швейцарія (0,0206), Бурунді (0,0216), Сенегал (0,0260), Ісландія (0,0273), Руанда (0,0295), Гондурас (0,0298), Гаяна (0,0299). Тобто, найбільш збалансованим є країни, як розвинуті, так й ті, що розвиваються, та найменш розвинені. Даний фактор свідчить про те, що не залежно від значень таргетів, країна має їх ефективне поєднання, що може виступати драйвером та сприяти в подальшому їх більш стрімкому та динамічному розвитку. Найменш збалансованими виявилися Демократична республіка Конго (1,2355), Саудівська Аравія (0,2343), Російська Федерація (0,2252), Україна (0,2216), Алжир (0,2047), Бразилія (0,1993), Еквадор (0,1943), Парагвай (0,1935), Аргентина (0,1904), Азербайджан (0,1812). Це говорить про те, що дані країни мають дисбаланс за рахунок превалювання переважно одного (як в Україні) або двох таргетів над іншими, що свідчить про несистемність розвитку всіх сфер та необхідність трансформації їх стратегій розвитку.

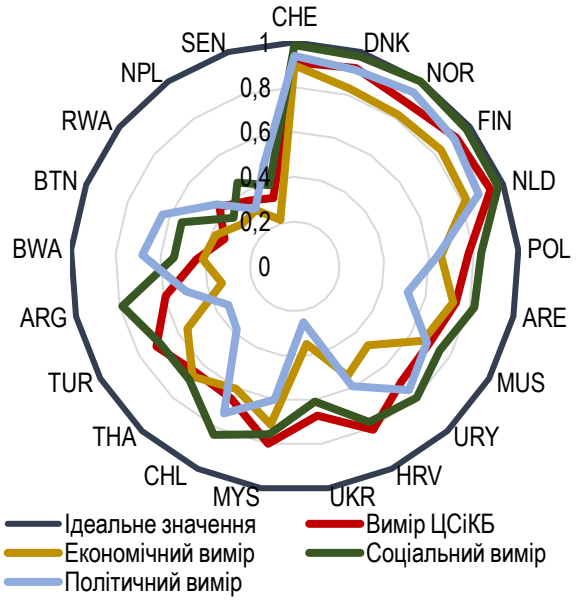
Отримані висновки показали, що є країни, для яких є характерний стійкий розвиток та збалансованість пар вимірів, причому це виявилися як розвинуті країни, так й ті, що розвиваються, та найменш розвинуті. Але рівень розвитку та збалансованості таргетів відповідає їх класифікаційній групі. Також виявилося, що 28 країн мають найбільш ефективним таргетом – інформаційну безпеку. Це розвинуті країни: Естонія, Франція, Республіка Корея, Литва, Норвегія, Сінгапур, Великобританія, США; країни, що розвиваються – Кот-д'Івуар, Хорватія, Грузія, Кенія, Молдова, Катар, Російська Федерація, Саудівська Аравія, Сербія, Україна; нові індустріальні – Єгипет, Індія, Малайзія, Пакистан, Туреччина; найменш розвинені – Бурунді, Чад, Ефіопія, Малі та Уганда. Оскільки є зв'язки між економічним виміром та інформаційним, то для країн із нестійким розвитком та незбалансованістю таргетів можна посилювати інформаційний напрям для трансформації економічних процесів у напрямок ї цифровізації.

Узагальнення запропонованої у підрозділі методології наведено на рисунку 4.24.

Етап 1. Вибір показників-факторів, що формують композитні індикатори вимірів: *економічного* – індекс економічної свободи, індекс нерівномірного економічного розвитку, індекс фінансового розвитку, індекс легкості ведення бізнесу, індекс глобальної конкурентоспроможності; *політичного* – індекс політичної стабільності, індекс демократії, індекс ефективності уряду, індекс сприйняття корупції; *соціального* – індекс щастя, індекс соціального прогресу, індекс людського розвитку; *цифрової спроможності НЕ та кібербезпеки (ЦСіКБ)* – індекс розвитку інформаційних та комунікаційних технологій, індекс мережевої готовності, глобальний індекс кібербезпеки, національний індекс кібербезпеки, рівень цифрового розвитку.

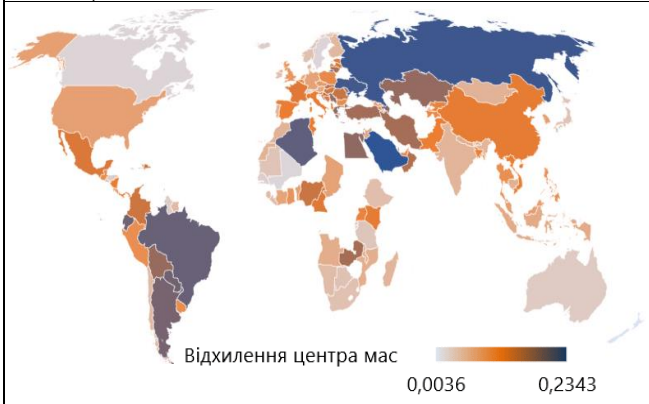
Етап 2. Нормалізація значень факторів за допомогою лінійної нормалізації

Етап 3. Розрахунок композитних індикаторів для кожного виміру: $G_{kl}(\widetilde{x_1}, \widetilde{x_2}, \dots, \widetilde{x_n}) = (\prod_{i=1}^{n} \widetilde{x_{ikl}})^{1/n}$, де $G_{kl}(\widetilde{x_1}, \widetilde{x_2}, \dots, \widetilde{x_n})$ – середньогеометричне значення нормалізованих вхідних значень факторів для *k*-го спостереження для *l*-го композитного індикатора; *n* – кількість факторів у кожному з вимірів. Значення будуть координатами точок



а) композитні індикатори економічного, соціального, політичного вимірів та виміру ЦСіКБ (фрагмент)

Розвинені країни (CHE – Швейцарія, DNK – Данія, NOR – Норвегія, FIN – Фінляндія, NLD – Нідерланди), країни, що розвиваються (POL – Польща, ARE – ОАЕ, MUS – Маврикій, URY – Уругвай, HRV – Хорватія, UKR – Україна), нові індустріальні (MYS – Малайзія, CHL – Чилі, THA – Таїланд, TUR – Туреччина, ARG – Аргентина), найменш розвинені (BWA – Ботсвана, BTN – Бутан, RWA – Руанда, NPL – Непал, SEN – Сенегал)



б) рівень збалансованості розвитку країн на основі відхилення центрів мас

Етап 4. Побудова чотириполюсної барицентричної моделі стійкості розвитку країни:

1) координати центра мас: $F_x = 1/6A \sum_{i=0}^{n-1}((x_i + +x_{i+1})(x_i y_{i+1} - x_{i+1} y_i))$; $F_y = 1/6A \sum_{i=0}^{n-1}((y_i + +y_{i+1})(x_i y_{i+1} - x_{i+1} y_i))$; де F_x та F_y – координати центра мас чотирикутника; $(x_i; y_i)$, $(x_{i+1}; y_{i+1})$ – координати вершин чотирикутника, де вершина з координатами $(x_n; y_n)$ буде збігатися з вершиною $(x_0; y_0)$; A – площа чотирикутника: $A = 1/2 \sum_{i=0}^{n-1}(x_i y_{i+1} - x_{i+1} y_i)$; 2) відхилення центра мас від еталонного значення як довжини відрізка: $AB = \sqrt{(x_b - x_a)^2 + (y_b - y_a)^2}$, де $(x_a; y_a)$ – координати точки A; $(x_b; y_b)$ – координати точки B; 3) косинуси кутів трикутників, на які розбивається чотирикутник: $\cos\alpha = (b^2 + c^2 - a^2)/(2 \cdot b \cdot c)$, де *a, b, c* – значення довжин трьох сторін трикутника, що визначаються як довжина відрізків; 4) радіус описаного кола: $R = \frac{1}{4}\sqrt{\frac{(ab+cd)(ad+bc)(ac+bd)}{(p-a)(p-b)(p-c)(p-d)}}$, де *a, b, c, d* – довжини сторін чотирикутника; *p* – напівпериметр чотирикутника: $p = (a + b + c + d)/2$

в) чотириполюсна барицентрична модель збалансованості розвитку України

Рисунок 4.24 – Методологія та результати оцінювання рівня збалансованості національної економіки на основі чотириполюсної барицентричної моделі (складено авторкою)

Таким чином, запропонований науково-методичний підхід дозволяє будувати чотириполюсну барицентричну модель збалансованості розвитку країни на основі інтеграції композитних таргетів економічного, соціального, політичного вимірів та виміру цифрової спроможності і кібербезпеки. Результати моделювання сприяють виявленню рівня збалансованості розвитку країни в цілому, пар соціально-політичного та економіко-цифрового вимірів, а також визначенню таргетів, які є найбільш незбалансованими. Це надає можливість урядовим організаціям аналізувати альтернативні способи розвитку та модернізовувати стратегії з урахуванням отриманих знань.

Висновки до розділу 4

1. Проведений аналіз за даними 160 країн світу за 2018 р. на основі аналітичної інформації e-Governance Academy Foundation методами багатоатрибутного прийняття рішень (VICOR, TOPSIS та MAAM) дозволив у підрозділі 4.1 визначити так звані «еталонні» (максимальні з досягнутих у досліджуваних країнах) значення 12 основних параметрів, що враховуються під час визначення національних індексів кібербезпеки. За результатами розрахунків найбільшою мірою наближеною до еталона за більшістю параметрів виявилася система інформаційної безпеки Естонії, тоді як в Україні лише чотири з 12 параметрів національної системи інформаційної безпеки відповідають таргетованим значенням, три – на середньому рівні щодо усіх країн із вибірки, а інші п’ять – на критично низькому рівні.

2. На підставі результатів розрахунків обґрунтовано пропозиції щодо ребілдингу національної системи інформаційної безпеки в Україні в напрямку: розвитку спеціалізованих аналітичних груп з аналізу стану інформаційної безпеки, активізації участі України в розробленні Конвенції про кіберзлочинність, створення в Україні представництв міжнародних організацій із кібербезпеки, формування спеціалізованих наглядових органів у сфері

інформаційної безпеки, розроблення національних стандартів та стратегії інформаційної безпеки національної економіки, формування плану управління кіберкризовими ситуаціями на національному рівні, забезпечення участі України в міжнародних навчаннях щодо реагування на кіберкризи, розроблення заходів щодо здійснення спеціалізованих кібероперацій тощо.

3. З метою вирішення завдання формування державних програм підвищення рівня інформаційної безпеки в Україні у підрозділі 4.2 розроблено двоетапний підхід, відповідно до якого: 1) на першому етапі на підставі даних звітів компаній IBM та Deloitte щодо втрат від кіберінцидентів із боку інсайдерів (за даними 193 суб'єктів господарювання світу) та втрат від зовнішніх кіберінцидентів (за даними 524 суб'єктів господарювання світу) визначено середній рівень втрат від кіберзлочинів на одного працівника залежно від розміру компаній. Розрахунки засвідчили, що найбільш уразливими як до внутрішніх, так і до зовнішніх кіберзагроз, є компанії малого та середнього бізнесу (за світовими стандартами з кількістю до 500 осіб). Таким чином, у фокусі підвищеної державної уваги повинні перебувати питання підвищення забезпечення рівня інформаційної безпеки саме цих суб'єктів; 2) на другому етапі визначено галузеву належність малих та середніх підприємств, питання забезпечення рівня інформаційної безпеки яких повинна особливо ретельно контролювати держава.

4. Було розраховано граничні розміри витрат на інформаційну безпеку різних груп економічних суб'єктів (безпосередньо витрати на інформаційну безпеку, на відновлення інформації внаслідок її втрат та погашення збитків) у їх відношенні до прибутків, що генерують інформаційні системи цих компаній за 2020 р. Для компаній різної галузевої належності розраховано максимальну та мінімальну межі витрат на інформаційну безпеку, забезпечення яких не загрожує втраті фінансової стійкості цих компаній, а також установлено, що найнижчий рівень забезпечення витрат на інформаційну безпеку мають підприємства сфери послуг, тому в роботі розроблено рекомендації щодо формування спеціалізованих програм державної підтримки сервісних компаній – суб'єктів малого і середнього бізнесу, що передбачають, зокрема, розроблення стандартів

з інформаційної безпеки для них, формування системи контролю та моніторингу рівнів їх кібербезпеки, створення центрів сертифікації й підвищення кваліфікації IT-аудиторів, співробітників цих компаній тощо.

5. У підрозділі 4.3 побудовано чотириполюсну барицентричну модель за методом центра мас для визначення збалансованості розвитку країн, згідно з якою: 1) чим ближче виявиться розрахунковий центр мас побудованого чотирикутника (його вершини – відповідні виміри розвитку національної економіки) до еталонного значення, тим більшим є загальний рівень її збалансованості; 2) чим ближче координата композитного індикатора для кожного виміру розвитку національної економіки до 1, тим більш розвиненою є країна в цьому напрямку. Виявилося, що найбільш збалансованими країнами є: Нова Зеландія (0,0036), Малі (0,0185), Швеція (0,0201), Канада (0,0203), Швейцарія (0,0206) та ін., а найменш збалансованими – Демократична Республіка Конго (1,2355), Саудівська Аравія (0,2343), Російська Федерація (0,2252), Україна (0,2216), Алжир (0,2047) та ін. Тобто, високий рівень збалансованості за всіма вимірами розвитку національної економіки можуть досягати країни як із високим, так і з низьким рівнем добробуту, що дозволяє їм бути більш стійкими до внутрішніх та зовнішніх загроз. Результати для України засвідчили, що її прогрес у напрямку забезпечення цифрової спроможності та кібербезпеки в країні є істотно більш відчутний, ніж щодо економічного, політичного та соціального розвитку, що має бути основою обґрунтування напрямків відповідних регуляторних інтервенцій.

Основні положення четвертого розділу дисертаційної роботи опубліковано авторкою в роботах [24, 264, 316, 387, 390, 391, 392, 393, 399, 402].

РОЗДІЛ 5 РОЗВИТОК ПРИКЛАДНОГО МЕТОДИЧНОГО ІНСТРУМЕНТАРІЮ ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1 Поглиблення методичних засад експрес-оцінювання ризиків втрати інформації

В сучасних умовах збільшення інформаційних потоків та зростання науково-технічного прогресу будь-яка компанія зацікавлена у забезпеченні її інформаційної безпеки на вищому рівні. Головною причиною цьому є втрата інформації та знань. Доступ до інформації відкриває шлях до фінансових потоків компанії, її документації, контрагентів, співробітників, технологій, продукції, індивідуальних даних людей тощо. Сьогодні компанії повністю залежать від інформації та знань, тому випадкова або невипадкова втрата будь-якої інформації може призвести до негативних наслідків для підприємця, що буде пов’язано не тільки з витратами на відновлення інформації, але й з фінансовими втратами – наслідками від втрат важливої інформації.

За результатами досліджень, проведених Ponemon Institute на замовлення компанії IBM Security, середній розмір фінансових втрат від взломів та витоків інформації на червень 2019 року для підприємств середнього бізнесу світу склав близько 3,92 млн. дол. [5]. Ця сума зросла в порівнянні з 2018 роком на 1,55% (3,86 млн. дол.), з 2017 роком на 8,29% (3,62 млн. дол.), а за останні 5 років на 12% (3,50 млн. дол.) [1, 2, 3]. Безперечним лідером в цій сфері є США, компанії якої втратили за 2019 рік в середньому 8,19 млн. дол. Також можна виділити компанії Середнього Сходу (5,97 млн. дол.), Німеччини (4,78 млн. дол.), Канади (4,44 млн. дол.) та Франції (4,33 млн. дол.). Підприємства Індії та Бразилії отримали найнижчі середні збитки 1,83 млн. дол. та 1,33 млн. дол. відповідно [5].

Якщо аналізувати втрати інформації за галузями, то найбільші середні втрати було понесено компаніями у сфері здоров’я (6,45 млн. дол.), фінансів (5,86 млн. дол.), енергетики (5,60 млн. дол.), промисловості (5,20 млн. дол.) та фармацевтики (5,20 млн. дол.) [5]. За даними Breach Level щодня втрачається

більше ніж 18 мільйонів записів, тобто 214 записів кожну секунду. Рекордну кількість було досягнуто у першій половині 2018 року, тобто 3 353 172 708 записів [35]. Тобто ситуація в цілому у світі є несприятливою, оскільки спостерігається тенденція збільшення фінансових втрат в результаті витоків, взломів, викрадення та інших видів втрат інформації.

Втрати інформації та знань можуть призвести до втрат репутації компанії та довіри клієнтів, оскільки інформація може виявитися у відкритому доступі [38]. Так, дані мільйонів клієнтів компанії Microsoft стали доступними у мережі Internet. Причиною стало некоректне налаштування бази даних Elasticsearch. 250 мільйонів записів знаходилися у відкритому доступі з 05.12.2019 по 31.12.2019 [201]. Аналогічна ситуація склалася у лютому 2020 року у компанії Decathlon, інформація про клієнтів якої також стала доступною у мережі. Причиною стала слабка захищеність серверу Elasticsearch [230]. Також у лютому 2020 року стало відомо, що хакерами було вкрадено дані більш ніж 10,6 мільйонів клієнтів компанії MGM Resorts у 2019 році під час хакерської атаки [50].

У 2019 році велика кількість компаній зіткнулась з проблемою втрат інформації, яка стосувалася не тільки особистих даних людей, але й банківських даних – кредитних та дебетних карток. Так, зазнали втрат такі відомі компанії, як Mastercard, Wyze, Honda, Toyota, Lexus, Yves Rocher, фінансовий холдинг Capital One, ряд банків Ірану. Компанії не тільки таким чином втрачають клієнтів, але й за часту вони повинні заплатити штрафи. Так, за витік даних 9,4 мільйонів клієнтів компанія Cathay Pacific повинна була заплатити штраф розміром близько 642 тис. дол. [159]. На жаль, це не поодинокі випадки, коли компанії зобов’язані сплатити штраф у випадку втрати ними інформації.

Оскільки проблема, пов’язана із втратою інформації та знань, є актуальною, то для її вирішення у даному досліджені буде розглядатися питання, пов’язане з оцінкою ризиків втрати інформації та знань для компаній, тому що насамперед визначення ризиків дозволяє компанії зробити прогноз не тільки про ймовірні втрати, але й визначити проблемні місця в системі безпеки. На практиці для оцінки ризиків застосовують такі методики, як COBRA, RA Software Tool,

CRAMM, MethodWare, тощо. Їх перевагами є комплексний підхід до визначення ризику, який має на увазі збір великої кількості даних, розрахунок за спеціальними методами, підтримка стандартів безпеки. Використання даних методик потребує значних витрат часу. Компаніям необхідно витратити в середньому 206 днів, щоб знайти втрату інформації, та додатково 73 дні, щоб її відновити [5]. Саме тому в цьому досліджені приділено увагу розробці експрес-методики, яка дозволить швидко оцінити рівень ризику втрати інформації та знань. Її застосування на практиці дозволить скоротити час та трудовитрати.

Проблеми, пов’язані з дослідженням ризиків втрати інформації та знань, є досить поширеними у світі та актуальними. Основна причина – це зростання рівня інформатизації та комп’ютеризації суспільства. Так, можна прослідкувати динаміку публікаційної активності з 1971 по 2019 рр., присвяченої ризикам втрати інформації (рисунок 5.1).

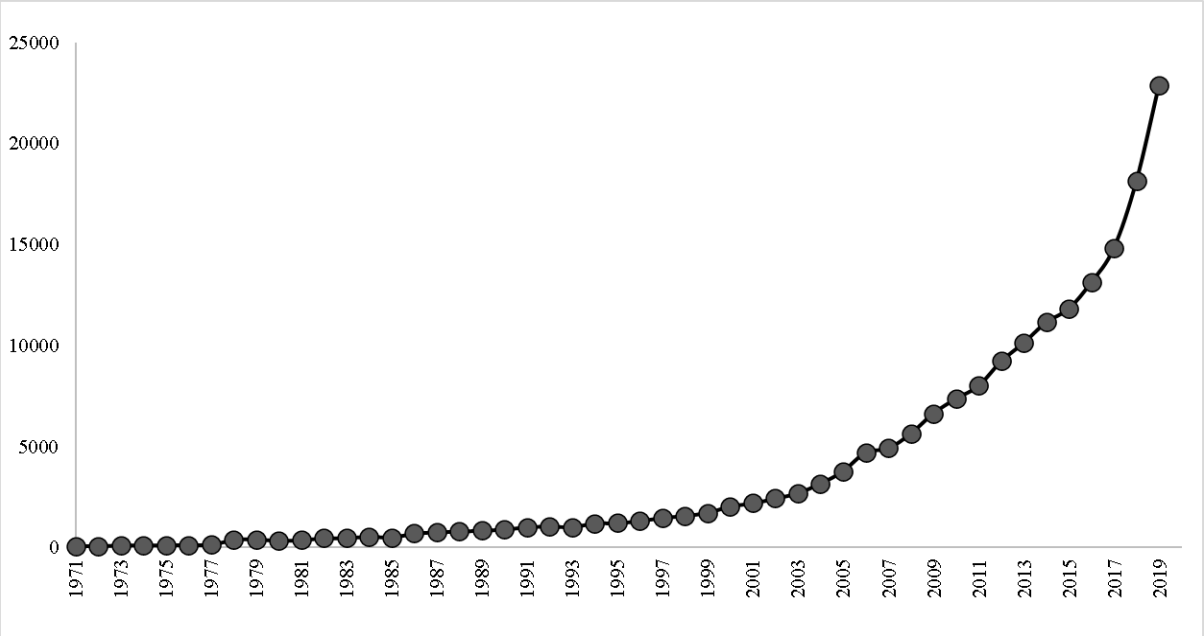


Рисунок 5.1 – Кількість публікацій, присвячених ризику втрати інформації та знань

Джерело: побудовано авторкою на основі даних Dimensions

Графік на рисунку 5.1 побудовано з використанням можливостей платформи Dimensions, на якій було знайдено 263 674 публікації за 48 років, які

стосуються тематики ризику втрати інформації. Можна спостерігати зростання зацікавленістю даною темою, особливо в останні 20 років. Це пов'язано із зростанням користувачів Інтернету, соціальних мереж, вільного доступу до багатьох ресурсів, активним впровадженням та використанням мобільних технологій, що в купі вплинуло на появу проблеми витоків та втрат інформації.

Ризик досліджують вчені в різних сферах. Особливо це актуально для комп'ютерних наук. На рисунку 5.2 представлено розподіл публікацій науковців світу в залежності від галузей дослідження, де можна спостерігати найбільшу зацікавленість для сфери комп'ютерних наук, для економічної сфери дослідження даної проблематики складають всього 0,45%.

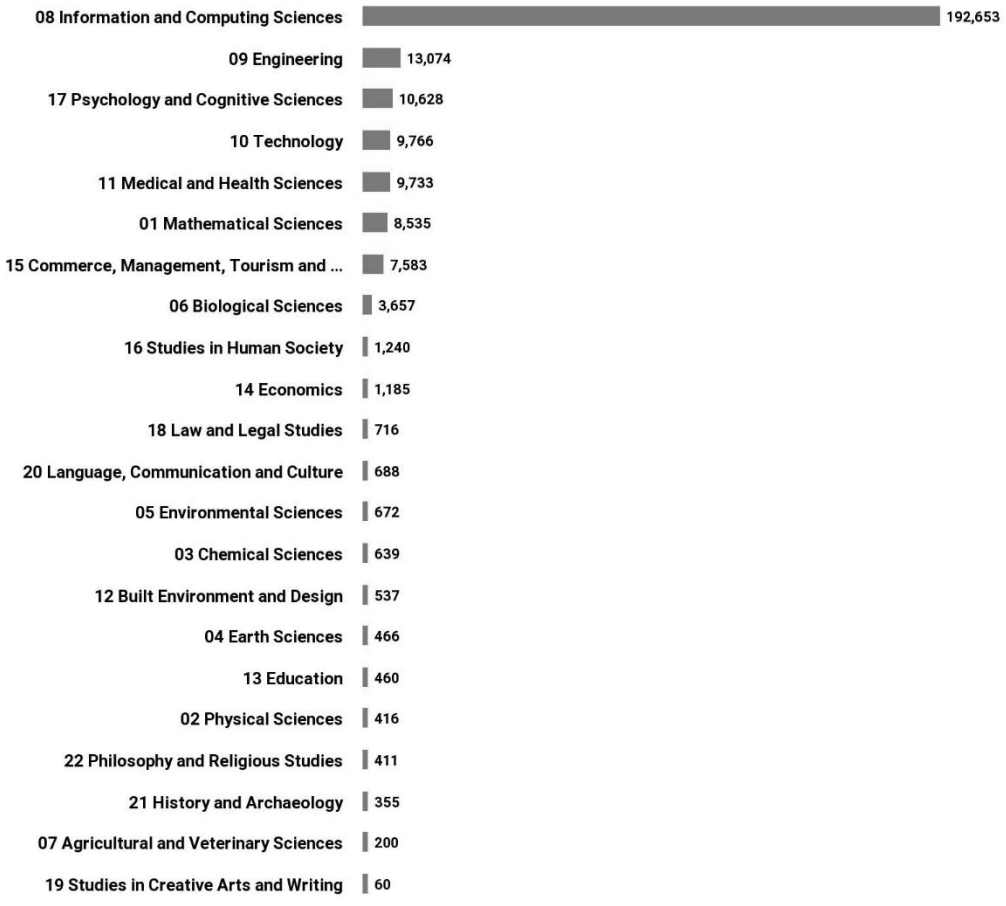


Рисунок 5.2 – Кількість публікацій, присвячених втраті інформації та знань, залежно від галузей досліджень

Джерело: побудовано авторкою на основі даних Dimensions

Так, серед зазначених сфер (рисунок 5.2) можна виділити наступні

дослідження, які розкривають аспекти втрати інформації у визначенні важливих детермінант: банківської сфери [15, 114, 164], підприємництва [32, 34, 137, 233], фондового ринку [166], сільського господарства [194], на державному рівні [161] та глобальному [216]. Окремо можна виділити методику, розроблену для визначення системних ризиків в банківській системі України, запропоновану в праці [250], яка дозволяє знижувати ризик втрати інформації в процесі консолідації банків. Описану в роботі Бойка А. та Роєнко В. [33] оцінку ризиків використовують у страхових компаніях для визначення підозрілих угод, що впливає на зміну підходів до збереження знань у страховій галузі.

Велика кількість наукових праць присвячується загальним питанням. Так, еволюція ризиків розглядається у статті Дворського Дж., Шонфелда Дж., Котаскова А. та Петракова З. [80]. Взаємодію різних видів ризиків – інвестиційного, фінансового та операційного, та їх вплив на економічну безпеку досліджували автори Диха М., Любохинець Л., Танасієнко Н. та ін. [81]. Основні етапи їх управління, принципи розподілу було вивчено в роботі Гриценко Л. та Красулі Т. [117]. Загальні теоретичні поняття ризику досліджувалися в роботі Лєонова С. та Лютої О. [168].

Для визначення ризиків пропонуються різні методики та математичні методи. Досить популярними є такі, як: статистичні [119, 245], фінансові [153], імітаційні, засновані на системній динаміці [135], ймовірнісні [196], Data Mining [227], економетричні [207, 243], теорія циклів [25]. Серед них найбільш популярними є оптимізаційні. Так, в роботі Ахмедова Ф. і Цейтун М. [8] було їх використано для побудови моделі кількісного оцінювання ринкових ризиків. Також даний інструментарій застосовується і в роботах [19, 156]. Нестандартним підходом є метод побудови чотирикутника факторів та визначення центру мас, який було застосовано у статті [24] для розрахунку ризиків ділової активності та який дозволяє здійснити прогноз їх стабільності. Також застосовується й підхід кількісного оцінювання індексованої інформації, що відповідає потребам Національної оцінки ризиків легалізації коштів, одержаних злочинним шляхом, та фінансування тероризму [73]. Окрім перелічених, можна виділити роботу

Дзівок Е. [82], в якій досліджувалися різні підходи моделювання операційного ризику: базовий індикаторний підхід (BIA) та стандартизований підхід (TSA), включаючи його варіант - альтернативний стандартизований підхід (ASA). Вченими Худаковою М. та Дворським Дж. було запропоновано оцінювати ризики та їх джерела залежно від швидкості впровадження процесу управління ними на малих та середніх підприємствах [118]. Також пропонують використовувати: методи "центру ваги", експертного оцінювання, багатовимірного факторного аналізу, апарату нейронної мережі [149]; галузевого аналізу [188]; теорії біфуркацій [246].

Однією з причин втрати інформації є шахрайства, які здійснюються працівниками, керівництвом компанії, зовнішніми злочинцями. Для протидії даного явища Евана Е., Металія М., Мірфазлі Е., Георгієва Д., Састродіхарйо І. [87] пропонують теорію пентагону шахрайств, яка може бути одним із засобів зниження витоків інформації з компанії. Деякі науковці вважають ефективним використання систем моніторингу для боротьби із шахрайствами, що впливають на втрату інформації [138, 151, 160], деякі пропонують трансформаційні моделі [148]. Однією з головних причин втрати інформації є людський фактор, що проявляється у здійсненні помилок працівниками за рахунок недостатнього досвіду або відсутності професійних знань. Тому важливо розвивати інноваційні підходи до створення та використання тренінгових систем в компаніях [253], а також розвивати системи навчання протягом усього життя та протягом усієї професійної діяльності працівників [199, 249]. Також важливо для забезпечення цього напрямку дотримуватися корпоративної соціальної відповідальності, яка може бути обєктом впливу великих даних [110].

Із зростанням рівня науково-технічного прогресу, інформатизації суспільства та підприємництва, зростають проблеми, пов’язані із збором, обробкою, зберіганням та архівуванням інформації на якісному та безпечному рівнях, що також може бути причиною втрати інформації. Цим аспектам приділено увагу у дослідженнях авторських колективів [25, 27, 116, 139]. Створення корпоративних баз даних здійснюють важливий вплив на інформацію

та знання в компанії, тому потрібні дієві інструменти для зниження ризику втрат в умовах функціонування Big Data. В цьому аспекті запропоновано використання теорії дифузії інновацій, що дозволить в процесі інтеграції даних зменшити ризик їх втрати [247, 248]. Також в цьому напрямку запропоновано в дослідженні Васильєвої Т., Лєонова С., Макаренко І. та Сірковської Н. [244] впровадження нових підходів до подачі та розкриття корпоративної інформації, що націлено на зниження ризику її втрати. Слід відмітити й заходи щодо збереження конфіденційності даних для забезпечення загального регламенту про їх захист, розкриті в роботі [158], а також для забезпечення захисту інформації у банках з метою протидії відмивання коштів та фінансування тероризму [162, 169].

Сучасні реалії вимагають комплексних підходів до управління ризиками, таких як створення: інтегрованої системи управління ризиками, яка позитивно впливає на довгострокові результати діяльності фірми [184]; автоматичної інформаційної системи оцінки ризиків, результати розробки якої для сільськогосподарських підприємств України запропонували Ніценко В., Мардані А., Стреймікіс Й., Іщенко М. та інші [187]. Поряд із цим зростає популярність стрес тестування для виявлення та зниження ризиків [136], а також методики швидкої оцінки ризиків [11].

Ризик втрати інформації та знань представляє собою можливу небезпеку, загрозу для компанії, що призводить до втрати найціннішого ресурсу – інформації та знань. Існування такого виду ризику залежить від певних умов – інцидентів, причинами виникнення яких можуть бути дії людини (персоналу компанії), проблеми технічного характеру, програмне забезпечення, незаконні дії кіберзлочинців, вірусні атаки. З іншого боку, появу такого інциденту можуть обумовлювати різні фактори. Наприклад, якщо працівник компанії несвідомо не зберіг результати своєї праці, то як результат було втрачено інформацію, на відновлення якої необхідно витратити додатковий час та додаткові ресурси, тобто компанія втратила не тільки інформацію але й фінансові ресурси, розміром яких, як правило, й вимірюються втрати інформації в компанії. Виходячи з наведеного прикладу, конкретна дія працівника – це фактор, який вплинув на

втрату інформації, тобто згенерував ризик. Оскільки ініціатором була людина, то наведений фактор відноситься до інциденту, обумовленому людськими діями.

Для визначення рівня ризику втрати інформації та знань визначимо інциденти (причини) та фактори впливу, які обумовлюють появу даного інциденту в компанії.

1. Інцидент, обумовлений помилковими діями персоналу компанії (“Людський фактор” – “Human Error Incident” – HE). Так, помилки користувачів, їх необережне поводження з комп’ютерною технікою, програмним забезпеченням, може призводити до втрат інформації. Так, за статистикою біля 32% втрат відбувається завдяки людського фактору [252]. До факторів впливу на появу даного інциденту можна віднести наступні: навмисне видалення файлів даних; ненавмисне видалення файлів даних; навмисне не зберігання інформації; ненавмисне не зберігання інформації; перезапис важливих файлів; випадкове форматування жорсткого диска; протікання рідини; навмисна помилка; ненавмисна помилка; використання інших імен користувачів та паролів; крадіжка інформації працівниками; порушення правил та процедур роботи з інформацією.

2. Інцидент, пов'язаний із вірусними атаками та дією антивірусних програм (“Віруси та шкідливе програмне забезпечення” – “Viruses and Malware” – VM). Компанії часто стикаються з ситуацією, коли завдяки некоректної дії антивірусної програми або завдяки появі нового вірусу, вірус проникає в систему, що призводить до втрати інформації, блокування роботи всієї компанії. За статистикою, близько 7% втрат інформації відбувається саме завдяки інциденту “Viruses and Malware” [252]. Фактори, які обумовлюють появу даного інциденту, це: відсутність оновлення антивірусів; відсутність сканування антивірусом; втрата інформації через вірус; псування вірусом; навмисна активація вірусного повідомлення користувачем; ненавмисна активація вірусного електронного листа користувачем; навмисне відключення антивірусного програмного забезпечення; ненавмисне відключення антивірусного програмного забезпечення; антивірусний помилковий сигнал;

видалення важливої інформації антивірусом.

3. Інцидент, який виникає завдяки технічним, механічним несправностям (“Технічний ризик” – “Technical risk” – TR). 44% втрати інформації та знань відбувається саме завдяки випадкам, пов’язаними з відмовою техніки, механічним пошкодженням, зносу носіїв, неналежної експлуатації [252]. Також до цієї групи можна віднеси фактори, які призводять до неналежної роботи техніки або її фізичному винищенню. Тому виділено ряд факторів, що обумовлюють даний інцидент: механічна несправність жорсткого диска; пошкодження комп'ютера через перегрів; пошкодження комп’ютера через скупчення пилу в ньому; навмисне падіння або штовхання комп’ютера; ненавмисне падіння або штовхання комп’ютера; торнадо, землетрус та інші стихійні лиха; вогонь; планове відключення електроенергії; незаплановане відключення електроенергії; навмисне вимкнення комп’ютера без збереження інформації; ненавмисне вимкнення комп’ютера без збереження інформації; конфлікт між пристроями.

4. Інцидент, обумовлений незаконними діями кіберзлочинців, вчинених по відношенню компанії з метою викрадення інформації або знань (“Кримінальний ризик” – “Criminal risk” –CR). На сьогодні цей інцидент зустрічається у 4% випадків [252], але він важко прогнозований та передбачуваний, оскільки є причиною дій, які здійснюють зовнішні по відношенню до компанії особи. Як правило, вони цікавляться інформацією щодо фінансових потоків компанії, нових технологій та новітніх розробок. Викрадення або псування цієї інформації призводить до незрівнянно великих збитків, можливо й банкрутства компанії. За часту конкуренти вдаються до такого виду злочину, щоб нашкодити іншим компаніям. Нами виділено можливі фактори, які пливають на появу CR: вхід за допомогою чужого логіна; крадіжка комп’ютера; втрата комп’ютера; копіювання інформації на знімний носій; надсилання інформації на зовнішню електронну адресу; крадіжка інформації; заміна інформації; несанкціоноване використання прав адміністратора; соціальна інженерія; DoS-атака; смурф атаки; UDP шторм; UDP-бомба; сніффінг; викрадення IP; фіктивний DNS-сервер; IP-

спуфінг; втрата інформації через шифрування / дешифрування; злом ключів шифрування.

5. Інцидент, пов'язаний з некоректною роботою програмного забезпечення (“Пошкодження програмного забезпечення” – “Software Corruption” – SC). 14% втрат інформації та знань припадає на збої у програмному забезпеченні компанії [252]. Це є результатом неналежних налаштувань операційних та прикладних програм, невикористання посадових інструкцій, порушення ліцензійних умов користування, неналежного тестування, помилок у програмному коді. Так, виділимо фактори, які впливають на формування SC: несподівані або неправильні вимкнення програмного забезпечення; відсутність оновлень програмного забезпечення; переформатування під час оновлення системи; помилки в реєстрах Windows; ситуації, коли програма не відповідає; неточне видалення або встановлення програмного забезпечення; помилки в драйверах; помилки обчислення; логічні помилки; помилки вводу-виводу даних; помилки обробки даних; помилки сумісності; помилки сполучення.

Перелік факторів може бути розширений кожною компанією але в даному досліджені було виділено найбільш типові. Кожен фактор характеризується кількістю випадків за певний проміжок часу та сумою грошових втрат, витрачених компанією на відновлення інформації та втраченого прибутку. Для здійснення розрахунків за розглянутою далі методикою було узято інформацію щодо випадків та сум втрат по наведеним факторам за місяць у компанії «А» (назва компанії не надається у зв’язку із умовами її комерційної таємниці).

Для оцінювання ризику втрат інформації та знань є доцільним використання саме експрес-методик, які дозволять швидко визначити його рівень. Однією з таких методик є побудова карти ризику, яка є розповсюдженою на практиці, оскільки використовується для наочної оцінки різних ризиків, що виникають в діяльності економічних агентів. Вона будується на площині, одна сторона якої – це ймовірність виникнення події, а інша сторона – сума, яку може втратити компанія при настанні даної події. Як правило, дана площина поділяється на сектори, кількість яких компанія визначає в залежності від того,

який рівень деталізації ризику вона хоче отримати. Потім аналізується предметна галузь та визначається до якого сектору буде відноситися подія, яка виникає за умови заданої ймовірності та пов'язана із заданим рівнем втрат. Але недоліком подібної карти ризику є те, що при її формуванні менеджери за часту використовують суб'єктивні судження, які підкріплюються тільки власним досвідом. Особливо це стосується ймовірності, до визначення якої на практиці підходять з використанням власних міркувань. Такий підхід є доцільним тільки для швидкого прийняття рішення.

В даному досліджені використаємо підхід побудови карти ризиків, але модифікуємо процес її побудови за рахунок математичного визначення оцінок ризику, що базується на розгляді факторів та інцидентів як елементів теорії множин, та використанні формалізації за допомоги бінарних оцінок. Такий підхід було використано для визначення операційного ризику банків, що лягло в основу розробки методики для Національного банку України, запропонованої в науковій праці [72].

Нехай ризик втрати інформації та знань обумовлюється рядом інцидентів від 1 до k (у роботі розглядається 5 інцидентів – HE, VM, TR, SC, CR, тобто $k = 5$). На формування кожного з цих інцидентів впливає ряд факторів (n факторів, в даній роботі наведено 66 факторів, дані по яким було узято для розрахунків), які розглядаються як кількість випадків, що трапляються в компанії та викликають втрату інформації, та сума фінансових втрат, пов'язана із втратою інформації та знань. Множини інцидентів $M_{i,i=1\div n} = \{g_{l,l=1\div k}\}$, обумовлені кожним j фактором, можуть перетинатися, утворюючи множину $M_{i,i=1\div n} \cap M_{j,j=1\div n,i\neq j} = \{g_{li,l=1\div k} = g_{lj,l=1\div k}\}$. Крім того, кожен з факторів обумовлює формування тільки одного інциденту. Виходячи з цього, методика оцінки ризику втрат інформації складається з наступних етапів.

Перший етап. Необхідно побудувати таблицю кількості випадків, які формують п'ять визначених інцидентів (див. табл. 5.1), та таблицю втрат, пов'язаних із здійсненням випадків у діяльності компанії (див. табл. 5.2).

Таблиця 5.1 – Кількість випадків факторів, які формують п’ять інцидентів

№	Назва факторів впливу	Інциденти, які асоціюються з ризиком втрати інформації				
		Людський фактор	Віруси та шкідливе програмне забезпечення	Технічний ризик	Кримінальний ризик	Пошкодження програмного забезпечення
1	Фактор 1	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}
2	Фактор 2	a_{21}	a_{22}	a_{23}	a_{24}	a_{25}
…	…	…	…	…	…	…
j	Фактор j	a_{j1}	a_{j2}	a_{j3}	a_{j4}	a_{j5}
…	…	…	…	…	…	…
n	Фактор n	a_{n1}	a_{n2}	a_{n3}	a_{n4}	a_{n5}

де n – максимальне значення кількості факторів;

a_{ji} - кількість випадків фактору j, які впливають на формування інциденту i.

Таблиця 5.2 – Суми втрат, пов’язаних із здійсненням випадків у діяльності компанії

№	Назва факторів впливу	Інциденти, які асоціюються з ризиком втрати інформації				
		Людський фактор	Віруси та шкідливе програмне забезпечення	Технічний ризик	Кримінальний ризик	Пошкодження програмного забезпечення
1	Фактор 1	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}
2	Фактор 2	s_{21}	s_{22}	s_{23}	s_{24}	s_{25}
…	…	…	…	…	…	…
j	Фактор j	s_{j1}	s_{j2}	s_{j3}	s_{j4}	s_{j5}
…	…	…	…	…	…	…
n	Фактор n	s_{n1}	s_{n2}	s_{n3}	s_{n4}	s_{n5}

де s_{ji} – сума втрат за фактором j, які впливають на формування інциденту i.

Далі необхідно провести класифікацію операцій на групи, які враховують принцип побудови карти ризиків. Тобто, необхідно відібрати операції з урахуванням кількості випадків та сум втрат. Для цього пропонуємо логіку відбору, який буде проводитися за формулою (5.1):

$$a_{pji} = \begin{cases} a_{1ji}, if\ a_{ji} \leq m\ \wedge s_{ji} \leq h \\ a_{2ji}, if\ \ a_{ji} > m\ \wedge s_{ji} \leq h \\ \quad ... \\ a_{tji}, if\ \ a_{ji} > m\ \wedge s_{ji} > h \end{cases} \quad (5.1)$$

де a_{pji} – відібране значення фактору j для інциденту i, що відповідає p ($p = 1 \div t; t = 4\ \vee p = 9\ \vee p = 25$ ...) групі карти ризику;

m – порогове значення для кількості випадків факторів, які встановлює компанія самостійно, виходячи з статистики даних по випадках за попередні періоди;

h – порогове значення для суми втрат, які встановлює компанія самостійно, виходячи з її політики. Це може бути сума, яка дорівнює відсотку від прибутку компанії або відсотку від грошового обороту, значення якого не є значущим для компанії.

Другий етап. Визначаємо, що ризик – це ймовірність здійснення події за умови негативних обставин, то для його визначення потрібно формалізувати значення факторів. Тобто необхідно значення кількості випадків для відібраних за p-групами факторів перерахувати із використанням бінарних характеристик. На практиці, якщо трапляється випадок, який призводить до втрат інформації та відповідно фінансових втрат, то незалежно від кількості таких випадків, це негативне явище, з яким компанія повинна боротися. Тому, незалежно від кількості випадків, значення для фактору буде дорівнювати “1”, що означатиме факт здійснення випадку втрати інформації та знань. Якщо значення буде дорівнювати “0”, то в компанії відсутні будь-які випадки втрати інформації завдяки певному фактору. Для формалізації використаємо формулу (5.2):

$$a_{pji} = \begin{cases} 1, if\ a_{ji} > 0 \\ 0, if\ \ a_{ji} = 0 \end{cases}. \quad (5.2)$$

Для визначення загальної кількості випадків по кожному інциденту з урахуванням вибірки даних для кожної групи карти ризику, необхідно визначити

суму бінарних характеристик за i-им інцидентом по кожній p групі карти ризиків за формулою (5.3):

$$A_{pi} = \sum_{j=1}^{n} a_{pji}. \tag{5.3}$$

Значення A_{pi} показує ефект від впливу факторів на інцидент ризику. Якщо $A_{pi} = 0$, то випадки впливу фактору на i-тий інцидент ризику відсутні, якщо $A_{pi} = 1$, то маємо один випадок впливу фактору, який може бути випадковим, але якщо $A_{pi} > 1$, то можна стверджувати, що компанія має проблеми в системі безпеки, які формують додатковий вплив на інцидент ризику. Тому для визначення рівня ризику потрібно визначити дві складові. Перша складова відображатиме, так би мовити, базову сукупність значень інцидентів ризику, які враховуватимуть тільки те, що є факт або відсутності впливу фактору на інцидент, або існування впливу фактору не залежно від кількості випадків такого впливу. Друга складова відображатиме додатковий вплив на інцидент ризику, який враховує те, що кількість випадків по кожному інциденту ризику може бути більше “1”, при чому врахуємо також й вплив сум втрат на інцидент ризику.

Значення першої складової визначається як $\sum_{i=1}^{k} Z_{pi} \,|A_{pi} \geq 1$. При цьому Z_{pi} – це базова сукупність значень інцидентів ризику, яка розраховується за формулою (5.4):

$$Z_{pi} = \begin{cases} 1, if\ A_{pi} > 0 \\ 0, if\ A_{pi} = 0 \end{cases}. \tag{5.4}$$

Значення другої складової для оцінки ризику визначається на третьому етапі.

Третій етап. Розраховані характеристики A_{ki} відображають загальну кількість негативних випадків по кожному інциденту, але треба враховувати, що

ці випадки можуть приводити до втрат різних обсягів інформації та відповідно завдавати компанії різні збитки. Так, наприклад, один випадок, пов'язаний із “DoS атаками”, може привести до втрати інформації на 1 000 000 дол., а декілька випадків, пов’язаних із “Проливом рідини”, можуть завдати збитку на 10 000 дол. Тобто необхідно врахувати вплив факторів не тільки з урахуванням кількості випадків їх здійснення, але й з урахуванням впливу суми втрат на інциденти ризику як сукупності $f\left(M_{i,i=1\div n} \cup M_{j,j=1\div n}\right) \approx \left\{d_{l,l=1\div k}\right\}$. Тому потрібно провести коректування бінарних значень a_{pji} шляхом використання формули (5.5):

$$a^*_{pji} = a_{pji} \times r_{pi}, \tag{5.5}$$

де a^*_{pji} – скоректоване значення a_{pji};

r_{pi} – вагові коефіцієнти, розраховані, як $\sum_{j=1}^{n} s_{pji}$ та потім проранжовані від 1 до i. Тобто отримуємо суму втрат для кожного з інцидентів та присвоюємо ранг наступним чином – найбільша сума дорівнює рангу “1”, найменша сума дорівнює рангу “i”.

Проведені коректування дозволять визначити другу складову для оцінки ризику, що відображає додатковий вплив на інцидент. Вона визначатиметься як $\left[\frac{1}{n}\sum_{j=1}^{n} a^*_{pij}\right] | A_{pi} \geq 2$.

Четвертий етап. Враховуючи результати другого та третього етапів, визначаємо кількість випадків здійснення факторів, які впливають на інцидент та які враховують базову сукупність значень інцидентів ризику та додатковий вплив на інцидент за формулою (5.6):

$$B_{pi} = Z_{pi} | A_{pi} \geq 1 + \left[\frac{1}{n}\sum_{j=1}^{n} a^*_{pij}\right] | A_{pi} \geq 2, \tag{5.6}$$

де B_p – кількість випадків здійснення факторів, які впливають на інцидент, та

які враховують базову сукупність значень інцидентів ризику та додатковий вплив на інцидент;

[] – ціла частина числа.

П'ятий етап. Для визначення рівня ризику необхідно врахувати також ситуацію, коли в компанії трапляються всі можливі випадки впливу факторів на інциденти ризику, тобто служба безпеки виявила хоча б один факт такого впливу кожного фактору на кожен інцидент. З цією метою будується матриця (див. табл. 5.3), елементи якої приймають значення, що дорівнюють "1". Це означає, що кожний j-тий ($j = 1 \div k$) інцидент ризику формується за рахунок впливу i-того фактору.

Таблиця 5.3 – Матриця бінарних характеристик для всіх можливих випадків впливу факторів на інциденти ризику

№	Назва факторів впливу	Інциденти, які асоціюються з ризиком втрати інформації				
		Людський фактор	Віруси та шкідливе програмне забезпечення	Технічний ризик	Кримінальний ризик	Пошкодження програмного забезпечення
1	Фактор 1	1	1	1	1	1
2	Фактор 2	1	1	1	1	1
…	…	…	…	…	…	…
j	Фактор j	1	1	1	1	1
…	…	…	…	…	…	…
n	Фактор n	1	1	1	1	1
∑		n	n	n	n	n

Використовуючи даний підхід, визначаємо за формулою (5.7) кількість усіх можливих випадків здійснення факторів, які впливають на інцидент, та які враховують додатковий вплив на інцидент в залежності від обсягу втрат:

$$B_{pi}^{*} = Z_{pi} + \left[\frac{1}{n}\sum_{j=1}^{n} r_{pj}\right], \tag{5.7}$$

де B_p^* – усі можливі випадки здійснення факторів, які впливають на інцидент, та які враховують додатковий вплив на інцидент в залежності від обсягу втрат;

Z_{pi} – це базова сукупність значень інцидентів ризику, яка розраховується за формулою (5.4);

r_{pj} – ранг j-го ($j = 1 \div n$) фактору, що впливає на i-тий інцидент ризику, та який було відібрано в залежності від p-групи карти ризиків;

$[\ ]$ - ціла частина числа.

Шостий етап. На цьому етапі проводиться розрахунок рівня ризику за формулою (5.8) на основі співвідношень: кількості випадків здійснення факторів, які впливають на інцидент, враховують базову сукупність значень інцидентів ризику та додатковий вплив на інцидент; та кількості усіх можливих випадків здійснення факторів, які впливають на інцидент, враховують додатковий вплив на інцидент в залежності від обсягу втрат:

$$R_{pi} = \frac{B_{pi}}{B_{pi}^*}, \tag{5.8}$$

де R_{pi} – оцінка рівня ризику за кожним інцидентом, значення якого буде знаходитися в межах від “0” до “1”. Результат, який ближче до “1”, говорить про підвищений рівень ризику для інциденту i, тобто втрати інформації будуть значними для компанії. Якщо значення ризику наближається до “0”, інцидент генерує низький рівень ризику, тобто втрати інформації будуть незначними або прийнятними для компанії.

Сьомий етап. На передостанньому етапі визначається за формулою (5.9) загальний рівень ризику по кожній з $p-$груп, які відповідають розподілу інформації в карті ризику:

$$R_p = \sum_{i=1}^{k}\left(Z_{pi}|A_{pi} \geq 1 + \left[\frac{1}{n}\sum_{j=1}^{n} a^*_{pij}\right]|A_{pi} \geq 2\right) / \sum_{i=1}^{k}\left(Z_{pi} + \left[\frac{1}{n}\sum_{j=1}^{n} r_{pj}\right]\right) \quad (5.9)$$

або скоротимо запис:

$$R_p = \sum_{i=1}^{k} B_{pi} / \sum_{i=1}^{k} B^*_{pi}$$

де R_p – загальний рівень ризику по кожному p-му сектору;

Восьмий етап. На завершенні будується карта ризиків втрат інформації компанією, яка відображає рівень ризику для кожного інциденту в залежності від належності факторів до одного з p-секторів карти.

Використовуючи вхідну інформацію щодо обраних 66 факторів, які стосуються випадків, що слугують основними причинами втрати інформації в компанії «А» (див. таблиця Л.1 додатку Л), проведено розподіл даних за 9 секторами для майбутньої карти ризиків. Цю кількість було обрано тому, що карти ризиків на 9 секторів є більш інформативними та не обтяжують процес їх побудови та ідентифікації отриманих результатів. Наступною причиною є те, що збільшення кількості груп потребує більшої вибірки даних, тому це не є доцільним для перевірки роботи представленої методики.

Виходячи з того, що первинна інформація, яку буде використано для побудови карти ризиків, – це кількість випадків та суми втрат для кожного фактору, то було проведено класифікацію даних за 9 секторами, що в подальшому дозволило провести розрахунки та побудувати карту для оцінки ризиків втрат інформації компанії (рисунок 5.3).

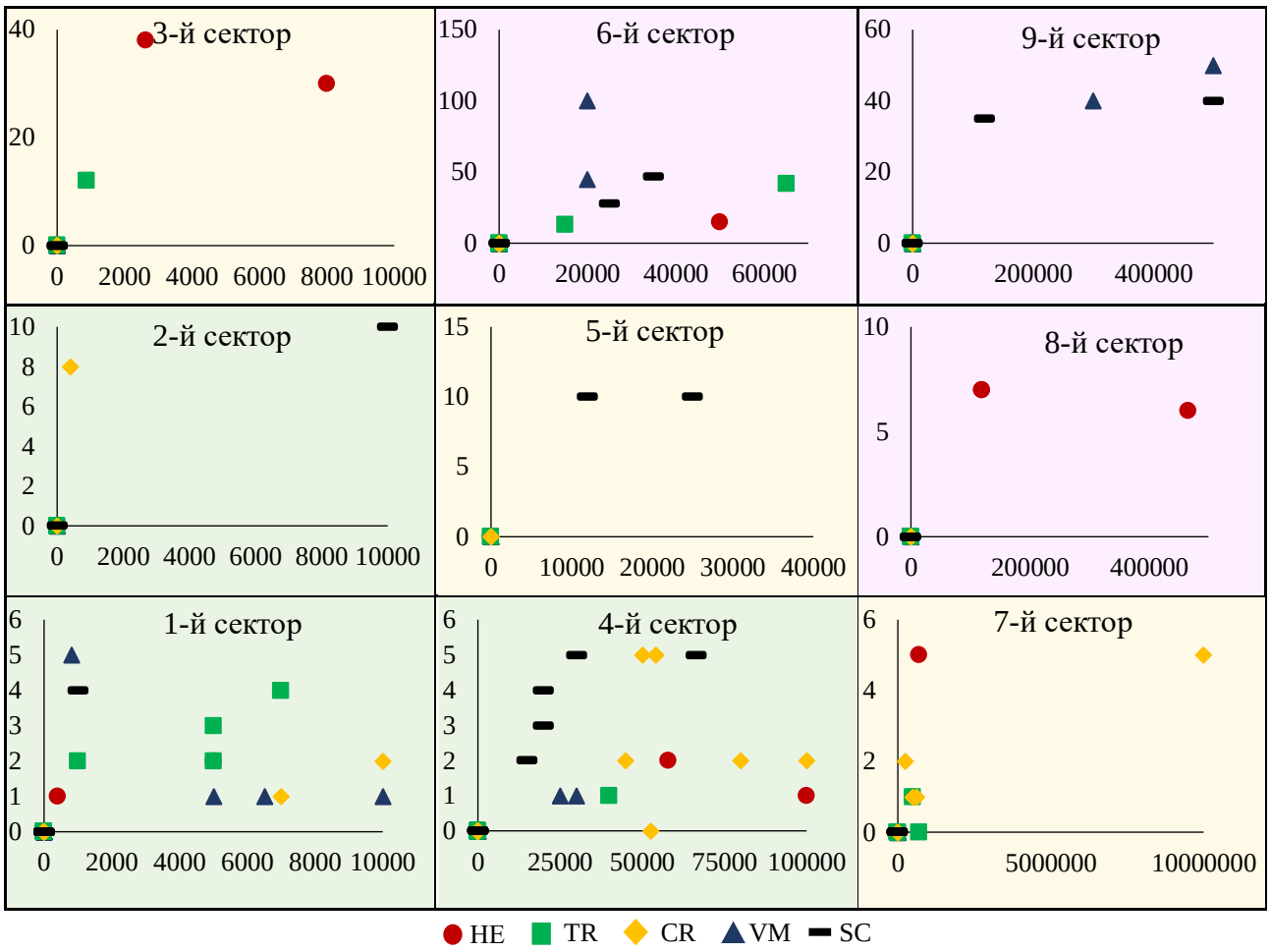


Рисунок 5.3 – Класифікація факторів, що формують п’ять інцидентів ризиків, за дев’ятьма секторами (складено авторкою)

На рисунку 5.3 проведено класифікацію факторів в залежності від кількості випадків (вісь Y) та сум втрат (вісь X). 1, 2 та 4 сектори за логікою побудови карти ризиків формують зону безпечних ризиків, в якій випадки втрат інформації зустрічаються рідко та суми втрати є незначними. 3, 5 та 7 сектори формують зону допустимих ризиків, тобто такі випадки трапляються дуже часто, але суми втрати є незначними, або випадки досить рідкі, але вони генерують значні для компанії втрати інформації. 6, 8 та 9 сектори – це зона небезпечного ризику, тому що втрати є значними для компанії та випадки трапляються досить часто. Так, сектори було сформовано за критеріями, значення яких було обрано на основі результатів аналізу даних компанії, яку було обрано для побудови карти ризиків (див. табл. 5.4).

Таблиця 5.4 – Критерії для класифікації факторів

№ сектору карти ризиків	Вісь Y		Вісь X	
	Мінімальна кількість випадків	Максимальна кількість випадків	Мінімальну сума втрат, дол.	Максимальна сума втрат, дол.
1	0	5	0	10,000
2	6	10	0	10,000
3	11	+∞	0	10,000
4	0	5	10,001	100,000
5	6	10	10,001	100,000
6	11	+∞	10,001	100,000
7	0	5	100,001	+∞
8	6	10	100,001	+∞
9	11	+∞	100,001	+∞

Компанії можуть самостійно вирішувати, які значення щодо кількості випадків та обсягів втрат вони можуть встановлювати для визначення обсягів ризику втрат інформації та знань. З рисунка 5.3 можна побачити, що найбільш масовими є випадки факторів з 1, 4 та 6 секторів, в інших групах присутні одиничні фактори. Але для кінцевих висновків необхідно визначити рівень ризику втрати інформації та знань. Використовуючи етапи запропонованої методики (формули 5.1-5.9), було розраховано рівень ризику для кожного інциденту та для кожного сектору (див. рисунки Л.1-Л.0 додатку Л). Результати представлено у вигляді карти ризиків на рисунку 5.4.

Першим розглянемо “Кримінальний ризик”, який присутній у 1, 2, 4 та 7 секторах (рисунок 5.4), тобто випадків факторів, що формують даний вид ризику, зустрічається небагато, оскільки вони пов’язані із зовнішнім втручанням у інформаційну систему компанії, але ризик їх існування є помірним – 0,5 та 0,67. Це говорить про те, що ймовірно компанія має певні проблеми з системою кіберзахисту, яка допускає ситуації, в яких відбувається втрата інформації та знань через зовнішні джерела, тобто шахраїв, хакерів, тощо. Попадання даної категорії в 7-й сектор також свідчить про те, що з певною долею ймовірності компанія може втрачати досить значні суми коштів, що врешті-решт може призвести до колосальних збитків. Тому варто звернути увагу на ті ситуації, які призводять до підвищення інциденту “Кримінальний ризик” в компанії.

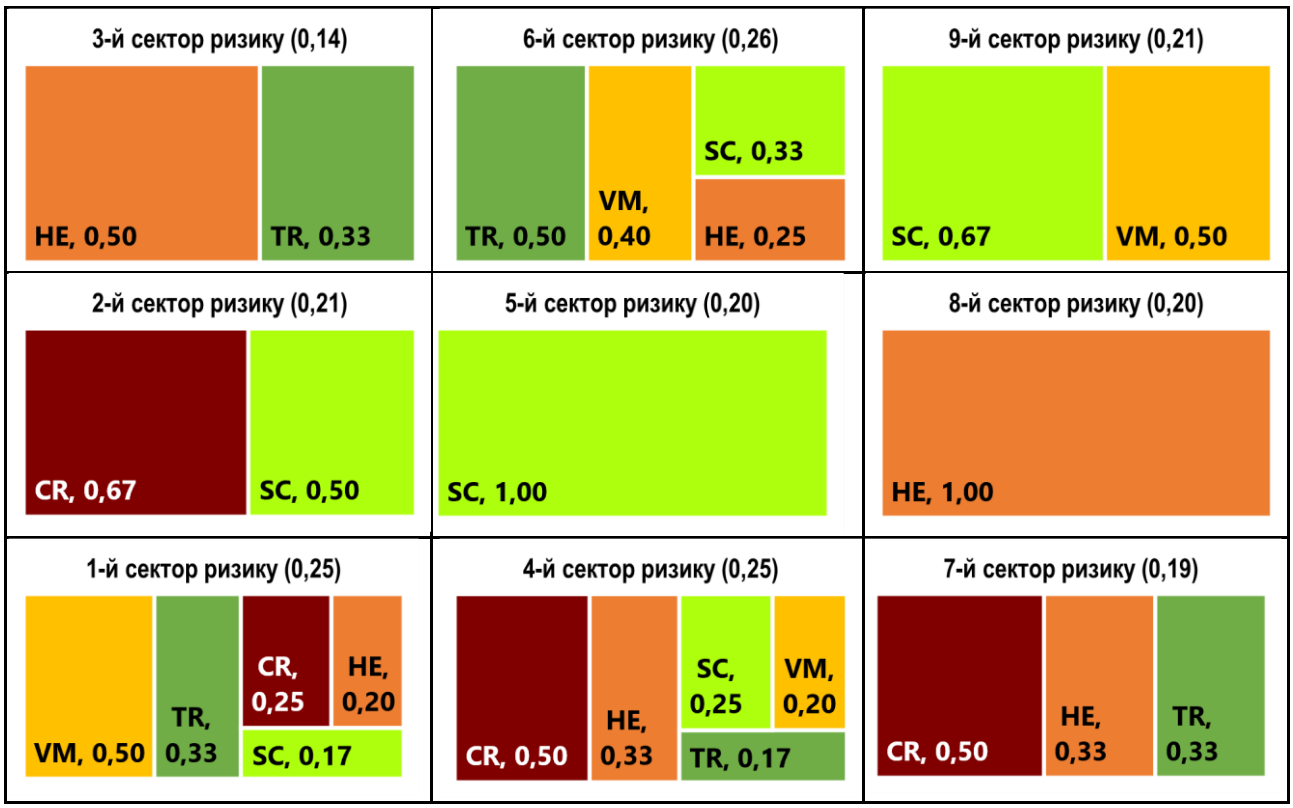


Рисунок 5.4 – Карта ризиків (складено авторкою)

“Пошкодження програмного забезпечення” зустрічається у 1, 2, 4, 5, 6, 9 секторах (рисунок 5.4), що свідчить про розповсюдженість даного виду ризику у випадках інцидентів, пов’язаних з втратами інформації та знань. Особливо критичним є даний вид ризику в 5-у та 9-у секторах, тобто випадки втрати інформації з високим ступенем ймовірності зустрічаються в компанії та їх причиною слугують фактори, що обумовлюють інцидент “Пошкодження програмного забезпечення”. Компанії варто переглянути інструкції та протоколи використання, налаштування програмного забезпечення, оскільки втрата інформації за даним напрямком може відбуватися за рахунок некоректних налаштувань операційної системи та користувацького програмного забезпечення, що сприяє викривленню інформації, зниженню працездатності комп’ютерів, втрати часу, тощо.

“Людський фактор” присутній у 1, 3, 4, 6, 7 та 8 секторах (рисунок 5.4), що говорить про масовість випадків втрати інформації, ініціатором яких є людина. Особливо критичним є ризик 8-го сектору (дорівнює 1,00), тобто з високим рівнем ймовірності дії працівників компанії призводять до значних втрат інформації та значних фінансових втрат. В купі з інцидентом “Пошкодження

програмного забезпечення” інцидент “Людський фактор” може сприяти появі проблемних місць в системі кібербезпеки, що призведе до простоїв. Як результат, це може стати причиною не тільки втрати інформації та знань, але й фінансових витрат на їх відновлення.

Інцидент “Віруси та шкідливе програмне забезпечення” проявляється у 1, 4, 6 та 9 секторах. Ризик втрат інформації за цим інцидентом є помірним. Його значення (0,5) у 9-у секторі може бути результатом вірусної атаки, що говорить про нетиповість впливу факторів цього інциденту на втрату інформації. Але факт наявності цього інциденту в 9-у секторі сигналізує компанії про вживання додаткових заходів антивірусного захисту.

Інцидент “Технічний ризик” зустрічається у 1, 3, 4, 6, 7 секторах (рисунок 5.4). Не дивлячись на його розповсюдженість, рівень ризику не перевищує 0,50 та у більшості випадків є низьким. Тобто випадки втрат інформації, причиною яких є проблеми технічного характеру, зустрічаються в діяльності компанії, але не призводять до значних втрат.

В цілому варто зауважити, що загальний рівень ризику по кожній групі є незначним і коливається від 0,14 до 0,26, тобто ситуація, коли втрата інформації може відбуватися під впливом факторів п’ятьох інцидентів, є малоймовірною. Але треба звернути увагу на те, що такі ситуації є можливими та кількість таких випадків не буде перевищувати “5” (сектори 1 та 4 з рисунку 5.4).

Таким чином, проблема втрати інформації та знань є досить актуальною для різних суб’єктів економіки, оскільки втрачаючи інформацію, вони втрачають грошові кошти. Будь-які сучасні технології, наднове програмне та технічне забезпечення можуть також піддаватися впливу внутрішніх та зовнішніх факторів, пов’язаних з помилками дій користувачів, зовнішніми вірусними та хакерськими атаками, тощо. Тому вчасне реагування менеджменту компаній шляхом передбачення виникнення негативних інцидентів сприятиме зменшенню втрат. Запропонована методика дозволить вчасно та швидко провести експрес-оцінку та виявити рівень ризику втрат інформації в цілому та в розрізі інцидентів. Оскільки вона базується на формалізації фактичних даних про кількість випадків

та сум втрат по кожному фактору, то даний підхід якраз дозволить уникнути суб'єктивізму, який присутній в методиках компаній. Також існує реальний досвід застосування подібних підходів в процесі оцінки операційних ризиків банків, якій використовується в Національному банку України.

Позитивним є візуальна інтерпретація ризику втрат інформації та знань у вигляді карти ризиків, яка враховує кількість випадків та втрат, виводить інформацію за секторами з визначенням ризику по кожному інциденту та загального рівня для нього. Аналізуючи подібну карту, можна чітко визначити проблемні місця в компанії, які слугують причинами втрат інформації та знань. Використовуючи результати карти, можна спрогнозувати наслідки для компанії за умови отриманого рівня ризику. Для цього доцільно визначити сценарії, тобто за наявності певного рівня ризику та за умови відсутності кардинальних рішень в системі інформаційної безпеки компаній, які вони отримують варіанти розвитку подій, якщо збільшиться (зменшиться) кількість випадків та сум втрат.

Запропонований в роботі підхід не замінить цілком того комплексу заходів, які необхідно впроваджувати, щоб знизити рівень ризику втрати інформації для економічних агентів. Так, для зменшення ризику, причиною якого є людський фактор, суб'єктам економіки варто проводити регулярні тренінги для підвищення комп'ютерної грамотності користувачів, особливо для молодих та недосвідчених працівників. Також необхідно ознайомити працівників з процедурами роботи з інформацією. Важливо дотримуватися відповідності прав доступу користувачів до посадових інструкцій. Цей захід зменшує обсяги шахрайств, які персонал може здійснювати, маючи розширений обсяг прав доступу або паролі адміністраторів. Регулярний моніторинг дій користувачів допоможе виявити помилки в їх роботі.

Для зниження рівня ризику, який обумовлюють фактори технічного інциденту, слід вживати більш конструктивних заходів, таких як: використання твердотільних дисків замість жорстких, використання захисних пристроїв від перенапруги, генераторів, резервних акумуляторів, проведення систематичної чистки комп'ютерів, утримання пристроїв в спеціально обладнаних кімнатах,

використання пило- та влагозахисних корпусів, тощо. Для зниження ризиків, пов’язаних із пошкодженням програмного забезпечення, необхідно проводити безпечну процедуру блокування/розблокування, правильного відключення програмного забезпечення після кожного використання, здійснювати декілька методик тестування програмного коду, використовувати систематичне резервне копіювання та архівування інформації на додаткових серверах або зовнішніх носіях. Для зменшення впливу шкідливого програмного забезпечення та кримінального ризику, слід впроваджувати протиугінне програмне забезпечення на ноутбуках, здійснювати регулярне оновлення антивірусного програмного забезпечення та сканування файлів, перевірку прав доступу та ролей працівників в інформаційній системі компанії, тощо.

Узагальнення ключових аспектів методичних засад та результати експрес-оцінювання ризиків втрати інформації представлені на рисунку 5.5.

5.2 Розвиток підходу щодо вибору найбільш ефективної системи захисту інформації

Не залежно від суб’єкта інформаційної безпеки існує проблема зниження із часом рівня надійності його системи інформаційного захисту за рахунок збільшення різновидів кіберзагроз, що призводить до появи вразливостей інформаційної системи в цілому та порушення конфіденційності, цілісності та доступності даних. Як наслідок, державі стає важко контролювати інформаційні потоки, а економічні агенти втрачають клієнтів, фінанси, репутацію. Для суб’єктів економіки це відбувається, як правило, за рахунок втручання кіберзлочинців з метою викрадання інформації, яка стосується особистих даних клієнтів та банківської інформації – даних рахунків, транзакцій, платіжних карток тощо.

Визначення інцидентів та факторів впливу: HE – інциденти, обумовлені діями персоналу; VM – інциденти, пов'язані із вірусними атаками; TR – інциденти завдяки технічним несправностям; CR – інциденти, обумовлені незаконними діями кібер-злочинців; SC – інциденти, пов'язані з некоректною роботою програмного забезпечення. Для кожної групи обрано набір факторів впливу (66 од.)

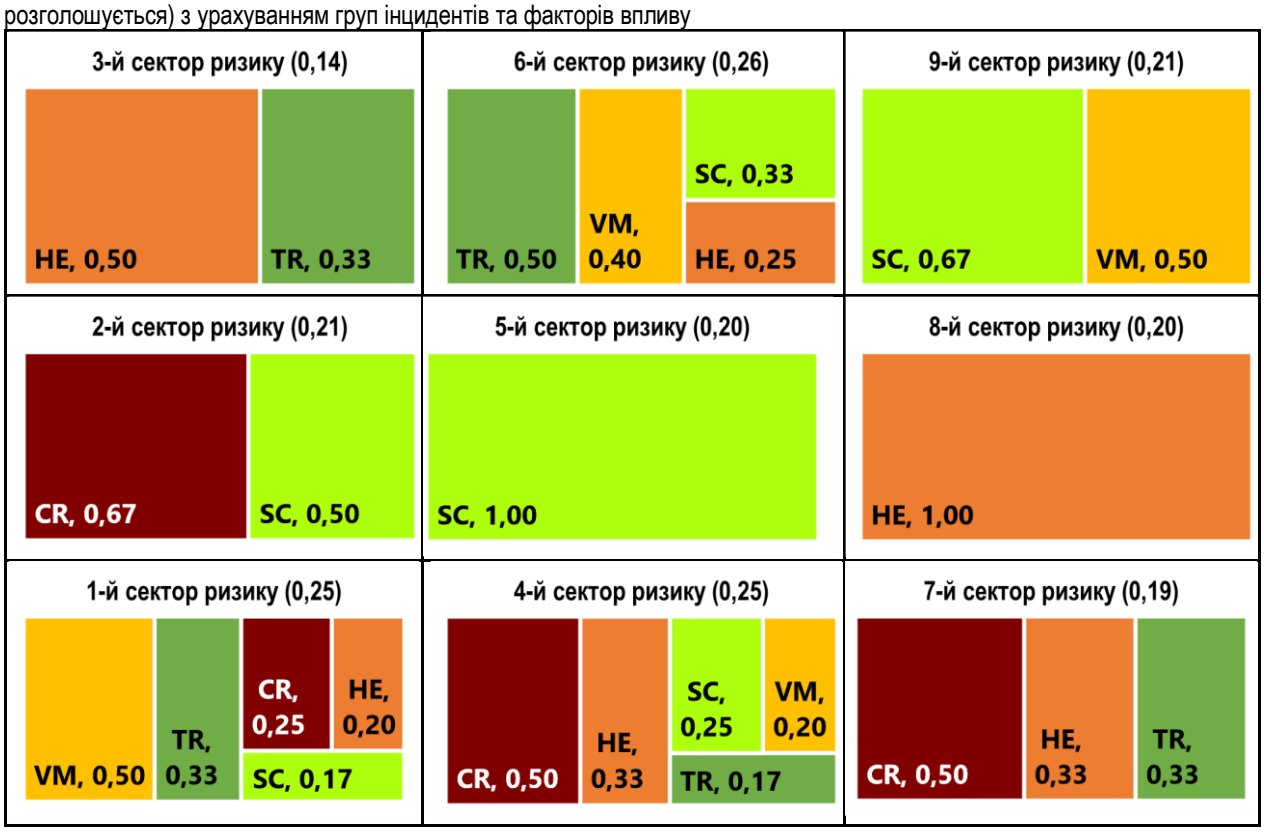
Визначення обсягів грошових втрат для кожного фактору та частоти повторення на основі фактичних даних: ведення статистики інцидентів щодо втрат, пов'язаних із відновленням даних після інциденту, та їх історичної ретроспекції

Формалізація факторів за допомогою бінарних характеристик і теорії множин, визначення загального рівня ризику за кожним із секторів, що відповідають розподілу інформації в карті ризику:

$$R_p = \sum_{i=1}^{k}\left(Z_{pi}|A_{pi} \geq 1 + \left[\frac{1}{n}\sum_{j=1}^{n} a^*_{pij}\right]|A_{pi} \geq 2\right) / \sum_{i=1}^{k}\left(Z_{pi} + \left[\frac{1}{n}\sum_{j=1}^{n} r_{pj}\right]\right),$$

де R_p – загальний рівень ризику за кожним *p*-м сектором (9 секторів карти ризиків); Z_{pi} – базова сукупність значень інцидентів ризику (1 – якщо $A_{pi} > 0$; 0 – якщо $A_{pi} = 0$; A_{pi} – ефект від впливу факторів на інцидент ризику (0 – випадки впливу фактору на *i*-й інцидент ризику (i = 1 ÷ k) відсутні; 1 – один випадок впливу; більше ніж 1 – компанія має проблеми в системі безпеки); r_{pj} – ранг *j*-го (j = 1 ÷ n) фактору, що впливає на *i*-й інцидент ризику, відібраний залежно від p-сектору карти ризиків; a^*_{pji} – скориговане формалізоване значення бінарної оцінки з урахуванням вагових коефіцієнтів; *[ ]* - ціла частина числа.

Результат: карта ризиків, побудована на даних суб'єкта господарювання реального сектору економіки (назва не розголошується) з урахуванням груп інцидентів та факторів впливу



Сектори карти ризиків 1-й, 2-й, 4-й: допустимі суми грошових збитків від втрати інформації та низька частота повторення.
Найбільш важливий тип інцидентів – CR (критичне значення – 0,67; 2-й сектор)

Сектори карти ризиків 3-й, 5-й, 7-й: критичні суми грошових збитків від втрати інформації з низькою частотою повторення; допустимі суми з високою частотою; середні значення сум та частот.
Найбільш важливий тип інцидентів – SC (критичне значення – 1,00; 5-й сектор)

Сектори карти ризиків 6-й, 8-й, 9-й: критичні суми грошових збитків від втрати інформації та висока частота повторення.
Найбільш важливий тип інцидентів: HE (критичне значення – 1,00; 8-й сектор); SC (критичне значення – 0,67; 9-й сектор)

За розрахунками ймовірність одночасного настання всіх інцидентів усіх груп є низькою (з імовірністю 0,14 – 0,26)

Рисунок 5.5 – Методичні засади та результати експрес-оцінювання ризиків втрати інформації (складено авторкою)

Окрім стороннього по відношенню до суб'єкта інформаційної безпеки втручання, поширеними є випадки здійснення внутрішніх кіберзлочинів, наприклад, з боку персоналу економічного агента. Особливо це трапляється серед тих працівників, які мають безпосередній доступ до бухгалтерської та фінансової інформації, а також при цьому вони мають необмежені права доступу до інформаційної системи. В тих компаніях, які використовують віддалений доступ, мобільні додатки, хмарні технології, також зростають ризики виникнення кіберінцидентів з боку інсайдерів. Тому будь-який суб'єкт економіки зацікавлений у створенні надійної системи інформаційного захисту, що дозволило б попереджати кіберзагрози та знизити його фінансові втрати.

Але практика свідчить про те, що не зважаючи на зростання обсягу інвестицій у побудову та розвиток інформаційної безпеки, поточні рішення для захисту даних не відповідають потребам бізнесу. Це підтверджують результати дослідження, проведеного компанією Dell Technologies, за результатами якого до такого висновку прийшли 81% респондентів [64]. Головною причиною цього є зростання обсягів інформації, якою володіють компанії. Так за 2019 рік її обсяг зріс майже на 40% по відношенню до 2018 року, при цьому орієнтована загальна вартість втрати даних зросла до понад 1 млрд. доларів на одну організацію за останні 12 місяців [64]. Інформація є цінним ресурсом, втрата якого впливає на всі бізнес-процеси компанії. Згідно дослідження "X-Force Threat Intelligence Index 2020", проведеного компанією IBM та опублікованого у 2020 році, 60% первинних проникнень у інформаційну систему компанії відбувалося за рахунок облікових даних, вкрадених раніше, або вразливостей програмного забезпечення [260]. Так, у 2019 році близько 29% випадків трапилося за рахунок викрадення облікової інформації, що призвело до втрати 8,5 млрд. записів, якими заволоділи кіберзлочинці. Також у 30% випадків ними було використано вразливості системи, що збільшилось у порівнянні з 2018 роком на 22% [260].

Проблема, пов'язана з підвищенням рівня ефективності системи кібербезпеки компаній є глобальною, оскільки середній розмір фінансових втрат від зломів та витоків інформації на червень 2019 року для підприємств

середнього бізнесу світу склав близько 3,92 млн. дол. [5]. Тому компанії зацікавлені у залученні новітніх технологій з метою забезпечення надійності та безпеки інформації. Так, найбільше застосування у 2019 році знайшли такі технології, як: хмарні додатки (58%); штучний інтелект та машинне навчання (53%); додатки «програмне забезпечення як послуга» (51%); інфраструктура 5G та гранична хмарна інфраструктура (49%); інтернет речей (36%) [64]. Але оскільки проблема існує та не зменшуються наслідки від неї, то відповідно існує потреба у залученні інших підходів, хоча за опитуванням 71% респондентів вважають, що нові технології створюють більшу складність захисту даних, тоді як 61% заявляють, що нові технології становлять ризик для захисту даних [64].

Тобто існує дилема, з одного боку, зростання кількості та різноманіття загроз потребують впровадження нових технологій, з іншого боку, цей крок може призвести до додаткових фінансових втрат, а також не вплинути на ефективність системи захисту від зовнішніх та внутрішніх загроз. Тому з метою обґрунтування процесів, пов’язаних із ребілдингом систем інформаційної безпеки, та доведення ефективності використання новітніх технологій з метою протидії витоків інформації пропонується методологічний підхід на основі системно-динамічного моделювання. Перевагою цього методу є його можливість моделювати поведінки систем на високому рівні, виходячи з їх інформаційно-логічної структури та на основі потокового підходу. Широкого застосування метод системної динаміки набув для моделювання будь-яких процесів. Наприклад, Січко Т. його використовував для моделювання бізнес-процесів [359], Сердюк В. застосував його для моделювання стратегічного розвитку [358], Шамрін Р. обґрунтував його можливості для моделювання економічних систем [375], Шевчук Я. запропонував на його основі модель розвитку міст та регіонів [377], Половцев О. описав його можливості для моделювання динаміки соціальних систем [346], та інші. Тобто системно-динамічне моделювання є універсальним методом, який можна використовувати для дослідження різного роду об’єктів та систем. Саме тому пропонуємо методологію системно-динамічного імітаційного моделювання для порівняння

технологій для захисту інформації та обґрунтування ефективності ребілдингу системи інформаційного захисту (рисунок 5.6).

Рисунок 5.6 – Методологія системно-динамічного імітаційного моделювання для порівняння систем захисту інформації (складено авторкою)

Запропонована методологія може застосовуватися для будь-яких суб'єктів інформаційної безпеки – держави, економічних агентів, та передбачає виконання наступних етапів (рисунок 5.6).

На *першому етапі* приймається рішення відповідальними особами щодо необхідності ребілдингу системи інформаційної безпеки, що є наслідком зростання кількості інформаційних загроз, витрат на відновлення інформації та обслуговування системи захисту.

На *другому етапі* обирається відповідний захід або технологія ребілдингу системи з урахуванням її вартісних та функціональних характеристик. З цією

метою можна використати систему підтримки прийняття рішення, яка дозволить обрати за параметрами найкращі варіанти. Запропоновану у даному дисертаційному дослідженні методологію було реалізовано для порівняння традиційної інформаційної системи із можливостями захисту та блокчейн-технології, яка найкращим чином зарекомендувала себе у фінансовій сфері.

Інвестиції в розробників корпоративних блокчейн-рішень у 2019 році сягнули майже 434 млн. дол., що перевищує на 62% інвестиції 2018 року [43]. Ця статистика свідчить про зростання попиту на дану технологію. Аналітична платформа CB Insights виділила 58 галузей, які є потенційними для застосування блокчейн, серед яких також зазначено й напрямок кібербезпеки [43]. Також фахівці компанії Goldman Sachs вважають, що за рахунок впровадження даної технології в процесі передачі даних відбуватиметься зниження ймовірності кіберзлому. Це можливо за рахунок того, що блокчейн передбачає відкритість реєстрів, просунуті методи криптографії, має потужні засоби кіберзахисту у порівнянні з традиційними системами [28]. Оскільки фахівці-практики вбачають значні її перспективи, то це й вплинуло на її вибір для реалізації запропонованої в дисертації методології.

На *третьому етапі* відбувається розробка діаграми причинно-наслідкових зв'язків. З цією метою було виділено основні її елементи, виходячи з двох категорій впливу: 1) внутрішніх та зовнішніх кіберзагроз: несанкціонований доступ; копіювання, знищення та зміна інформації; користувацькі помилки; навмисне незбереження інформації та ін.; 2) засобів попередження кіберзагроз, реалізованих за допомогою технологій, що порівнюються: заборона на використання зовнішніх носіїв, завантаження інформації, відкриття та запуск невідомих файлів, обмеження доступу користувачів; рівень доступу користувачів; наявність віддаленого доступу; рівень відкритості бази даних та ін. Також виділяємо додаткові елементи, які виступатимуть джерелом впливу (намір людини здійснити кіберзлочин); реакцією на кіберінцидент (запис інформації у блокчейн та базу даних традиційної інформаційної системи); а також функції користувача, політика компанії та вразливості системи. Між елементами встановлюються причинно-наслідкові зв'язки, які у сукупності із

ними формують параметри системи. Причинно-наслідковий зв'язок є позитивним, якщо збільшення (зменшення) параметру впливає на збільшення (зменшення) того параметру, на який впливають, або від'ємним у випадку, коли збільшення (зменшення) параметру впливає на зменшення (збільшення) того параметру, на який впливають.

На *четвертому етапі* відбувається розробка діаграми потоків за допомогою виділення рівнів, тобто таких параметрів, на які здійснюють вплив більша кількість інших з урахуванням їх позитивної та від'ємної дії. При цьому необхідно врахувати спеціальні параметри, які викликають збільшення або зменшення відповідного рівня. Також можуть використовуватися додаткові змінні та константи.

На *п'ятому етапі* задаються початкові значення параметрів системи та здійснюється симуляція або тестове моделювання. З цією метою встановлюються граничні (максимальні та мінімальні) значення початкових параметрів, які показують стан системи в результаті намірів людини здійснити кіберзлочин. Змін потребують наступні параметри: заборона на завантаження інформації, заборона на відкриття та запуск невідомих файлів, заборона на використання зовнішніх носіїв, обмежений доступ, апаратні помилки, відкритість бази даних, наявність віддаленого доступу. Якщо виникає потреба, то можна провести відладку відповідних рівнів. Далі здійснюється симуляція, результатом якої є візуалізація поведінки системи, коли є потенційні наміри здійснити кіберзагрози та ймовірні реакції системи. Моделювання відбувається з урахуванням двох випадків: запису всієї інформації у блокчейн (використання нової технології) або фіксування тільки окремих повідомлень у агрегатному вигляді (використання традиційної інформаційної системи). Результат симуляції також показує реакцію системи на її вразливості в результаті використання блокчейн-технології та традиційної інформаційної системи.

На *шостому етапі* проводиться оцінка результатів та приймається рішення щодо вибору технології.

Запропоновану методологію було апробовано для модифікованих даних компанії, назва якої не розголошується у зв'язку із дотриманням комерційної

таємниці, та для якої проводилося обґрунтування застосування блокчейн-технології для захисту інформації у порівнянні із традиційною інформаційною системою. Системно-динамічне моделювання було проведене у програмному середовищі Vensim, яке використовується у наукових цілях задля здійснення такого роду моделювання [251]. В результаті було побудовано діаграму причинно-наслідкових зв'язків (рисунок 5.7), яка відображає логіку функціонування потоків між елементами системи.

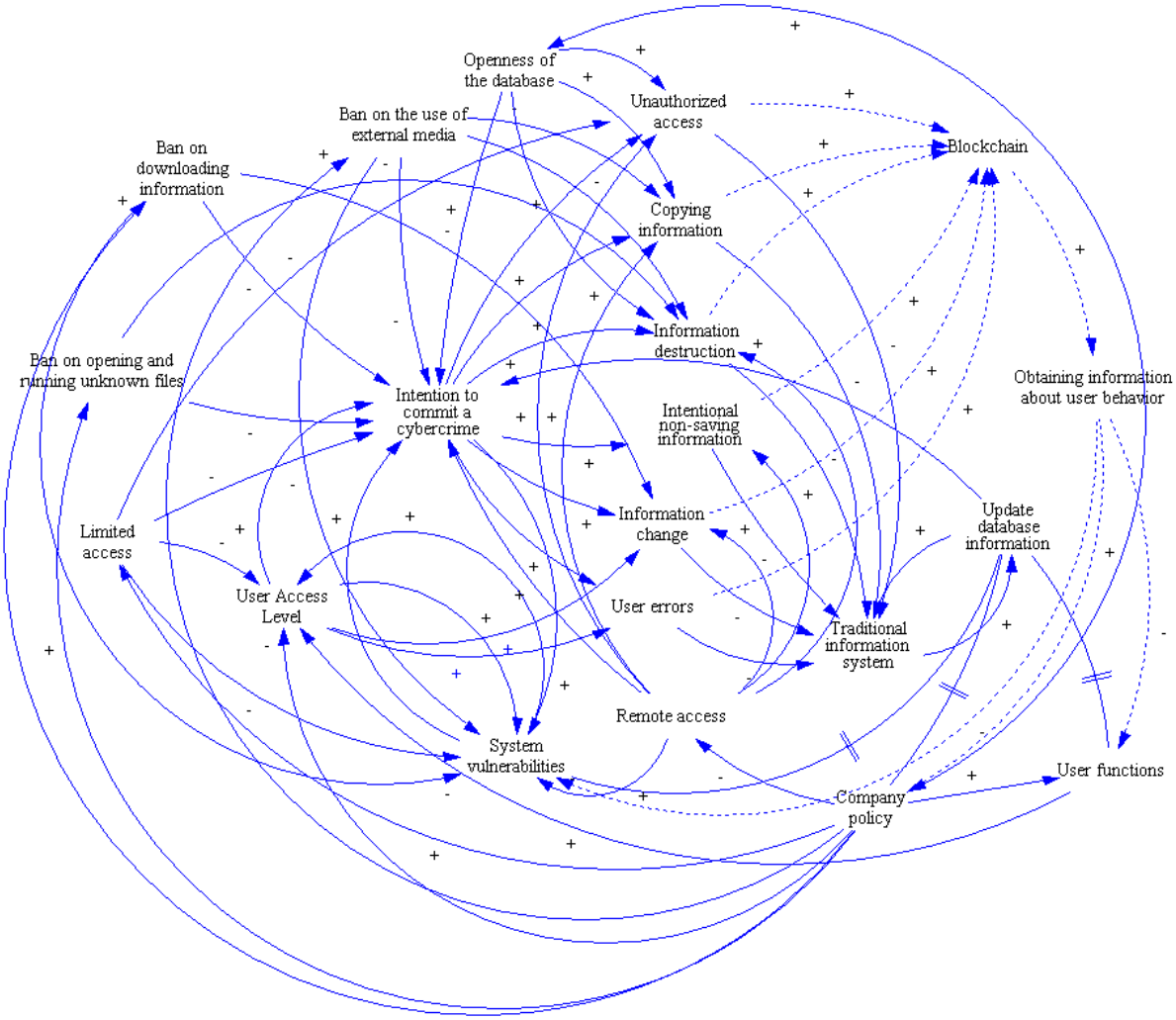


Рисунок 5.7 – Діаграма причинно-наслідкових зв'язків (складено авторкою)

Так, головним елементом є «Намір здійснити кіберзлочин» («Intention to commit a cybercrime»), який виникає у людини. На стан цього елементу впливають фактори, такі як заборона на завантаження інформації («Ban on

downloading information»), заборона на відкриття та запуск невідомих файлів («Ban an opening and running unknown files»), заборона на використання зовнішніх носіїв («Ban on the use of external media»), обмежений доступ («Limited access»), рівень доступу користувача («User Access Level»), відкритість бази даних («Opening of the database»), наявність віддаленого доступу («Remote access»). В залежності від стану цих факторів, намір може збільшуватися, якщо користувач знає або про відсутність таких заборон, або має безмежні права доступу, тощо. Намір може зменшуватися у випадках, коли підприємство має високий рівень захисту, встановлює різні заборони, надає права доступу у відповідності до функціональних обов'язків працівника, тощо. Модель передбачає, що кіберзлочинець має намір вкрасти інформацію шляхом її копіювання, або знищення даних, або змінення інформації, або здійснення навмисного незбереження даних, або несанкціонованого доступу, або викривлення інформації шляхом допущення помилок. Перераховані незаконні дії обрано як найбільш розповсюджені незаконні дії, які сприяють появі вразливостей системи та зниженню рівня її кібербезпеки. Якщо технологія блокчейну буде впроваджена у компанію, то вона передбачає, що всі дії записуються до блокчейну та не підлягають жодним змінам. Відповідно, використовуючи систему штучного інтелекту, дані з блокчейну можуть швидко надати інформацію про поведінку користувачів та, як результат, виявити порушення. Системно-динамічна модель передбачає, що запис також може відбуватися і в інформаційній системі, але якщо відбуватиметься оновлення інформації, то запис в системі не буде зберігатися у первинному вигляді. Службі кібербезпеки знадобиться досить тривалий час на перевірку журналів активностей, щоб виявити порушення. Також в залежності від результатів змінюється й політика компанії, функції користувачів та стан вразливостей системи, що, в свою чергу, впливають на намір здійснення кіберзлочину. Чим жорсткіші ці умови, тим наміри злочинця слабшають.

Також було отримано діаграму потоків (рисунок 5.8), при побудові якої було використано математичний апарат, представлений формулою (5.10),

позначення якої відповідають позначенням елементів рисунку 5.8.

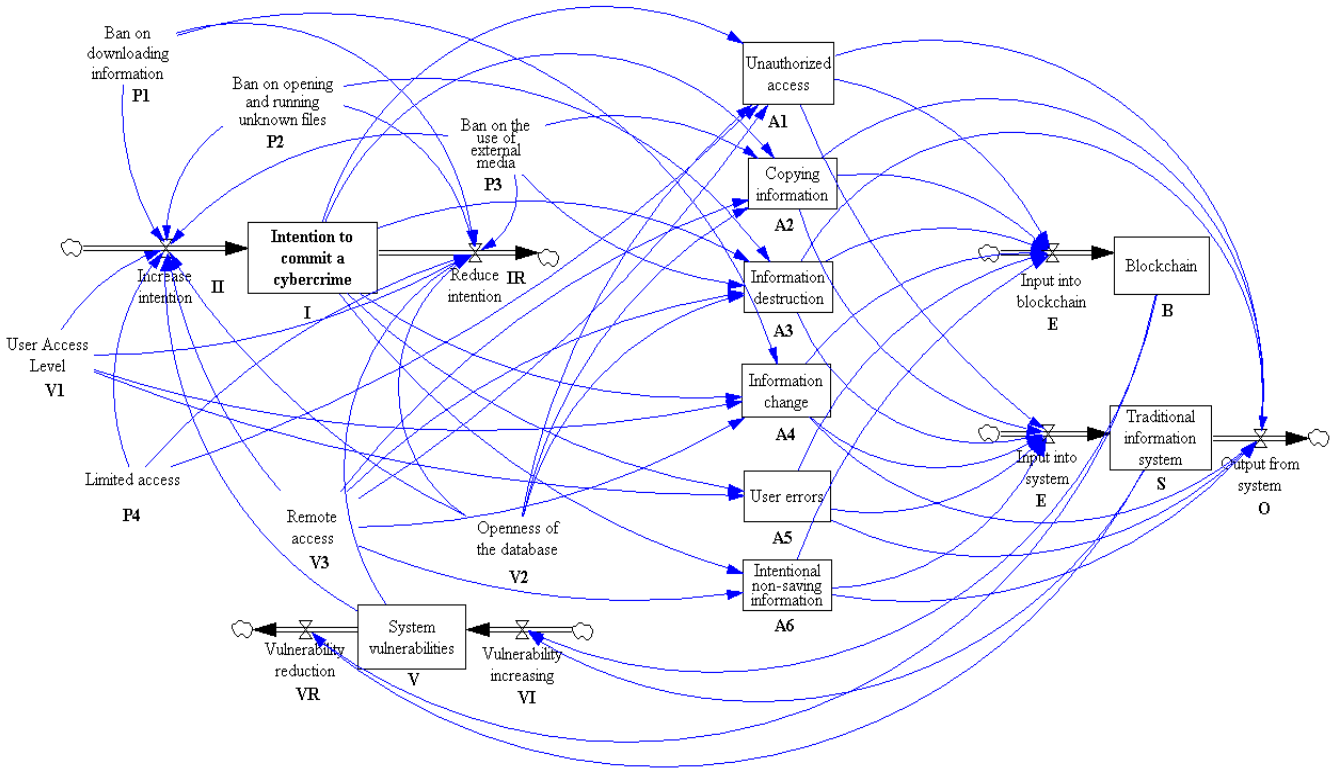


Рисунок 5.8 – Діаграма потоків (складено авторкою)

$$
\begin{cases}
\dfrac{dI}{dt} = \big(II(t) - IR(t)\big)\,|_{\,II(t)>IR(t)} \;\vee\; \dfrac{dI}{dt} = \big(IR(t) - II(t)\big)\,|_{IR(t)>II(t)} \\
II(t) = \dfrac{1}{1 + EXP\Big(-\big(0.50288 \;-\; 2.75474 \;*\; (P_1 + P_2 + P_3 + P_4) + 4.8164 * (V(t) + V_1 + V_2 + V_3)\big)\Big)} \\
IR(t) = 1 - II(t) \\
A_1(t) = 1\,|_{\,V_2 \geq 0.5 \;\vee\; V_3 \geq 0.5 \;\vee\; P_4 < 0.5 \;\vee\; I(t) \geq 0.5} \;\vee\; A_1(t) = 0\,|_{V_2 < 0.5 \;\vee\; V_3 < 0.5 \;\vee\; P_4 \geq 0.5 \;\vee\; I(t) < 0.5} \\
A_2(t) = 1\,|_{P_3 < 0.5 \;\vee\; V_2 \geq 0.5 \;\vee\; V_3 \geq 0.5 \;\vee\; I(t) \geq 0.5} \;\vee\; A_2(t) = 0\,|_{P_3 \geq 0.5 \;\vee\; V_2 < 0.5 \;\vee\; V_3 < 0.5 \;\vee\; I(t) < 0.5} \\
A_3(t) = 1\,|_{P_2 < 0.5 \;\vee\; P_3 < 0.5 \;\vee\; V_2 \geq 0.5 \;\vee\; V_3 \geq 0.5 \;\vee\; I(t) \geq 0.5} \;\vee\; A_3(t) = 0\,|_{P_2 \geq 0.5 \;\vee\; P_3 \geq 0.5 \;\vee\; V_2 < 0.5 \;\vee\; V_3 < 0.5 \;\vee\; I(t) < 0.5} \\
A_4(t) = 1\,|_{\,P_1 < 0.5 \;\vee\; V_1 \geq 0.5 \;\vee\; V_3 \geq 0.5 \;\vee\; I(t) \geq 0.5} \;\vee\; A_4(t) = 0\,|_{P_1 \geq 0.5 \;\vee\; V_1 < 0.5 \;\vee\; V_3 < 0.5 \;\vee\; I(t) < 0.5} \\
A_5(t) = 1\,|_{I(t) \geq 0.5 \;\vee\; V_1 \geq 0.5} \;\vee\; A_5(t) = 0\,|_{I(t) < 0.5 \;\vee\; V_1 < 0.5} \\
A_6(t) = 1\,|_{I(t) \geq 0.5 \;\vee\; V_3 \geq 0.5} \;\vee\; A_6(t) = 0\,|_{I(t) < 0.5 \;\vee\; V_3 < 0.5} \\
E(t) = A_1(t) + A_2(t) + A_3(t) + A_4(t) + A_5(t) + A_6(t) \\
\dfrac{dB}{dt} = \left(\dfrac{1}{2} + \dfrac{1}{2} * \left[\dfrac{1}{6} * E(t)\right]|_{E(t) \geq 2}\right)|_{E(t) \geq 1} \;\vee\; \dfrac{dB}{dt} = 0\,|_{E(t) < 1} \\
O(t) = A_1(t) + 4 * A_2(t) + 2 * A_3(t) + 3 * A_4(t) + 5 * A_5(t) + 6 * A_6(t) \\
\dfrac{dS}{dt} = \left(\dfrac{1}{4} + \dfrac{1}{4} * \left[\dfrac{1}{6} * O(t)\right]|_{E(t) \geq 2}\right)|_{E(t) \geq 1} \;\vee\; \dfrac{dS}{dt} = 0\,|_{E(t) < 1} \\
\dfrac{dV}{dt} = \big(VI(t) - VR(t)\big)\,|_{VI(t)>VR(t)} \;\vee\; \dfrac{dV}{dt} = \big(VR(t) - VI(t)\big)\,|_{VR(t)>VI(t)} \\
VI(t) = 1\,|_{B(t)>0.5 \;\vee\; S(t)>0.5} \;\vee\; VI(t) = 0\,|_{B(t) \leq 0.5 \;\vee\; S(t) \leq 0.5} \\
VR(t) = 1\,|_{B(t) \leq 0.5 \;\vee\; S(t) \leq 0.5} \;\vee\; VR(t) = 0\,|_{B(t)>0.5 \;\vee\; S(t)>0.5} \\
P_1, P_2, P_3, P_4, V_1, V_2, V_3 \in [0,1]
\end{cases}
\tag{5.10}
$$

В результаті було проведено симуляцію, для чого було змінено значення початкових параметрів (P_1, P_2, P_3, P_4, V_1, V_2, V_3) та узято їх 128 комбінацій граничних значень ([0,1]). Значення таких параметрів, як заборона на завантаження інформації, заборона на відкриття та запуск невідомих файлів, заборона на використання зовнішніх носіїв, обмежений доступ дорівнювало 1, що свідчить про наявність встановлених заборон та обмежень, або 0, тобто їх відсутність у компанії. Значення для апаратних помилок, відкритості бази даних, наявності віддаленого доступу дорівнювало 1 у випадку, якщо ці параметри є типовими для системи, та 0, якщо ці параметри відсутні. Симуляція відбувалася на однаковому проміжку часі. В результаті було зібрано 128 випадків поведінки системи для використання блокчейн-технологій та традиційної інформаційної системи. Результат симуляції представлений на рисунку 5.9.

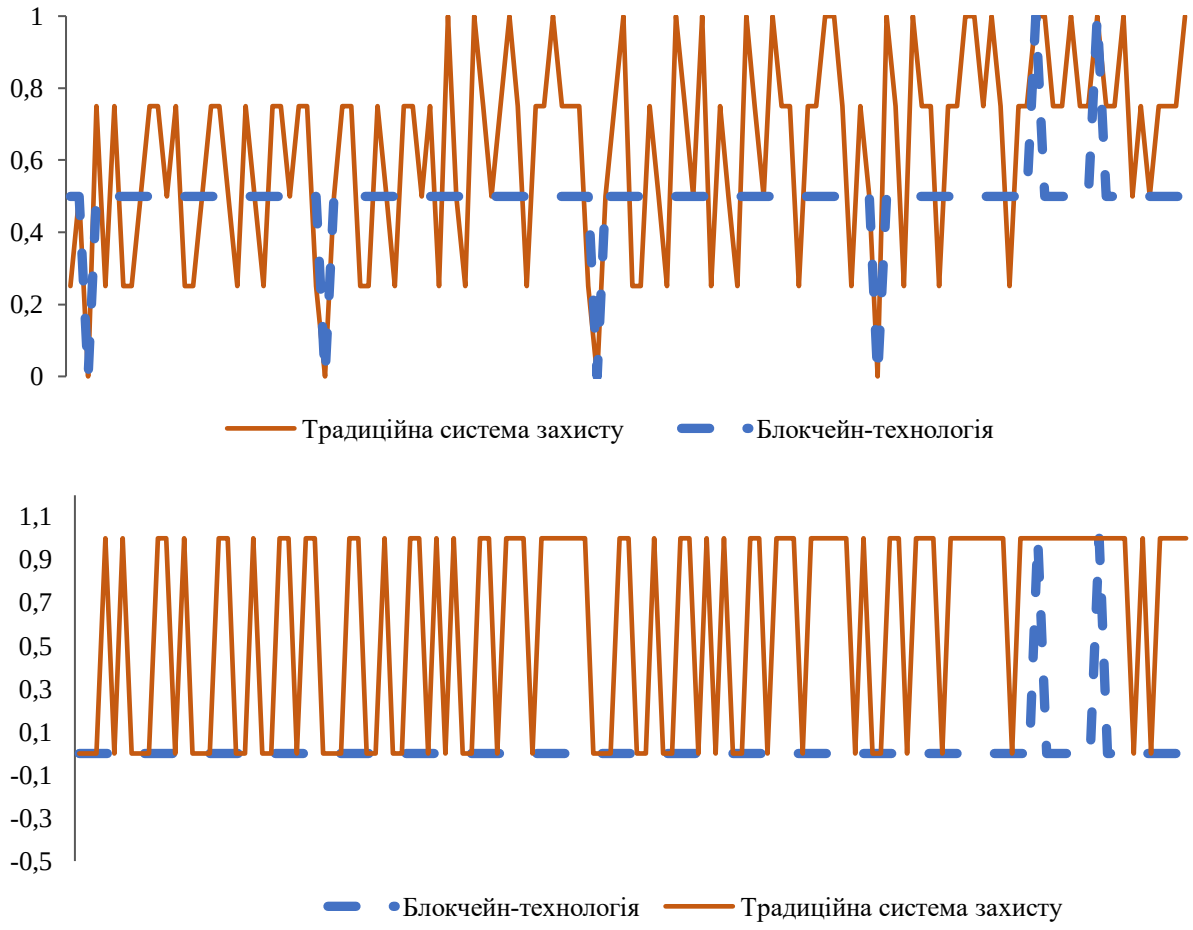


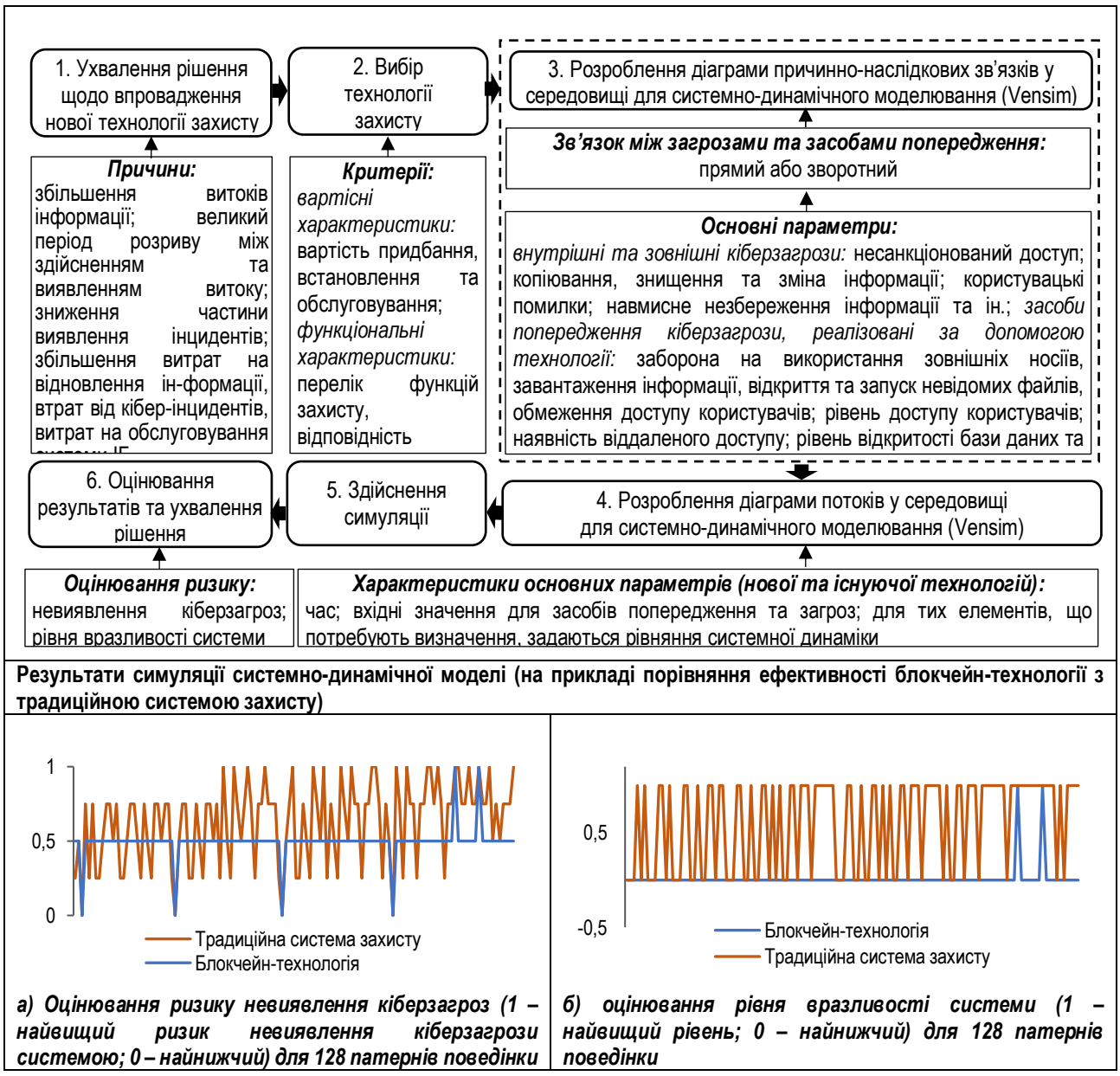
Рисунок 5.9 – Результати моделювання (складено авторкою)

На верхньому графіку рисунку 5.9 представлено рівень ризику, який визначає система, що використовує блокчейн-технологію, та традиційна інформаційна система. За реалізованою методикою, якщо значення наближається до 0, тим нижче ризик не виявити кіберзлочинну активність, якщо значення наближається до 1, ризик є вищим. Тобто практично у всіх випадках система, що використовує технологію блокчейн має рівень ризику нижчий, ніж традиційна інформаційна система. Випадки, в яких обидві системи мають рівень ризику рівний 1, це випадки, коли компанія не встановлює заборони, надає необмежений доступ користувачам, тобто це варіант, коли відсутні всі заходи безпеки. Відповідно, в цьому випадку жодна технологія не спроможна позитивно вплинути на систему кіберзахисту. Тобто ризик невиявлення кіберзагроз (визначено як середнє значення отриманих результатів поведінки системи, представлених на верхньому графіку рисунку 5.9) блокчейн-технологією дорівнює 0,49, а для традиційної системи – 0,63, що говорить про більшу ефективність нової технології.

На нижньому графіку рисунку 5.9 представлений результат впливу виявлених даних на вразливості системи. Значення, яке дорівнює 0, свідчить про зменшення вразливостей, 1 – про їх збільшення. Тобто, застосування блокчейн-технології дозволить зменшити вразливості системи практично у більшості випадків (98,44%), а застосування традиційної інформаційної системи тільки в частині (39,06%). Тобто, застосування блокчейнів є більш ефективним (на 59,38%) в порівнянні із традиційними системами, що позитивно сприятиме на надійність системи кіберзахисту компанії у випадку її впровадження.

Узагальнення результатів та етапів запропонованої методології представлено на рисунку 5.10

Таким чином, проблеми, пов’язані із порушенням надійності системи інформаційної безпеки не залежно від суб’єкта економіки, є актуальними. Наслідками можуть бути втрати фінансових ресурсів, довіри клієнтів, зниження репутації, рівня конкурентоздатності для економічних агентів; зниження стабільності економічної, політичної та соціальної сфер для держави.



а) Оцінювання ризику невиявлення кіберзагроз (1 – найвищий ризик невиявлення кіберзагрози системою; 0 – найнижчий) для 128 патернів поведінки

б) оцінювання рівня вразливості системи (1 – найвищий рівень; 0 – найнижчий) для 128 патернів поведінки

Рисунок 5.10 – Методологія та результати системно-динамічного імітаційного моделювання для порівняння систем захисту інформації (складено авторкою)

Тому фахівці із кіберзахисту повинні вчасно реагувати у випадках появи нових видів кіберзагроз або збільшення ймовірності появи вразливостей в системі. Унікальних інструментів, які допоможуть повністю вирішити проблеми кіберзахисту не існує. Тобто це повинен бути комплекс заходів, які сприятимуть ефективності та надійності системи захисту. Більшість компаній збільшують інвестиції в напрямку застосування сучасних технологій, що засуджується деякими фахівцями. На нашу думку, це правильний підхід, тому що зростання

обсягів інформації, рівня обізнаності людини в питаннях застосування сучасних технологій та пристроїв, вимагають нових та нестандартних підходів. На сьогодні технологія блокчейн нарощує темпи використання та розширює сфери застосування. Тому є досить гарна перспектива щодо її використання для підвищення рівня надійності системи кіберзахисту в компаніях. Запропонована в роботі методологія системно-динамічного моделювання порівняння систем захисту інформації дозволяє зімітувати роботу системи та обґрунтувати переваги обраної технології над традиційними інформаційними системами вже на етапі її вибору. Слід зазначити, що вибір блокчейн для інформаційного захисту можна розглядати не як стовідсоткову альтернативу, а як додатковий захід, оскільки його головна прерогатива – це зберігання інформації у первинному вигляді без змін, що дозволить виявляти відхилення при спробі їх здійснення.

5.3 Формування системи попередження фінансових кіберзагроз

За оцінками експертів серед галузей, які найбільше потерпають від кіберзлочинців, перше місце займає банківський сектор, друге – енергетичний та добувний сектор, третє – телекомунікаційний. Так, у 2017 році від фішингових атак найбільшої шкоди зазнали 51,7% банків в порівнянні з електронною комерцією та платіжними системами – представниками фінансового сектору [237].

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

темпами модернізації способів та інструментів шахраїв. Відповідно рівень протидії загрозам поступається рівню зростаючих загроз.

За статистичними даними ЕМА (Української міжбанківської асоціації членів платіжних систем), сума збитків громадян внаслідок дій шахраїв із платіжними картками у 2017 році досягла 670 млн.грн., що значно перевищує збитки за попередні роки – 339,13 млн.грн. (2016 р.), 181,00 млн.грн. (2015 р.), 90,00 млн.грн. (2014 р.). Збільшилася також і середня сума втрат від одного шахрайства із використанням методів соціальної інженерії. Так, у 2017 році ця сума склала 2543,00 грн. проти 1403,00 грн. у 2016 році та 834,00 грн. у 2015 році [364].

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

Одним із головних напрямків боротьби із шахрайством, зазначеним у Постанові НБУ №95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» від 28 вересня 2017 року, є впровадження банками основних технічних систем [347]: виявлення атак; моніторингу події управління інцидентами; контролю доступу до мережі; захисту електронної пошти; запобігання атак, спрямованих на відмову в обслуговуванні; антивірусного захисту; двофакторної автентифікації. Але роз’яснення щодо їх створення, впровадження, фінансування, тощо, відсутні. Тобто перед банками поставлена задача, а її виконання – це вже

прерогатива власників, при цьому спостерігається нехватка спеціалістів в галузі кібербезпеки, що ускладнює виконання задачі.

До вирішення такої складної проблеми треба підходити системно, та ключем її рішення має бути розвиток та комплексне удосконалення автоматизованих інформаційних технологій та систем у поєднанні із математичними методами. Так, в сфері інтеграції автоматизованих та математичних методів для банківської сфери багато зроблено працівниками американської компанії в галузі бізнес-аналітики “SAS Institute”, результатом чого стають програмні розробки для банківського сектору [206].

Також можна виділити роботу в цьому напрямку компанії “Kaspersky Lab”, яка багато років розробляє програмні рішення для антивірусного захисту та інтернет-безпеки, а також здійснює статистичні дослідження видів, способів, типів шахрайств для різних сфер економіки [242].

В умовах зростання кількості та різновидів інформаційних та кіберзагроз для забезпечення функціонування ефективної системи інформаційної безпеки будь-якого суб’єкту економіки слід застосовувати комплекс програмно-технічних, інформаційних та організаційних заходів. Тільки їх системне поєднання дозволить сформувати надійну систему захисту, яка буде не тільки виявляти наслідки, але й попереджувати загрози. Тому вкрай важливим є розуміння сутності та структури процесів забезпечення безпеки інформації, особливо тих, що стосуються заходів перевірок стосовно виявлення порушень цілісності, конфіденційності даних або наслідків кібершахрайств та кіберзагроз.

Пропонуємо розробку трирівневої системи попередження фінансових кіберзагроз, яку буде реалізовано для банківських установ та яка буде охоплювати організаційний, інформаційний та алгоритмічний рівні, заходи кожного з яких будуть спрямовані на виявлення ознак кіберзагроз на етапі, що передує здійсненню зовнішніх та внутрішніх загроз. Концептуальна модель даної системи представлено на рисунку 5.11.

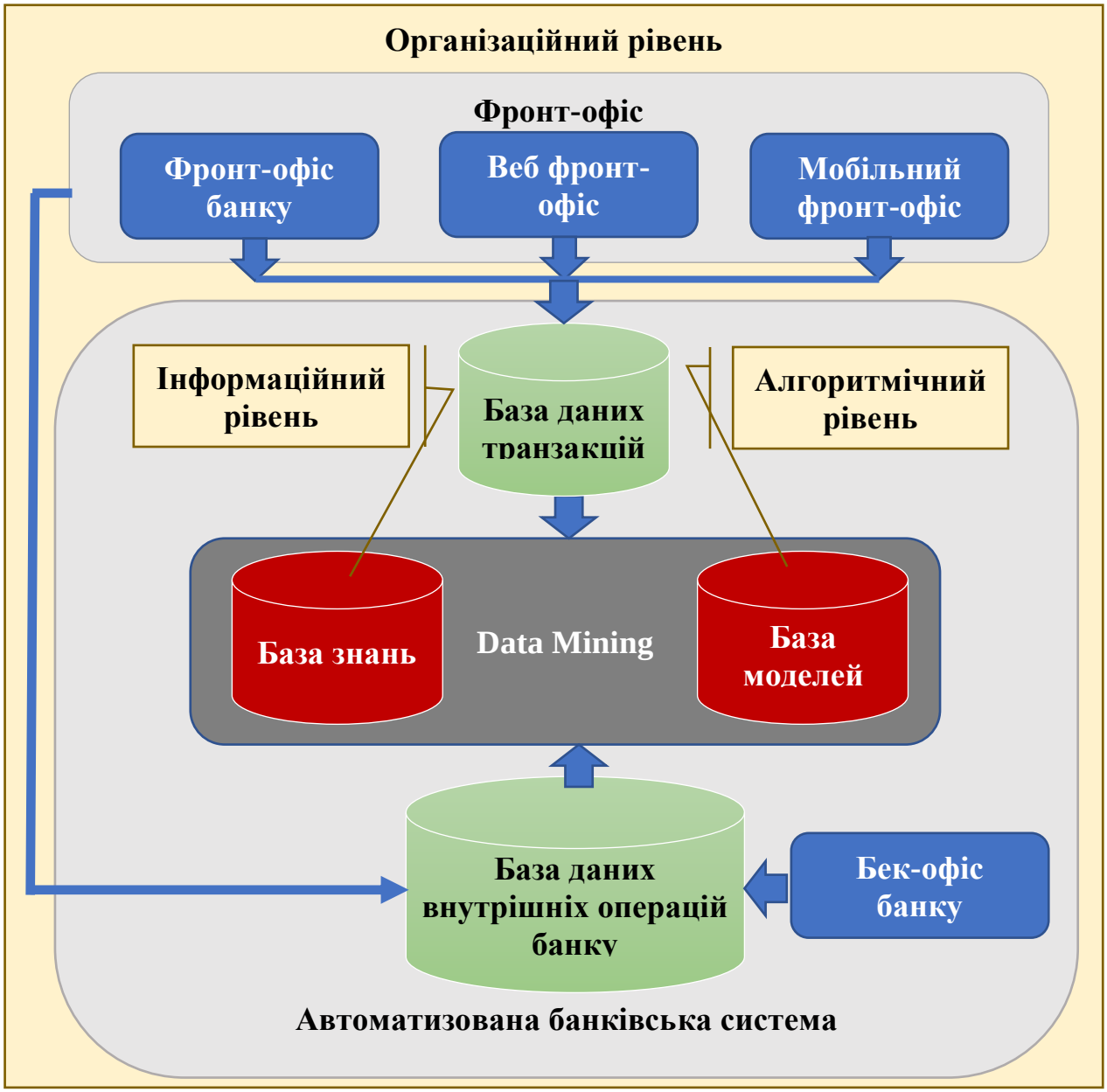


Рисунок 5.11 – Концептуальна модель трирівневої системи попередження фінансових кіберзагроз (складено авторкою)

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

відслідковування ознак шахрайств) (рисунок 5.11). Його головне призначення – виявляти потенційні фінансові кіберзагрози незалежно від природи ініціатора (зовнішнього – клієнта банку та його операцій “База даних транзакцій”, чи внутрішнього – персоналу банку та його операцій “База даних внутрішніх операцій банку”). Операції перевіряються на відповідність певним критеріям, які визначають, чи має операція ознаки кібершахрайської, які сформовані у базі знань та правил з урахуванням накопичених статистичних даних, чи не має. Означені процеси перевірки відбуваються з урахуванням заходів організаційного рівня, на якому відбувається оптимізація бізнес-процесів інформаційного захисту, що дозволяє виявляти слабкі місця в системі захисту інформації. Виходячи з окреслених завдань трьох рівнів, розробимо конкретні пропозиції для їх реалізації.

Організаційний рівень системи попередження кіберзагроз.

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

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

Так, на *першому кроці* будується модель процесу на основі нотації BPMN 2.0, яка є стандартом бізнес-моделювання, що враховує попроцесний підхід. Тобто будь-яка діяльність компанії розглядається не з позиції функцій, з якими вона пов’язана, а з позицій учасників та їх дій, які вони здійснюють протягом певного періоду часу. Це дозволяє бачити – хто виконує, що робить, по

відношенню до чого (кого) діє, протягом якого періоду, чим керується. Відповідно в процесі побудови моделі повинні визначатися:

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

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

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

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

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

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

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

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

На *третьому етапі* проводиться симуляція за різними типами – “Аналіз часу” та “Аналіз ресурсів”. Результати “Аналіз часу” надають інформацію щодо мінімального, максимального та середнього часу по кожній операції, а також загального часу, витраченого на заданий обсяг симуляції. Так, отримане значення середнього часу по кожній з операцій дозволить виявити слабку ланку, пов’язану із відхиленням від показників по типовим операціям, що сприятиме в подальшому оптимізації даної ділянки процесу.

Також можна отримати інформацію щодо кількості операцій, отриманих на виході та здійснених на кожному вузлі моделі. Так, дана кількість визначатиметься за формулою (5.11):

$$NO_{out} = (((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil) - \lceil p_3^- \times ((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil)\rceil) - \cdots - \lceil p_n^- \times ((((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil) - \lceil p_3^- \times ((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil)\rceil) - \cdots - \lceil p_{n-1}^- \times ((((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil)) - \lceil p_3^- \times ((N_0 - \lceil p_1^- \times N_0 \rceil) - \lceil p_2^- \times (N_0 - \lceil p_1^- \times N_0 \rceil)\rceil)\rceil) - \cdots \rceil \quad (5.11)$$

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

N_0 – кількість операцій на початку симуляції;

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

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

⌈ ⌉ – округлення кількості операцій до найближчого цілого у більший бік.

У випадку моделювання основних бізнес-процесів системи інформаційної безпеки рекомендується визначати коефіцієнт результативності за формулою (5.12), який відображатиме якість її роботи:

$$KR = \frac{NO_{out}}{N_0}, \tag{5.12}$$

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

Системи, які використовують банки для фінансового моніторингу, можуть блокувати операції, які при подальшій їх перевірці не виявляють ознаки відмивання кримінальних доходів. Це можна пояснити тільки тим, що використовуються непрозорі критерії перевірки, тому система автоматично відносить такі транзакції в категорію підозрілих. Використання індексу (5.12) дозволить накопичувати статистику результативності системи та у випадку помилкового відбору операцій здійснювати коригування критеріїв перевірок.

Результати симуляції "Аналіз ресурсів" надають інформацію щодо завантаженості кожного з виду задіяних ресурсів та їх вартості. Це дозволяє сформувати уявлення щодо фінансових витрат, пов'язаних із виконанням даного процесу. Якщо задіяно декілька учасників (ресурсів), то можна визначити

відповідні витрати на кожного з них окремо та порівняти вартісні показники у випадку вибору альтернатив, що дозволить визначити шляхи економії.

На *четвертому етапі* проводиться оптимізація бізнес-процесу шляхом внесення змін та коректувань у модель, які будуть враховувати слабкі місця, виявлені в результаті здійснення симуляції на попередньому кроці. Тобто будується модель “ЯК БУДЕ”, яка буде відображати бажані елементи процесу. Далі здійснюється процес налаштування симуляції (другий етап) та сама симуляція (третій етап). Отримані результати порівнюються із результатами для моделі “ЯК Є”. Це стосується даних часу та вартості ресурсів. Якщо значення показників покращилися, то отримана модель буде вважатися придатною для практичного використання. Якщо показники після оптимізації не змінилися у найкращий бік, то оптимізацію проводимо ще раз. Це відбуватиметься доти, доки результати моделювання не будуть придатними для практичного застосування.

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

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

По-перше, банківську установу розглядаємо як складну систему, складовими якої виступають внутрішнє середовище: персонал, менеджмент банку, його власники, автоматизована банківська система (АБС); та зовнішнє середовище: клієнти, кіберзлочинці, пов’язані особи, програмно-технічні пристрої. Тобто банк – це система взаємозв’язаних суб’єктів та об’єктів внутрішнього та зовнішнього середовища. До складу системи будь-якої природи

входять елементи різного рівня надійності, які можуть вторгнутися в певний момент за певних умов, що може призвести до порушення її функціонування, а також порушення конфіденційності, цілісності та цінності інформації. По суті кожен з цих елементів може стати джерелом загрози безпеки інформації, потенційного шахрайства або ініціатором, або співучасником, або бути опосередковано залученим.

По-друге, різні дослідження в сфері банківського шахрайства розглядають в основному зовнішнє середовище як ініціатора шахрайства або порушення інформаційної безпеки, що є не зовсім коректно. 80% від усього обсягу інцидентів пов’язано із персоналом банку. Тому можливості вторгнення повинні враховувати також і внутрішні аспекти загрози.

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

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

Проводимо моделювання тих процесів, які задіяні безпосередньо у системі банківської безпеки. На рисунку 5.12 представлено бізнес-модель процесу ідентифікації та верифікації клієнта, яка є придатною у випадку здійснення дистанційних операцій. Вона вже є результатом “ЯК БУДЕ”.

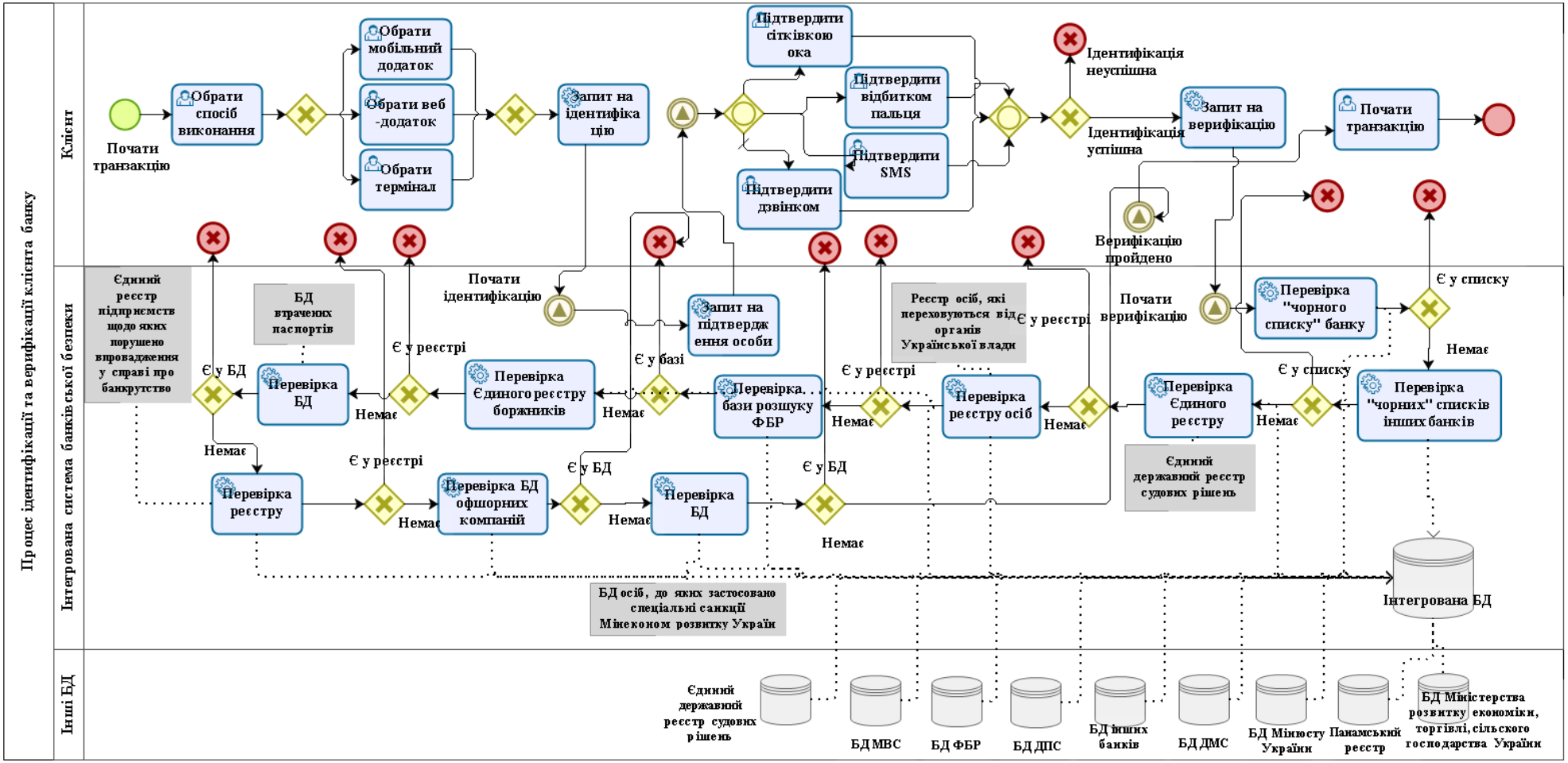


Рисунок 5.12 – Бізнес-модель процесу ідентифікації та верифікації клієнта в інтегрованій системі банківської безпеки (складено авторкою)

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

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

Після успішного підтвердження, починається другий етап – верифікація, тобто здійснюється перевірка клієнта на наявність у (рисунок 5.12): «чорному списку» банку, де він є клієнтом, та у «чорних списках» інших банків; реєстрі судових рішень по клієнту; реєстрі осіб, які переховуються від органів української влади; базі розшуку ФБР; Єдиному реєстрі боржників; базі даних втрачених паспортів; базі даних офшорних компаній; Єдиному державному реєстрі підприємств, щодо яких порушено впровадження у справі про банкрутство; базі даних осіб, до яких застосовано спеціальні санкції Мінеконом розвитку України. Якщо клієнт успішно проходить верифікацію, то система надає йому дозвіл на здійснення операції, в протилежному випадку система його блокує та повідомляє відповідні органи безпеки.

Результати проведеної симуляції для даного бізнес-процесу представлені на рисунку М.1 у додатку М. В якості умов симуляції було задано: кількість

операцій – 1000; ймовірність відхилення операції у випадку не проходження перевірки – 1% по кожному вузлу (бажаний показник); час на виконання операцій в інтегрованій системі банківської безпеки – 1 с. (це максимальний час на виконання 1 запиту у будь-якій системі) [284]; для операцій ідентифікації час виставлявся, виходячи із власних замірів максимального часу в процесі користування мобільним банкінгом. В результаті отримано, що середній час на ідентифікацію та верифікацію клієнта за умови впровадження даної схеми на практиці буде дорівнювати 69,75 с. Кількість операцій після перевірки – 903 (формула 3.16). Коефіцієнт результативності – 0,903 (формула 3.17). Тобто за умови визначення 1% операцій такими, які носять ознаки шахрайських по кожному з критеріїв перевірки, система буде ідентифікувати після верифікації та ідентифікації 90,3% операцій як таких, що пройшли моніторинг.

Після проходження ідентифікації та верифікації пропонується перевірка операцій у відповідності із їх сумами. Якщо сума транзакції перевищує 400 000 грн., то банк зобов'язаний здійснити її моніторинг за критеріями на предмет легалізації кримінальних доходів [298]. В протилежному випадку, рекомендується перевірити на наявність ознак шахрайства. Це актуально в умовах зростання кількості постраждалих від соціальної інженерії. Так, на 4 квартал 2019 року цей вид злочинності у поєднанні із шкідливим програмним забезпеченням використовувався у 54%. Для приватних осіб соціальна інженерія склала 67%, для приватних – 62%. При чому для різних компаній його доля є значною: для державних компаній – 66%, промислових – 88%, фінансових організацій – 94%, IT-компаній – 50%, торгівля – 36% [269].

На практиці установи зобов'язані здійснювати моніторинг, але процес перевірки організується банками самостійно. Тому більшість з них його проводить вручну. Згідно із Постановою НБУ №65 від 19.05.2020 «Про затвердження Положення про здійснення банками фінансового моніторингу» налаштування та автоматизацію відповідних процесів банки повинні організувати до 30.06.2021 року [348].

Науковці різних країн світу пропонують власні підходи до організації автоматизованого моніторингу. Так, авторським колективом Чен З., Ван Хоа Л.Д., Тео Е.Н. , Назір А., Каруппія Е.К., Лам К.С. досліджено техніки машинного навчання, як засіб протидії відмивання коштів [45]. Авторами Гао С., Сю Д., Ванг Х., Грін П. розроблено мультиагентну систему з використанням технології інтелектуальних агентів, яка може бути інтегрована в бізнес-процеси банку для виявлення операцій, пов'язаних з відмиванням грошей [96]. Робота Дівії Е. та Умадеві П. присвячена розробці інформаційної моделі, яка базується на аналізі потоку транзакцій, що дозволяє здійснювати кластеризацію банківських операцій з точки зору ймовірності відмивання грошей [239].

Цікавий підхід представили у своїй роботі Калдера Х., Хейн Д. та Шерлок К., які запропонували платіжну систему з доповненим автоматизованим функціоналом протидії відмиванню незаконно отриманих коштів, яку було ними запатентовано [41]. Колхаткар Д., Фатнані С., Яо Ю. та Мацумото К. представили та запатентували багатоканальну систему протидії легалізації коштів для платіжних карт, яка здійснює моніторинг операцій у режимі реального часу [146]. В роботі Діонісія С. Деметиса розглянуто сучасний напрямок реалізації сучасних систем протидії відмиванню коштів (Anti-money laundering), які базуються на підходах визначення ризиків [71]. У дослідженні Коельо Р., Де Сімоні М. та Преніо Дж. представлений новий напрямок “Suptech”, який є передовим інструментом збору даних та їх аналізу на основі штучного інтелекту та машинного навчання, який застосовується у боротьбі з легалізацією кримінальних доходів [53]. У праці Йонг Лі висвітлені аспекти технічної реалізації AML-інформаційних систем, особливо планування їх впровадження, проектування, аналізу поточного та майбутнього стану, деяких технічних рішень та практичних підходів [266].

Не дивлячись на значний вклад закордонних вчених у вирішення проблеми протидії відмивання коштів, вітчизняна наука відстає в питанні створення, розвитку, удосконалення інформаційних систем та технологій моніторингу, які використовуються для виявлення кримінальних доходів в процесі їх легалізації.

Тому вирішення даного питання є досить актуальним для економіки та наукової спільноти України. Практичного досвіду вітчизняних банків пропонується бізнес-модель процесу первинного фінансового моніторингу банку, який здійснюється в умовах автоматизованої обробки інформації (рисунок 5.13).

Запропонована модель (рисунок 5.13) демонструє здійснення автоматизованого моніторингу за 13-ма показниками. Якщо операція не проходить хоча б одну із запрограмованих перевірок, система її блокує та вводить до бази даних запис про ризик, пов'язаний із здійсненням даної транзакції, після чого дані надсилаються до Держфінмоніторингу. У разі проходження транзакцією всіх етапів перевірки, приймається рішення щодо обслуговування клієнта та ухвалення даної операції.

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

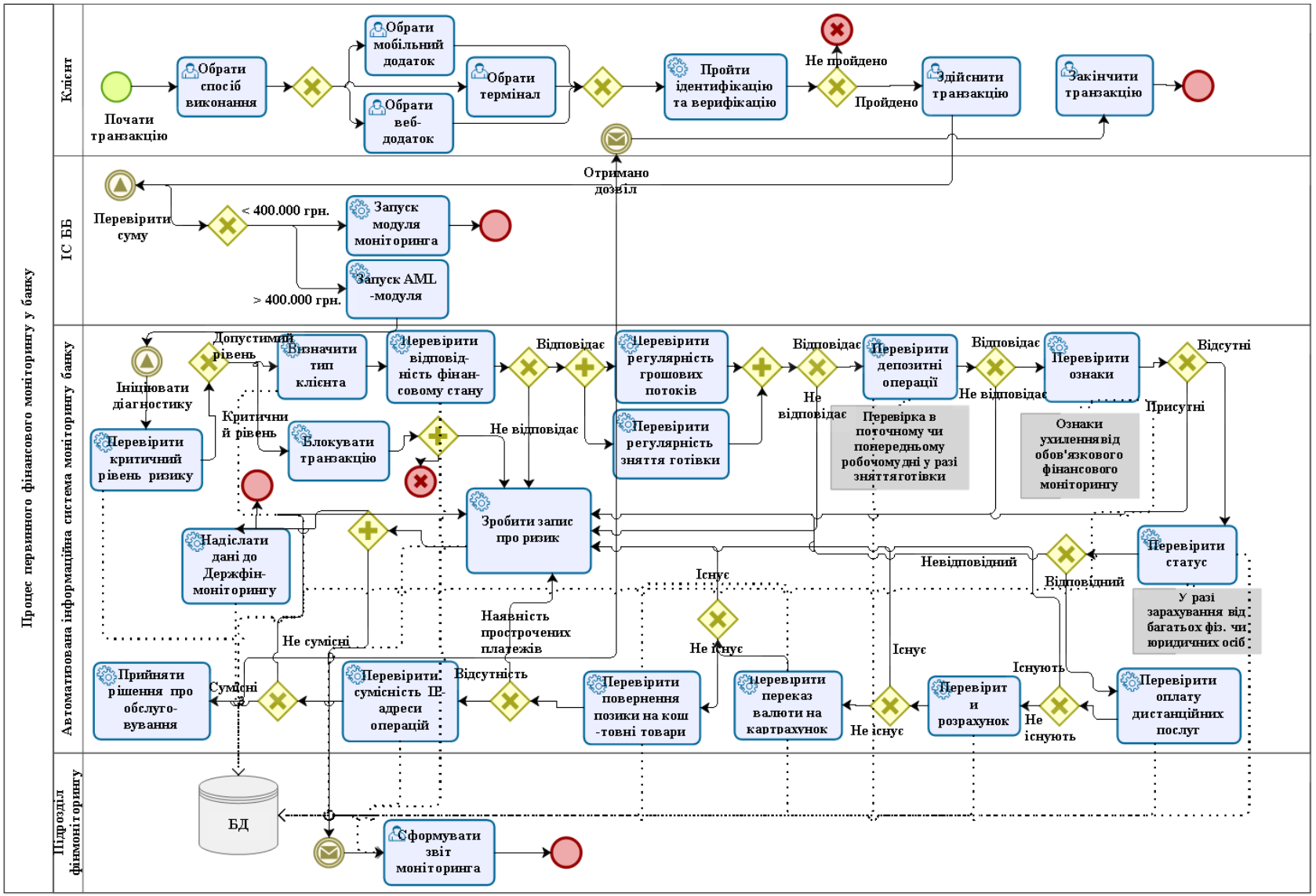


Рисунок 5.13 – Бізнес-модель процесу автоматизованого фінансового моніторингу банку (складено авторкою)

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

При здійсненні симуляцій враховуються два важливих твердження:

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

2) симуляції результатів здійснюємо, виходячи з автоматизованої та ручної обробки даних, оскільки запропоновані бізнес-процеси мають вже елементи оптимізації, тобто процеси, реалізовані на практиці є вже застарілими та прогнозуються удосконалюватися, виходячи із дотримання норм законодавства.

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

Кількість операцій після перевірки – 877, розрахованих за формулою (3.16),

коефіцієнт результативності – 0,877 (за формулою (3.17)). Тобто за умови 1% операцій, які носять ознаки відмивання кримінальних доходів, по кожному з критеріїв перевірки, система буде позитивно ідентифікувати 87,7% операцій, що є високим результатом.

Проведемо симуляцію по ресурсам. Для цього задаємо фахівця, який здійснює моніторинг, та автоматизовану інформаційну систему фінансового моніторингу (AML-модуль). Визначимо їх вартісні оцінки, а саме вартість людино-години та машино-години. Для розрахунків використаємо дані, які відображають фактичні витрати азіатських банків, понесені на AML-систему (AML – Anti-Money Laundering – протидія відмиванню коштів), які за принципами роботи у даному напрямку схожі з українськими. Інформація міститься у звіті компанії LexisNexis та охоплює період 09.2015 – 01.2016 [240]. Розрахунки наведені у таблиці 5.5:

Таблиця 5.5 – Розрахунки вартості людино-години та машино-години

Назва показника	Фактичне значення, узяте із звіту [240]	Розраховане значення
Кількість опитаних компаній	210	X
Кількість опитаних банків	50%	105
Витрати на AML по всім банкам, дол. США	1500000000	X
Середні витрати на 1 банк, дол. США	X	14285714,29
Витрати на програмне та технічне забезпечення (зовнішні та внутрішні), дол. США	19%	2714285,71
Витрати на персонал, задіяний в AML, дол. США	81%	11571428,57
Час функціонування AML-системи за рік за умови 24-годинної роботи, год.	X	8760
Вартість машино-години, дол. США	X	309,85
Вартість людино-години, дол. США	X	1320,94

Наведені у таблиці 5.5 розрахунки показують вартість машино-години, якщо задіяно увесь комплекс програмно-технічних засобів, та вартість людино-години, якщо задіяно увесь штат працівників. Оскільки значення вартісних показників є комерційною таємницею для банків, то можна скористатися тільки умовним визначенням витрат. Але й ці розрахунки можуть дати уявлення про ефективність. Використовуючи отримані значення вартості машино-години та людино-години, проведемо симуляцію «Аналіз ресурсів», результат якої представлений на рисунку 5.14.

Scenario information

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

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

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

Рисунок 5.14 – Результати симуляції за ресурсами для бізнес-процесу автоматизованого фінансового моніторингу банку (складено авторкою)

Результати, представлені на рисунку 5.14, показують, що витрати на 1000 транзакцій, перевірених фахівцями фінансового моніторингу, у 4,26 разів вище, ніж витрати на 1000 транзакцій, перевірених AML-модулем. Можна зробити висновок, що при реалізації запропонованого бізнес-процесу фінансового моніторингу, його ефективність буде вищою для автоматизованого варіанту, ніж

для ручного. Для остаточних розрахунків важливо мати інформацію щодо витрат на придбання та впровадження такої системи, а також мати інформацію щодо її результативності.

Перед тим, як побудувати модель бізнес-процесу перевірки транзакцій на наявність ознак кібершахрайств, необхідно сформувати інформаційну модель виявлення ознак шахрайств для операцій, ініційованих зовнішнім середовищем, яка відображає функціонування інформаційних потоків у автоматизованому середовищі. Модель (рисунок 5.15) побудовано у нотації DFD (data flow diagrams), яка є одним із інструментів структурного моделювання та проектування інформаційних систем, із використанням програмного забезпечення “All Fusion Process Modeller” [12].

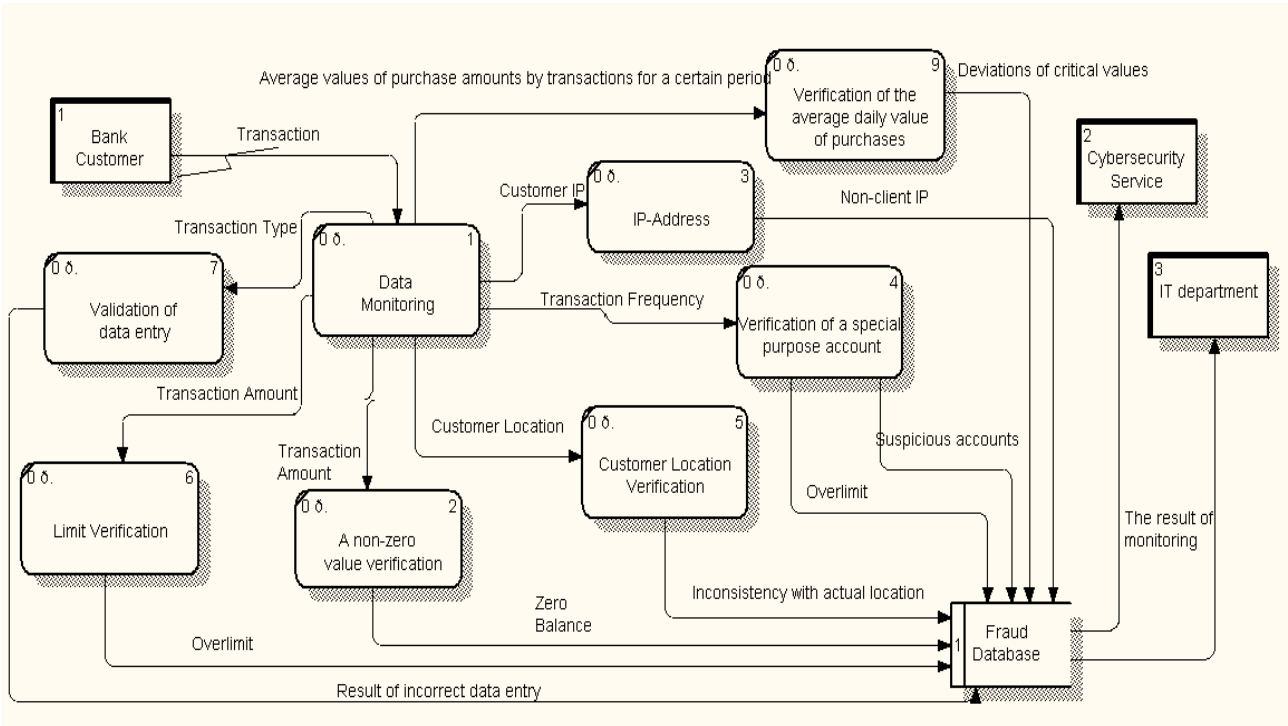


Рисунок 5.15 – Інформаційна модель виявлення ознак шахрайств клієнтів (складено авторкою)

Побудована на рисунку 5.15 модель відображає інформаційні потоки, які будуть задіяні в модулі перевірки (моніторингу) транзакцій для виявлення ознак шахрайств та їх попередження. Це відбувається шляхом перевірки банківської транзакції (“Transaction”), яку здійснює клієнт (сутність “Bank Customer”), із

використанням функцій “Data Monitoring” (перевірка даних). Перевіряються:

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

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

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

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

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

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

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

Інформація щодо ймовірні порушення, шахрайства, зламування надходить до бази даних шахрайств (“Fraud Database”), обробляється. Результати

моніторингу (“The Result of Monitoring”) передаються відділам IT (“IT Department”) та кібербезпеки банку (“Cybersecurity Service”).

У відповідністю із запропонованою інформаційною моделлю (рисунок 5.15) розроблено бізнес-модель процесу перевірки транзакцій на наявність ознак кібершахрайств у нотації BPMN 2.0 (рисунок 5.16).

Процес виглядатиме наступним чином (рисунок 5.16): клієнт банку або потенційний шахрай здійснює вхід до системи або з використанням веб-сайту, або мобільного пристрою, або терміналу; якщо він успішно пройшов ідентифікацію та верифікацію, система в залежності від суми транзакції буде перевіряти або на предмет відмивання коштів, або на ознаки шахрайства. Система перевіряє операцію на наявність ознак шахрайства із застосуванням модулю моніторингу за критеріями, які представлені на рисунку 5.16. Якщо результат перевірки не виявляє ознак потенційного шахрайства, то система дозволяє здійснити операцію та клієнт її завершує; якщо результат перевірки виявляє ознаки шахрайства, система робить запит на підтвердження операції шляхом sms-повідомлення або дзвінка, або іншим способом; клієнт здійснює додаткову аутентифікацію; якщо операція була ініційована клієнтом, то її успішно буде завершено; у випадку, якщо клієнт виявиться шахраєм, тобто він не зможе пройти додаткову аутентифікацію, його буде заблоковано та проінформовано систему безпеки.

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

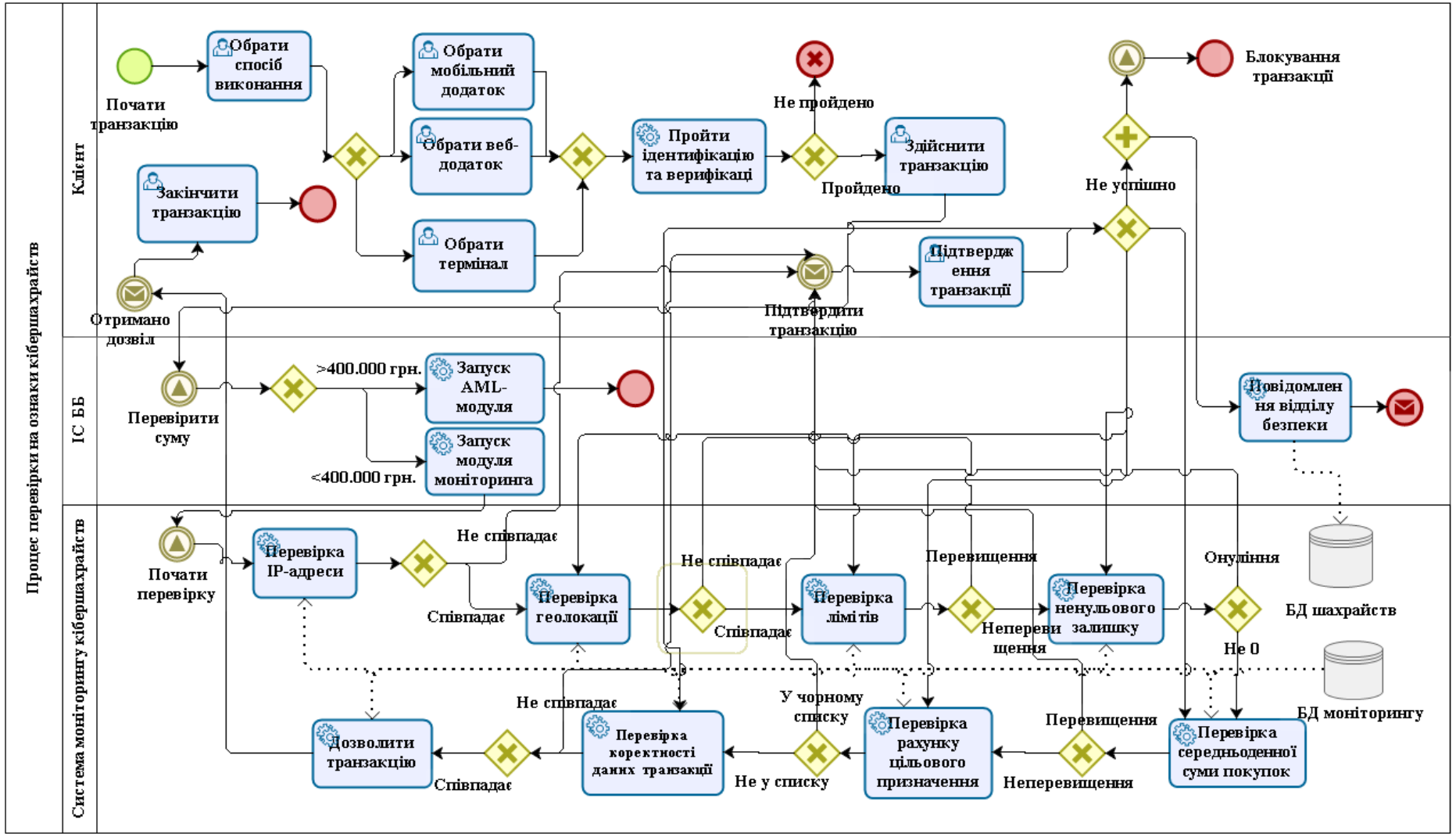


Рисунок 5.16 – Бізнес-модель процесу перевірки транзакцій на наявність ознак кібершахрайств (складено авторкою)

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

Проведемо симуляцію процесу по ресурсах. Для цього визначимо собівартість людино-години та машино-години. У звіті компанії Deloitte зазначається, що у 2020 році банки здійснювали витрати на інформаційну безпеку в розмірі від 0,6% всіх витрат, що склало приблизно 9,4% від IT-бюджету або $2688 на 1 людину на рік [23]. Виходячи із того, що у 2020 році було 251 робочий день, та беручи до уваги 8-годинний робочий день, визначаємо, що вартість 1 машино-години буде дорівнювати $1,34: $2688 / (251 днів * 8 годин). Для порівняння даного процесу із ручною обробкою визначаємо, що заробітна плата банківського аналітика в Україні дорівнює 17500 грн. на місяць [361]. Виходячи із того, що у 2020 році було 251 робочий день, та беручи до уваги 8-годинний робочий день, визначаємо, що вартість 1 машино-людини буде дорівнювати $1,34: $2688 / (251 днів * 8 годин).

Результати проведеної симуляції по ресурсах представлено на рисунку 5.17, де можна побачити, що у разі забезпечення практично 100% виконання транзакцій автоматизованою системою та аналітиком, витрати ресурсів для першого варіанту є меншими у 2,79 разів. Тобто економічно доцільним є здійснення перевірки із використанням автоматизованого модулю (3,27 дол. витрат на 1000 операцій) у порівнянні із здійсненням перевірки фахівцем (9,12 дол. витрат на 1000 операцій).

Що стосується випадків внутрішніх шахрайств, то також було розроблено інформаційну модель виявлення шахрайства, якщо шахраєм виступає персонал банку, тобто інсайдери (рисунок 5.18).

Scenario information

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

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

Scenario information

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

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

Рисунок 5.17 – Результати симуляції за ресурсами для бізнес-процесу перевірки транзакцій на наявність ознак кібершахрайств (складено авторкою)

Модель, представлена на рисунку 5.18, відображає інформаційні потоки, які циркулюють в процесі перевірки модулем моніторингу (“Data Monitoring”) операцій (“Bank operation”), що здійснюються персоналом банку (“Staff”) на предмет виявлення ознак шахрайства. Перевіряються:

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

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

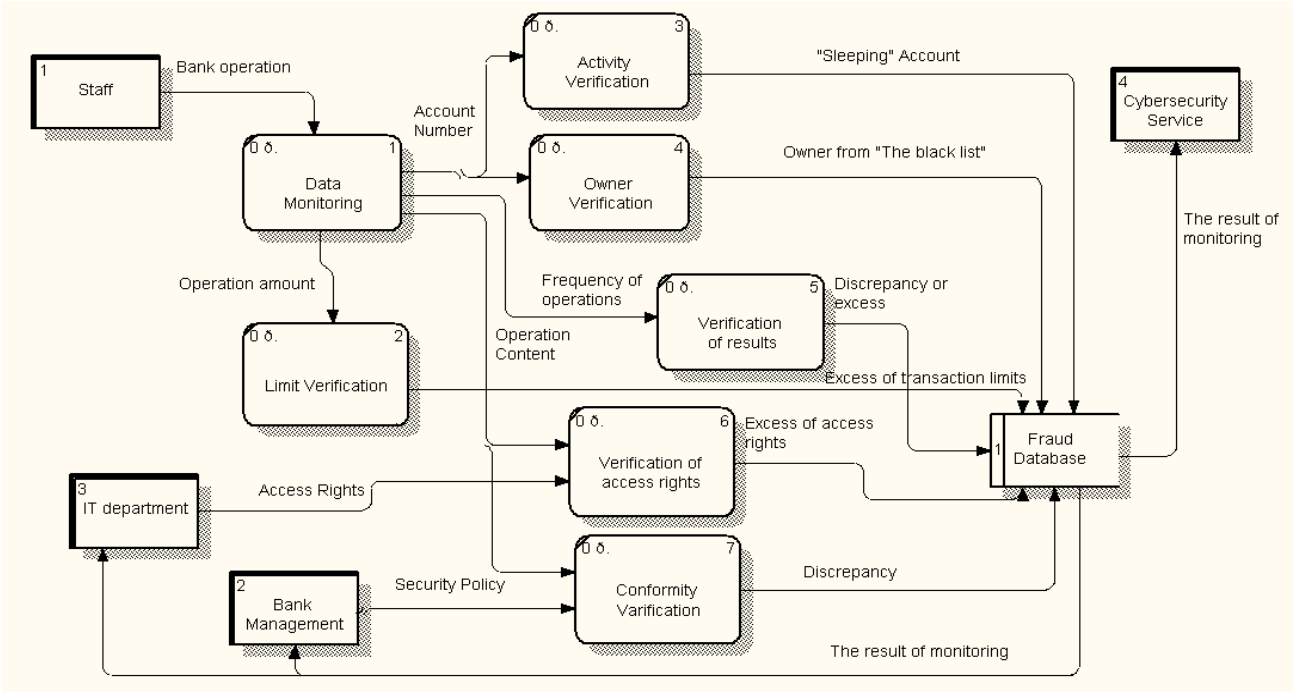


Рисунок 5.18 – Інформаційна модель виявлення ознак шахрайств персоналу банку (складено авторкою)

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

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

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

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

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

У відповідністю із запропонованою інформаційною моделлю (рисунок 5.18) розроблено схему процесу здійснення операції персоналом з урахуванням її перевірки на ознаки шахрайства у нотації BPMN 2.0 (рисунок 5.19).

Процес виглядатиме наступним чином:

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

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

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

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

По даному процесу було проведено симуляції по витратам часу та ресурсів (рисунок М.4 у додатку М). За умовами: кількість операцій – 1000; ймовірність відхилення операції у випадку не проходження перевірки – 1% по кожному вузлу (бажаний показник); час на виконання 1 запиту в автоматизованій системі – 1 с. Виявлено, що середній час на перевірку 1 транзакції на предмет наявності ознак кібершахрайств з боку інсайдерів дорівнює 6,86 с., тобто на 1000 операцій буде витрачено 1,90 год. Було виявлено 65 операцій з ознаками шахрайств, відповідно показник результативності системи складає 93,5%. Результати симуляції по ресурсам (рисунок 5.20) показують, що ефективність автоматизованого виявлення ознак кіберзагроз є менш витратним в 2,79 разів.

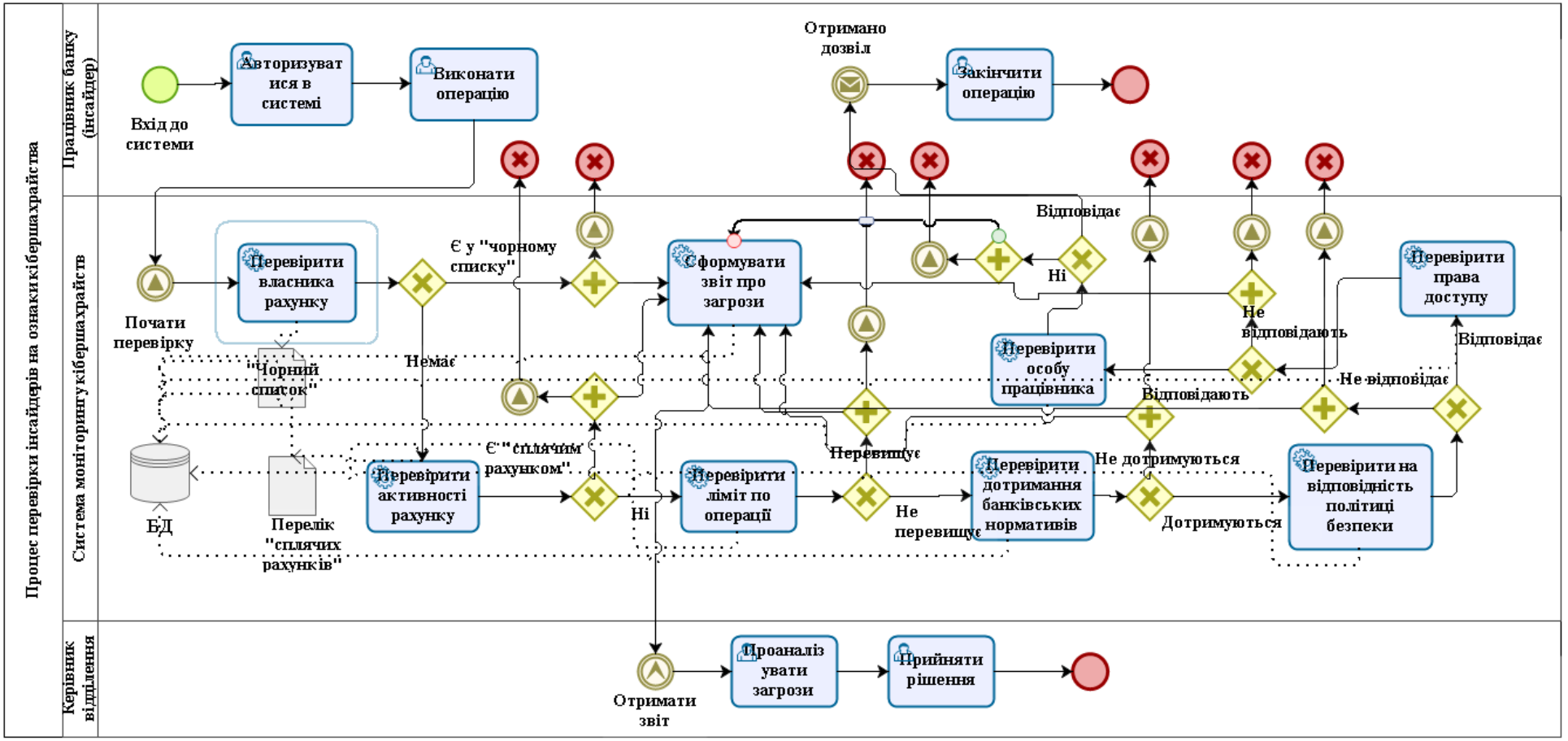


Рисунок 5.19 – Бізнес-модель процесу перевірки дій інсайдерів на ознаки кібершахрайств (складено авторкою)

Scenario information

Название Scenario 1

Time unit Seconds

Продолжительность 030,00:00:00

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

Scenario information

Название Scenario 1

Time unit Seconds

Продолжительность 030,00:00:00

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

Рисунок 5.20 – Результати симуляції за ресурсами для бізнес-процесу перевірки дій інсайдерів на ознаки кібершахрайств (складено авторкою)

Реалізація запропонованої методики оптимізації бізнес-процесів інформаційної безпеки дозволить формувати передумови виявлення транзакцій, наслідком яких може бути здійснення шахрайства з боку зовнішнього злочинця чи інсайдера, а також відмивання кримінальних доходів. Впровадження в практичну діяльність розроблених моделей дозволить охопити широке коло операцій незалежно від їх належності до зовнішнього чи внутрішнього середовища. Запропоновані моделі дозволять не тільки виявити слабкі місця в захисті інформації, але також вони слугують передумовою конвергенції систем кібербезпеки та фінансового моніторингу в рамках єдиної інтегрованої банківської автоматизованої системи. Це сприятиме здійсненню системного моніторингу для перевірки банківських транзакцій на предмет наявності ознак

кібер- і фінансових злочинів. Врешті-решт впровадження запропонованого підходу до оптимізації бізнес-процесів підвищить ефективність й системи управління за рахунок своєчасного прийняття оперативного рішення.

Інформаційний рівень системи попередження кіберзагроз.

Для формування інформаційної бази кіберзагроз потрібна статистика щодо реальних випадків, яка на практиці є недоступною для зовнішніх користувачів. Тому для дослідження даної проблематики було взято статистичні дані щодо шахрайств у Великій Британії за 2015-2018 роки за різними видами фінансових продуктів. Статистика була надана агентством звітності споживчого кредитування “Experian”, яке збирає та обробляє інформацію про понад мільярд людей та підприємств по всьому світу та входить в трійку найбільших кредитних бюро США. На жаль аналітичні агентства та банки України не публікують подібного роду статистику в періодиці або в офіційних виданнях. Тому в даному досліджені буде представлений узагальнений підхід до моделювання портретів потенційного шахрая та жертви, виконаний на прикладі даних Великої Британії, який можна застосовувати для формування таких портретів в різних країнах та з урахуванням їх умов.

Для дослідження було використано статистику за двома основними групами шахраїв. Перша група включає в себе осіб, які є споживачами послуг банків чи фінансово-кредитних компаній, тобто шахраї від першої сторони – безпосередні учасники. Шахрайство починається тоді, коли клієнт не має наміру в подальшому погасити виплати за фінансовим продуктом. Саме в цьому намірі й полягає найбільша різниця між кредитним ризиком та ризиком не повернення коштів в результаті шахрайства. Кредитний ризик включає клієнтів, які отримали товари чи послуги з наміром їх погасити, але просто не мають ресурсів для виконання своїх зобов'язань у зв’язку з непередбачуваними для них самих обставинами. За другим варіантом людина цілеспрямовано не віддає кошти. Такий вид шахрайства може включати широкий спектр тактик. Наприклад, коли одна особа передає відповідальність за виплату коштів на іншу особу. Тобто шахрай дуже гарно знає особу, на яку оформлює кредит, за виплату якого буде

відповідати жертва, а не шахрай. Найуспішними шахрайствами є випадки, коли шахраї поєднуються з клієнтами, які мають гарну кредитну історію, що створює підґрунтя для довгострокових масштабних шахрайств. [404]

Другу групу складають шахрайства від третьої сторони, тобто від осіб, які не пов'язані ні з провайдером фінансово-кредитних послуг, ні з їх клієнтами. Таке шахрайство здійснюється сторонніми особами шляхом застосування фальшивих ідентифікаційних документів, без відома особи, яка використовується для здійснення шахрайства. Сюди ж відноситься шахрайська діяльність, пов'язана з незаконним отриманням конфіденційних даних клієнтів банків, ПІН-кодів та CVV2-кодів банківських карток, логінів та паролів від інтернет-банкінгу, заволодівання мобільними фінансовими номерами клієнтів, за якими здійснюється аутентифікація, тощо. У випадку шахрайства від третьої сторони вкрай складно визначити особу самого шахрая, відслідкувати його місцезнаходження. Тому такі види шахрайств є найбільш популярними, оскільки зловмисники часто залишаються не спійманими. [404]

Так, розподіл шахрайств від першої сторони за видами фінансових продуктів в Великій Британії за 2015-2018 роки представлений на рисунку 5.21.

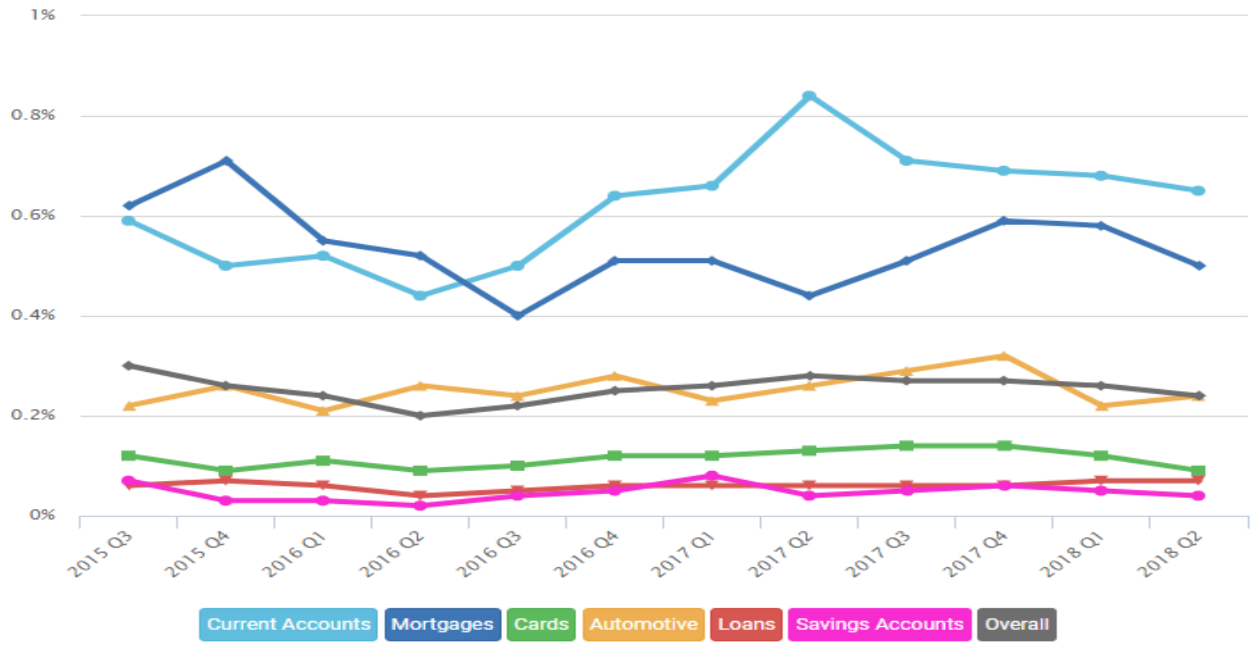


Рисунок 5.21 – Розподіл шахрайств від першої сторони за видами фінансових продуктів в Великій Британії за 2015-2018 роки [200]

Шахрайства від першої сторони найбільш ймовірно припадають на шахрайства з поточними банківськими рахунками (Current Accounts) та іпотекою (Mortgages) (рисунок 5.21). В даному випадку розглядається традиційне іпотечне шахрайство, яке включає в себе заходи, спрямовані на те, щоб обдурити кредитора, наприклад, намагання шахраєм отримати кредит, на який він не може законно претендувати, коли позичальники хибно представляють свою фінансову інформацію. [404]

Що стосується шахрайств від третьої сторони, то вони здійснюються переважно над поточними рахунками клієнтів (Current Accounts). Також популярними є афери з банківськими картками (Cards) та ощадними рахунками (Saving Accounts) (рисунок 5.22).

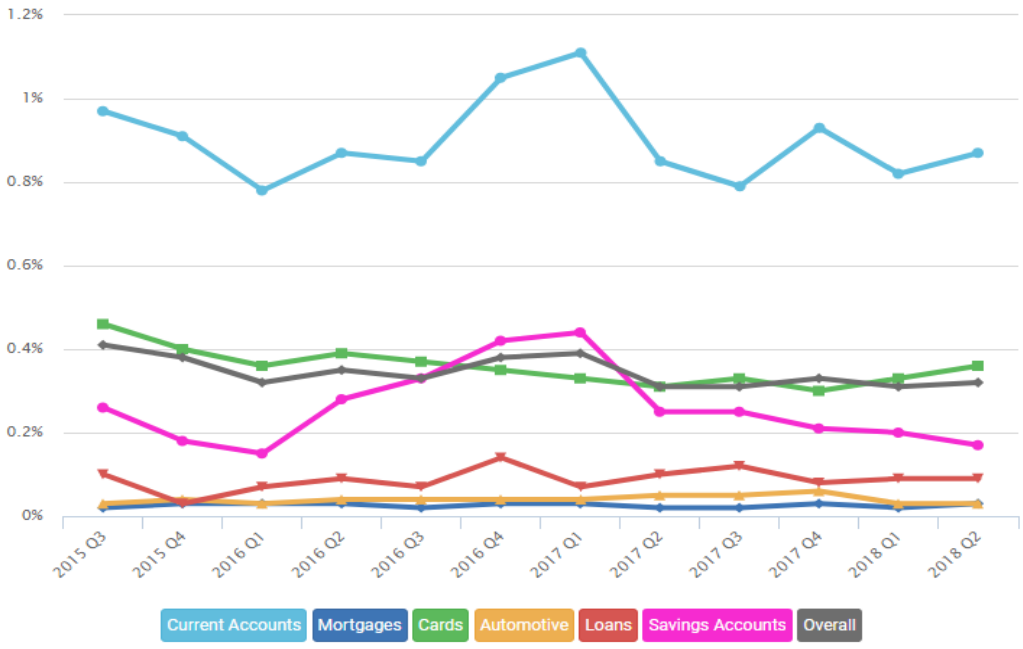


Рисунок 5.22 – Розподіл шахрайств від третьої сторони за видами фінансових продуктів у Великій Британії за 2015-2018 роки [200]

Злочинці можуть отримати доступ до рахунку клієнта шляхом застосування методів соціальної інженерії, що є найбільш популярним способом шахрайства. Також можливі випадки, коли ідентифікаційні дані клієнта викрадаються з бази даних банку. Відомі випадки, коли банківські працівники продавали бази даних стороннім особам, за рахунок чого шахраї отримували

доступ до даних клієнтів. Тут певну роль відіграє нехтування клієнтами елементарних правил безпеки власних конфіденційних даних, їх необережність при здійсненні розрахункових операцій та довірливість.

За останні три роки шахрайства від третьої сторони переважають над шахрайствами від першої. У 2018 році співвідношення шахрайств від першої сторони до шахрайств від третьої складає 44%, а шахрайств від третьої сторони до шахрайств від першої – 56%, тоді як ще в 2015 році ситуація була протилежною (рисунки 5.21–5.22). Можна припустити, що це пов'язано з більш масовим використанням Інтернет-технологій для здійснення банківських операцій, оскільки в просторах Інтернету набагато складніше забезпечити максимальну конфіденційність даних.

Використовуючи статистику по розподілу шахраїв від першої сторони на групи за віком, статтю та соціальним статусом, а також статистику по жертвах шахрайств з боку третьої сторони за такими ж параметрами, побудовано два ймовірнісні дерева із використанням програми MS Excel, які являють собою змодельовані портрети потенційного шахрая від першої сторони та потенційної жертви шахрайств з боку третіх сторін.

Дерево ймовірностей – це модель, яка широко застосовується для прийняття рішення, та складається з вузлів, які відповідають моменту настання події, в даному випадку – здійснення шахрайства з фінансовими продуктами. Гілки дерева – це можливі варіанти розвитку події, кожна зі своєю ймовірністю.

На першому етапі побудови дерева розподіляємо клієнтів (потенційних шахраїв) за статтю. Ймовірності для гілок будуть дорівнювати: 68,9 % – ймовірність першого варіанту розвитку подій, при якому шахрай виявиться чоловіком; 31,1 % – ймовірність того, що шахраєм буде жінка.

На наступному етапі враховуємо розподіл шахраїв за віковими групами. Ймовірність кожної наступної гілки отримуємо, як добуток ймовірностей фактору статі до ймовірності кожної з вікових груп. На другому етапі отримуємо з двох гілок – двадцять, за різними варіантами розвитку подій. На третьому етапі аналогічним чином уточнюємо модель, включивши фактор приналежності до

однієї з 15 соціальних груп. В результаті отримали дерево, в якому буде 300 гілок, тобто ми змоделювали 300 можливих варіантів розвитку подій і розрахували їх ймовірності. Для третього рівня використаємо інструмент «Пошук рішення», оскільки є ряд соціальних груп, які для певних вікових категорій будуть мати нульове значення (наприклад, категорія освіченої молоді не може бути у віці більше ніж 25 років і т.д.).

Побудоване дерево рішень, тобто модель потенційного шахрая від першої сторони за ознаками статі, віку та соціальної групи, представлено на рисунку 5.23. В матриці результатів моделі її елементи мають різні кольори у відповідності із рівнем ймовірності: зелений колір – найменша ймовірність шахрайства, жовтий – середня, червоний – найвищий рівень ймовірності шахрайства. В результаті побудованої моделі шахрая (рисунок 5.23) отримано, що найбільш схильною до шахрайства групою клієнтів є чоловіки у віці до 25 років, які належать до категорії освіченої молоді, що винаймає житло в міських районах. Ця група складає 4,81% (20-24 років) та 4,46% (до 20 років) від усіх шахраїв і є найбільш ризикованою групою клієнтів для банків та інших фінансово-кредитних організацій. Також до великої схильності шахрайства можна віднести чоловіків у віці від 25 до 29 років, що належать до сімей з обмеженими ресурсами (3,34%). Серед жінок можна виділити групи у віці до 20 років та 21-24 років, що відносяться до категорії освіченої молоді, яка винаймає житло. Це можливо пояснити за рахунок того, що люди у віці до 25 років ще не мають стабільного працевлаштування, постійного місця проживання, тому й стикаються з певними фінансовими труднощами, які схиляють їх до шахрайств. Малоймовірно, що шахраєм будуть жінки похилого віку із високим рівнем пенсійного забезпечення та власники приміських будинків середнього рівня, що досить давно проживають на даній території.

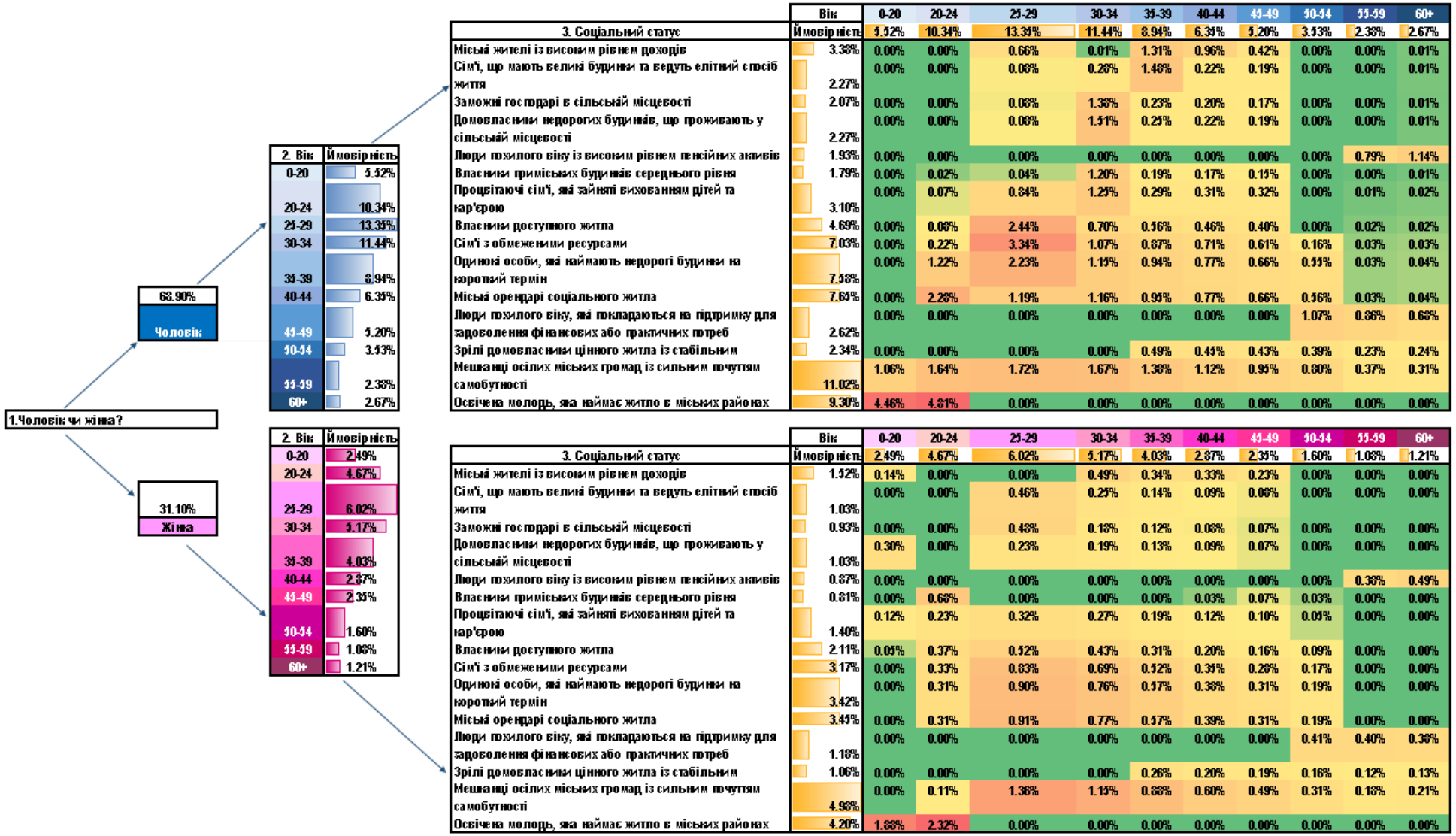


Рисунок 5.23 – Модель портрету потенційного шахрая від першої сторони за ознаками статі, віку та соціальної групи (складено авторкою)

Отримана модель дає можливість швидко визначити рівень ймовірності шахрайства для тієї чи іншої особи-клієнта, враховуючи три основні фактори: стать, вік та соціальну групу. Вона може бути корисною при прийнятті рішення про видачу позики, реалізації будь-яких ризикованих фінансових операцій, для забезпечення яких може використовуватися нерухомість, тощо. При впровадженні даної моделі у практичну діяльність банк може самостійно відслідковувати різні групи та ознаки, за якими може бути виникати шахрайство.

Результат побудованої моделі потенційної жертви шахрайства від третьої сторони за ознаками статі, віку та соціальної групи, представлено на рисунку 5.24. Отримана модель вказує на те, що найбільше від сторонніх шахраїв потерпають чоловіки у віці 20 - 25 років, які відносяться до соціальної групи «Освічена молодь, що винаймає житло у місті», а також чоловіки у віці 60+, які належать до категорії міських жителів із високим рівнем доходу. Тобто переважно це або молоді люди, які перебувають на ранній стадії своєї кар'єри або продовжують навчання, або одинокі люди похилого віку, які мають високий рівень достатку та мають власне житло. Схожі результати було отримано й для жінок, які знаходяться у віці 20 - 25 років та орендують житло, а також жінки похилого віку (60+), які мають високий рівень доходу.

Отримані результати для молодих людей можна пояснити їх більшою фінансовою активністю, тобто вони частіше здійснюють будь-які фінансові операції через Інтернет або мобільні пристрої, частіше користуються послугами фінансово-кредитних організацій, онлайн-сервісами, програмними додатками.

Найменша ймовірність бути жертвою шахрая є у чоловіків та жінок, які належать до категорії власники приміських будинків середнього рівня та зрілі домовласники цінного житла із стабільним доходом. Це можна пояснити тим фактом, що маючи власне житло такі категорії осіб можуть дозволити собі купувати речі, не звертаючись до кредитних послуг банківських установ, що знижає ймовірність стати жертвою кібершахрая.

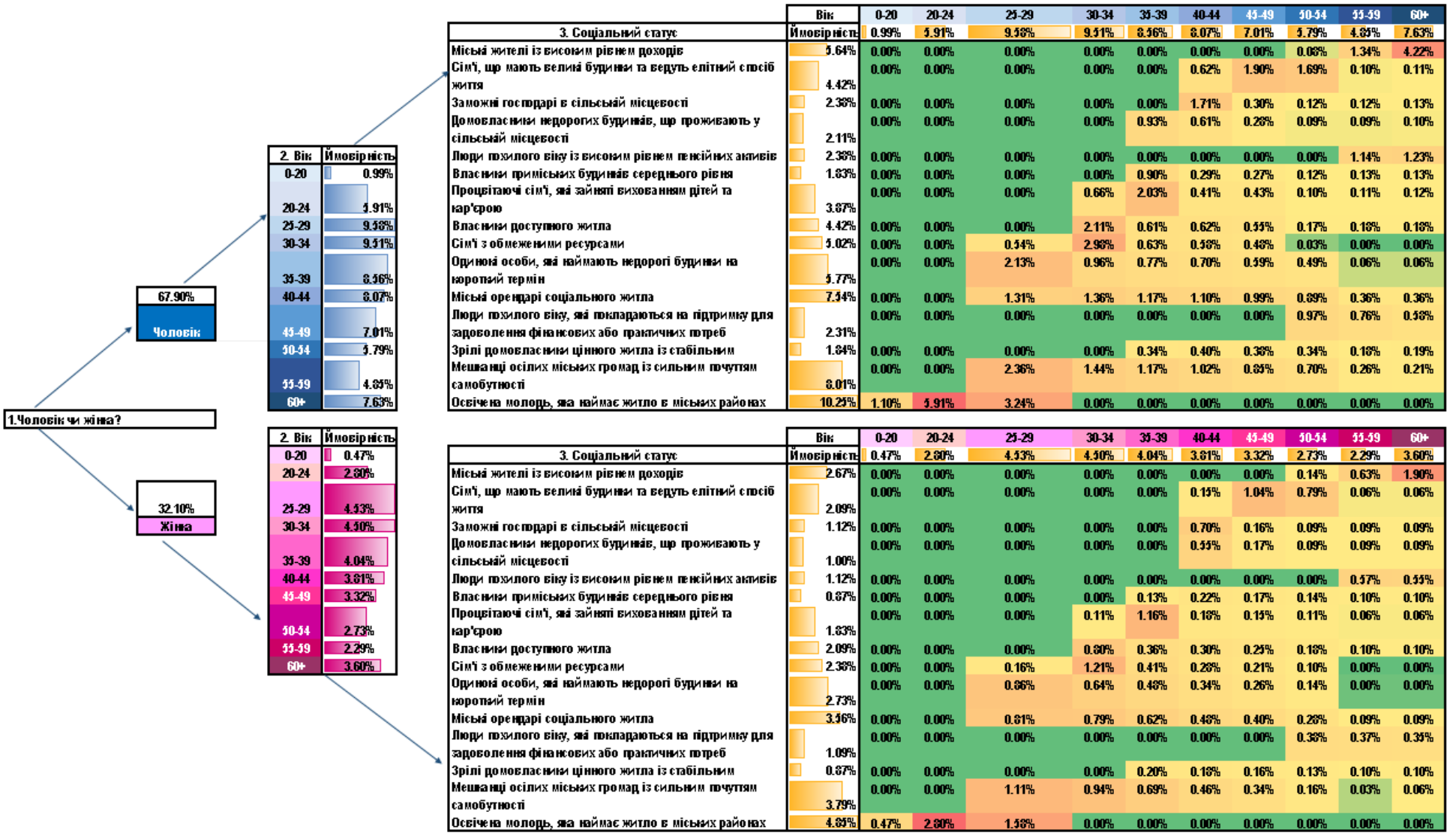


Рисунок 5.24 – Модель портрету потенційної жертви шахрайства від третьої сторони за ознаками статі, віку та соціальної групи (складено авторкою)

Розроблена модель допомагає вирізнити тих клієнтів, для яких потрібно посилити систему безпеки за всіма видами банківських продукті, особливо банківських карт, поточних та ощадних рахунків, щоб уникнути небажані збитки. Можливе також введення додаткових заходів для інформування клієнтів про найпоширеніші актуальні схеми банківських шахрайств.

Методику побудови портретів шахраїв можна використати й в роботі українських банків. Ймовірно, що портрети будуть відрізнятися, оскільки співвідношення віку, статі та фінансової стабільності клієнта є різними для громадян з розвинутої країни та країни, що розвивається. Але застосування цієї методики дозволить вже на етапі здійснення операції визначити потенційного шахрая чи жертву. Це призведе до коригування інструкцій в банках та зменшить навантаження на людину в процесі прийняття рішення.

Алгоритмічний рівень системи попередження кіберзагроз.

Для реалізації алгоритмічного рівня необхідно визначити ті методи, які можливо використовувати для виявлення та попередження фінансових кібершахрайств. Їх застосування залежить від способів шахрайства, яких на сьогодні існує досить багато. Тому визначимо ті, які є найбільш поширеними у сфері кредитних карток:

1) фізичні способи: використання фальшивих карток, спеціальних пристроїв, які встановлюють на банкомати, фальшивих терміналів та банкоматів, що не належать банку та інші;

2) програмні способи: використання фейкових веб-сторінок, фальшивих Інтернет-магазинів, зламування акаунтів клієнтів та інші.

Фактично, в процесі здійснення шахрайської операції шахраї можуть використовувати різні способи, але для банку результати таких дій відображаються в його базі даних. Якщо проаналізувати операції, які підлягали шахрайським діям, то існують наступні узагальнюючі ознаки, які дозволяють ідентифікувати операцію у більшості випадків як шахрайську:

1) зняття всієї суми з рахунку, тобто його обнуління, або частковий випадок – зняття великої суми з рахунку, яка перевищує можливий ліміт;

2) здійснення великої кількісті операцій на одному рахунку за короткий проміжок часу (час, день), що в кінцевому рахунку призводить до його обнуління;

3) переведення великої суми коштів, не притаманної попереднім операціям, на сторонній рахунок, відкритий в іншому банку;

4) здійснення операції з території іншої країни.

Будь-які ситуації шахрайства не залежно від способу в будь-якому випадку будуть мати одну з цих ознак. Якщо автоматизована банківська система буде спроможна автоматично здійснювати моніторинг транзакцій своїх клієнтів в процесі їх здійснення, та виявляти операції, які потенційно відповідають цим ознакам, то в такому випадку система буде сигналізувати про необхідність контролю та повторної ідентифікації клієнта. Якщо операція дійсно кібершахрайська, то людина, що її здійснює, не отримає дозволу на її проведення. При чому система повинна повідомити про причини ідентифікації.

Яким чином система зможе визначати за цими ознаками шахрайську операцію? Це можливо у разі використання інструментів інтелектуального аналізу для виявлення подібних ситуацій. Звичайно ж, що використання подібного інструментарію вимагає створення й автоматизованого модулю. Це дозволить постійно проводити моніторинг операцій та превентивно й оперативно виявляти порушення. Методика передбачає випадок, коли в якості «клієнта» виступає шахрай, то в цьому разі він не зможе пройти додаткову аутентифікацію. Також у випадку контакту клієнта банку із шахраєм та інформування його щодо кодів, паролів, номерів рахунків, карток, подібна схема буде працювати теж ефективно. Це відбувається за рахунок того, що клієнт буде попереджатися не тільки про вхід до його акаунту, але про здійснення операції, що має ознаки кібершахрайства.

Головною функцією алгоритмічного блоку є проведення інтелектуального аналізу транзакцій не тільки наявних, але й ті, які знаходяться в процесі обробки чи ініціалізації. Інтелектуальний аналіз має в своєму арсеналі значний перелік методів. Найбільш розповсюджені з них представлені в таблиці 5.6.

Таблиця 5.6 – Переваги та недоліки найбільш розповсюджених методів інтелектуального аналізу [227]

Назва методу та його суть	Переваги	Недоліки
Асоціація дозволяє знаходити певні закономірності між пов'язаними подіями	Дозволяє знаходити цікаві закономірності між даними; працює з даними будь-якої природи; результати представляє у вигляді таблиці, дерева, тексту	Складність розуміння правил; громіздкість правил, що інколи викликає незручності аналізу закономірностей
Кластеризація здійснює розбиття множини об'єктів на однорідні групи (кластери)	Використання різних ознак для розбиття; не має обмежень до вигляду спостережень	У зв'язку із стисканн інформації можуть виник певні викривлення; ма обмеження на кількість та ск кластерів; працює тільки кількісними даними
Лінійна регресія виявляє залежність досліджуваного показника від одного або декількох факторів	Простота побудови та інтерпретації результатів; усталений алгоритм розрахунків	Складність визначення виду функціонального зв'язку та моделювання нелінійних процесів; застосовується для лінійних процесів
Logit та Probit-models дозволяють визначити ймовірність виникнення події шляхом підгонки даних	Виправляє недоліки лінійної регресії по відношенню до значення ймовірності; проста в побудові та реалізації	Оцінки є ефективними тільки при кількості спостережень понад 500
Дерева прийняття рішення графічно систематизують процес прийняття рішення щодо прогнозу значення цільової змінної з урахуванням того, що кожне наступне рішення залежить від попереднього [407, с. 241]	Масштабованість, що прискорює обчислення; однозначність процесу навчання; самоадаптованість з мінімальним втручанням людини; висока точність прогнозу; можливість використання категоріальних змінних	Складність визначення кількості оптимальних рішень; потребує значних витрат часу на побудову; може мати багато варіантів розгалуження; необхідність використання інших методів для відбору факторів
Нейронні мережі представляють систему штучних нейронів, що поєднані між собою та взаємодіють один з одним, яка дозволяє на основі процесу навчання визначити результат [407, с. 241]	Можливість вирішення слабко формалізованих або неформалізованих нелінійних задач; стандартний алгоритм; простота побудови із використанням програмного забезпечення; можливості навчання як людиною, так й автоматизовано	Складні для інтерпретації та розуміння; наявність неточних даних з випадковою складовою; обмеженість використання
Баєсівський аналіз визначає найбільш точну ймовірність настання певної події з огляду виникнення нової інформації	Можливості оцінки особою, що приймає рішення ймовірності довіри до моделі; гнучкість до врахування нової інформації;	Не враховує поточний стан об'єкту, що досліджується; складність обчислення; не можливо обрати апріорний розподіл

Продовження таблиці 5.6

Назва методу та його суть	Переваги	Недоліки
	застосування до ситуацій, які раніше не аналізувалися	
Генетичні алгоритми призначені для вирішення задач багатомірної оптимізації методом випадкового пошуку	Можливість застосування до даних різного типу; дозволяють знаходити універсальні рішення; знаходять множину рішень та обирають найкраще; саморозвиваються	Невідомий час на пошук; низька швидкість пошуку; велика кількість вільних параметрів; не доказовість збіжності

Найбільш гнучким інструментом інтелектуального аналізу даних, на нашу думку, є нейронні мережі, які знайшли широке використання в різних сферах економіки. Нейронна мережа імітує поведінку людського мозку, що дозволяє її використовувати для вирішення нетипових задач. Якщо порівнювати нейронні мережі з традиційними обчислювальними системами, то:

– їх використання дозволяє вирішувати задачі із невідомими закономірностями розвитку ситуації та залежностями між вхідними та вихідними даними, що не можливо для традиційних систем;

– такі системи мають можливість роботи із великим набором даних, при чому вони самостійно обирають придатні вхідні сигнали;

– вони мають властивість адаптовуватися до змін навколишнього середовища, тобто в нестаціонарних умовах, коли інформація змінюється з часом. Цю властивість як раз доцільно використовувати у випадку створення нейронної мережі для аналізу банківських операцій, зміни в яких відбуваються постійно;

– такі системи у випадку пошкодження будь-яких зв’язків або самого нейрону не втрачають свою продуктивність;

– вони володіють можливістю швидкодії за рахунок використання масового паралелізму обробки інформації [227].

Виходячи з переваг та властивостей нейронних мереж можна зробити висновок про їх потенційні можливості використання для виявлення кібершахрайств з банківськими операціями. Це пов’язано з їх властивостями самонавчання та динамічного врахування нової інформації.

В даному дослідженні реалізовано алгоритм побудови нейронної мережі для набору даних, узятих на прикладі Сумської філії банку «А», повна назва якого не зазначається у відповідності із комерційною таємницею. Набір спостережень сформовано з 5000 транзакцій клієнтів з банківськими картками. Його було поділено на три види вибірки – 70% навчальна, 15% тестова, 15% контрольна. У якості вхідних параметрів було обрано 9 змінних, опис і значення яких представлені у таблиці 5.7.

Таблиця 5.7 – Опис вхідних змінних [407]

Ім’я змінної	Зміст змінної	Роль змінної	Тип
Y	Випадки шахрайства	цільова	binary
X1	Частота щоденного використання картки	вхідна	interval
X2	Відношення логарифму величини транзакції, до логарифму часу між транзакціями	вхідна	interval
X3	Відношення логарифму загального обсягу транзакцій за день, до логарифму середнього часу між транзакціями впродовж дня	вхідна	interval
X4	Стандартизоване відношення загального обсягу транзакцій за день до кумулятивного інтервалу між транзакціями за день	вхідна	interval
X5	Стандартизований обсяг щоденного використання картки	вхідна	interval
X6	Стандартизований обсяг транзакції	вхідна	interval
X7	Стандартизований інтервал часу між використанням карти	вхідна	interval
X8	Тип покупки за обсягом	вхідна	ordinal
X9	Тип покупки за ймовірністю шахрайства	вхідна	ordinal

Змінна Y показує випадки шахрайства за даною операцією – «1», якщо був прецедент шахрайства; «0», якщо ні. Вона виступає цільовою, оскільки дозволяє ідентифікувати випадок шахрайства.

Інші змінні обиралися згідно тих ознак, які було означено вище. Так, було обрано частоту щоденного використання картки (x1), яка дозволяє відбирати тих клієнтів, які найчастіше використовують картку протягом дня. Із збільшенням частоти підвищується ризик того, що даною карткою користується шахрай. Змінні x2 та x3 було розраховано з урахуванням обсягів та часу транзакцій за певною карткою. Для приведення змінних до нормального розподілу проведено їх логарифмування. Змінні x4-x7, які сформовано з урахуванням інтервалів

використання карток та обсягів щоденного використання, було стандартизовано для усунення впливу різних факторів. Для того, щоб врахувати ознаку нетипового використання коштів картки у разі її втрати або викрадення, введено змінні x8 та x9, які характеризують групи потенційних покупок за ймовірністю шахрайства. Ці змінні оцінювалися банком самостійно згідно його методики.

Для реалізації моделі обрано програмний продукт STATISTICA. Для розрахунків було використано модуль “Data Mining”. [223]

Побудову нейронної мережі було виконано за наступним алгоритмом (рисунок 5.25).

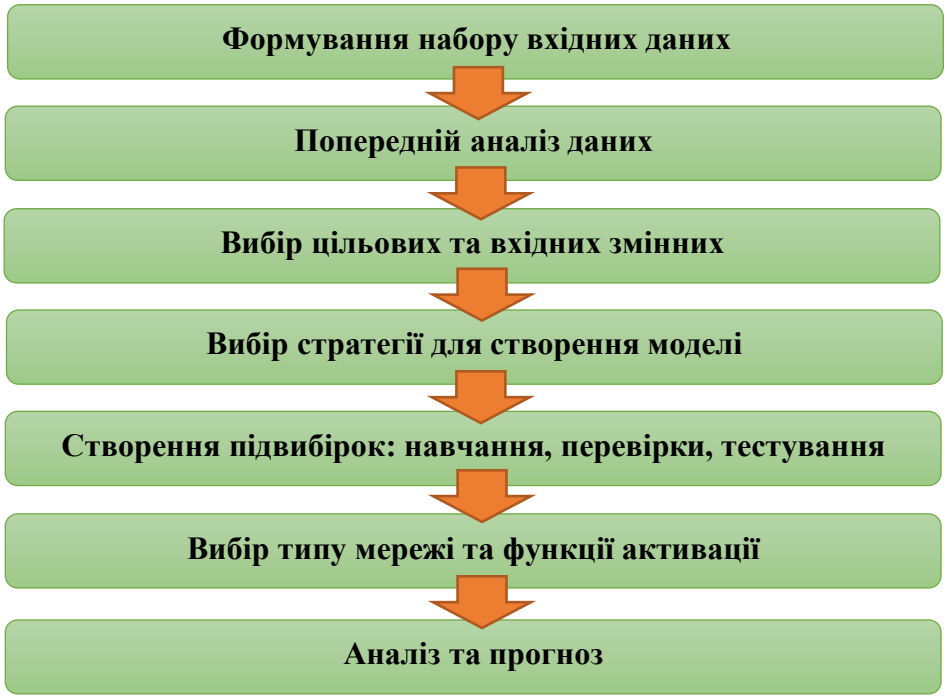


Рисунок 5.25 – Алгоритм побудови нейронної мережі (складено авторкою)

Так, було побудовано декілька варіантів нейронної мережі з використанням автоматичного інструментарію та із задаванням користувацьких налаштувань в пакеті STATISTICA. Найбільш придатною за параметрами виявилася мережа, значення ROC-кривої для якої дорівнює 0,7687 (рисунок 5.26).

	ROC areas and thresholds Samples: Train, Test, Validation								
	2. MLP 9-13-2	3. MLP 9-5-2	**4. MLP 9-5-2**	5. MLP 9-5-2	6. MLP 9-3-2	7. MLP 9-3-2	8. MLP 9-3-2	9. MLP 9-3-2	10. MLP 9-3-2
ROC area	1,000000	1,000000	0,999999	0,999371	1,000000	1,000000	1,000000	1,000000	1,000000
ROC threshold	0,536086	0,396754	0,768721	0,364330	0,507139	0,268588	0,402272	0,178912	0,601024

Рисунок 5.26 – Вибір нейронної мережі за значенням ROC-кривої (складено авторкою)

В результаті побудовано нейронну мережу, схема якої представлена на рисунку 5.27.

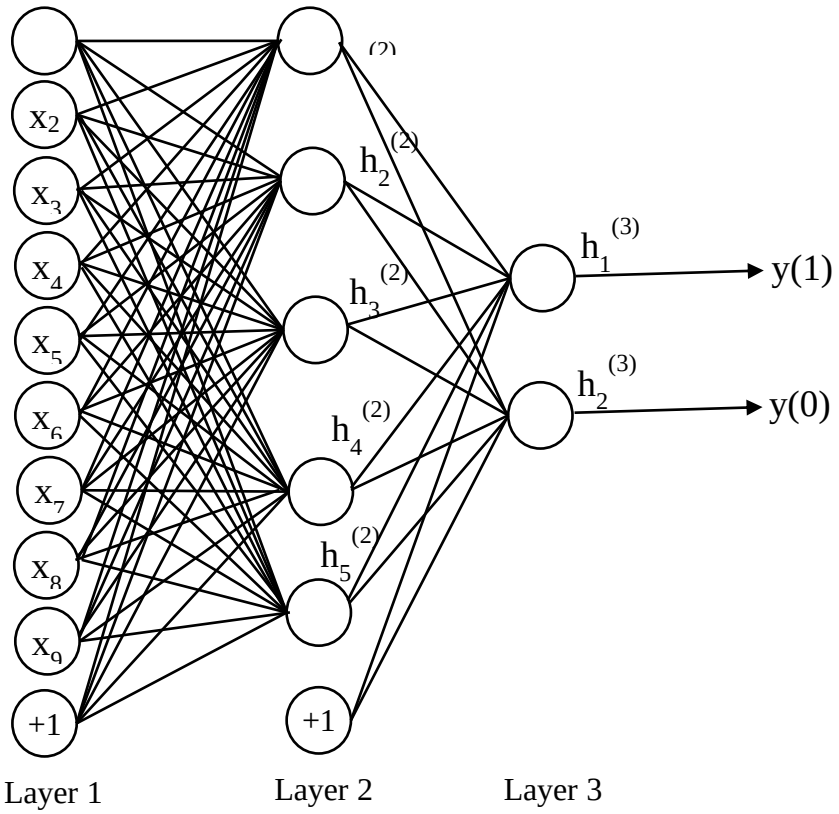


Рисунок 5.27 – Схема отриманої нейронної мережі (складено авторкою)

Математичну модель нейронної мережі з урахуванням вхідних та вихідних змінних, представлених в таблиці 5.7, в загальному вигляді можна представити у вигляді формул (5.13)-(5.19):

$$h_1^{(2)} = f\left(w_{11}^{(1)}x_1 + w_{12}^{(1)}x_2 + \cdots + w_{19}^{(1)}x_9 + b_1^{(1)}\right), \quad (5.13)$$

$$h_2^{(2)} = f\left(w_{21}^{(1)}x_1 + w_{22}^{(1)}x_2 + \cdots + w_{29}^{(1)}x_9 + b_2^{(1)}\right), \quad (5.14)$$

$$h_3^{(2)} = f\left(w_{31}^{(1)}x_1 + w_{32}^{(1)}x_2 + \cdots + w_{39}^{(1)}x_9 + b_3^{(1)}\right), \quad (5.15)$$

$$h_4^{(2)} = f\left(w_{41}^{(1)}x_1 + w_{42}^{(1)}x_2 + \cdots + w_{49}^{(1)}x_9 + b_4^{(1)}\right), \quad (5.16)$$

$$h_5^{(2)} = f\left(w_{51}^{(1)}x_1 + w_{52}^{(1)}x_2 + \cdots + w_{59}^{(1)}x_9 + b_5^{(1)}\right), \quad (5.17)$$

$$y(1) = h_1^{(3)} = f\left(w_{11}^{(2)}h_1^{(2)} + w_{12}^{(2)}h_2^{(2)} + w_{13}^{(2)}h_3^{(2)} + w_{14}^{(2)}h_4^{(2)} + w_{15}^{(2)}h_5^{(2)} + b_1^{(2)}\right), \quad (5.18)$$

$$y(0) = h_2^{(3)} = f\left(w_{21}^{(2)}h_1^{(2)} + w_{22}^{(2)}h_2^{(2)} + w_{23}^{(2)}h_3^{(2)} + w_{24}^{(2)}h_4^{(2)} + w_{25}^{(2)}h_5^{(2)} + b_1^{(2)}\right), \quad (5.19)$$

де f(·) – активаційна функція вузла, в даному випадку логістична функція;

$h_1^{(2)}$ – вихід першого вузла у другому шарі, входами у якій є вихід першого вузла у другому шарі, тобто $w_{11}^{(1)}x_1^{(1)}$, $w_{12}^{(1)}x_2^{(1)}$, …, $w_{19}^{(1)}x_9^{(1)}$ та $b_1^{(1)}$. Ці входи складаються та передаються в активаційну функцію для розрахунку виходу першого вузла. Інші вузли $h_2^{(2)}$, $h_3^{(2)}$, $h_4^{(2)}$ та $h_5^{(2)}$ – аналогічно;

$h_1^{(3)}$ та $h_2^{(3)}$ – виходи другого вузла у третьому шарі, в якому беруться зважені виходи вузлів другого шару ($h_1^{(2)}$, $h_2^{(2)}$, $h_3^{(2)}$, $h_4^{(2)}$ та $h_5^{(2)}$).

В якості активаційної функції для прихованих шарів та виходів застосовано сигмоїдальну (логістичну) функцію.

Логістична функція для активації вихідних вузлів має вигляд формули (5.20):

$$OUT = \frac{1}{1+\exp(-a \times net)}, \quad (5.20)$$

де OUT – виходи вузлів нейронної мережі у другому та третьому шарах, тобто $h_1^{(2)}$, $h_2^{(2)}$, $h_3^{(2)}$, $h_4^{(2)}$, $h_5^{(2)}$, $h_1^{(3)}$ та $h_2^{(3)}$;

net – сума вхідних сигналів, помножена на відповідні ваги для другого та третього шару, наприклад, $\left(w_{11}^{(1)}x_1 + w_{12}^{(1)}x_2 + \cdots + w_{19}^{(1)}x_9 + b_1^{(1)}\right)$ для $h_1^{(2)}$, розраховані за формулами (5.13)–(5.19);

a – ступінь крутизни логістичної функції.

В результаті застосування алгоритму побудови нейронної мережі (рисунок 5.27) отримано оцінки вагових коефіцієнтів найбільш адекватної нейронної мережі, які представлено на рисунку 5.28.

	Network weights	
Weight ID	Connections 4.MLP 9-5-2	Weight values 4.MLP 9-5-2
1	x1 --> hidden neuron 1	-16,3151
2	x2 --> hidden neuron 1	4,3070
3	x3 --> hidden neuron 1	-4,5189
4	x4 --> hidden neuron 1	-0,5108
5	x5 --> hidden neuron 1	4,2696
6	x6 --> hidden neuron 1	7,3127
7	x7 --> hidden neuron 1	2,5316
8	x8 --> hidden neuron 1	0,5070
9	x9 --> hidden neuron 1	0,4482
10	x1 --> hidden neuron 2	-5,9908
11	x2 --> hidden neuron 2	-39,7783
12	x3 --> hidden neuron 2	-3,0862
13	x4 --> hidden neuron 2	3,3070
14	x5 --> hidden neuron 2	-39,6615
15	x6 --> hidden neuron 2	-25,1488
16	x7 --> hidden neuron 2	-5,3583
17	x8 --> hidden neuron 2	-0,8634
18	x9 --> hidden neuron 2	1,1390
19	x1 --> hidden neuron 3	-6,6870
20	x2 --> hidden neuron 3	-12,1640
21	x3 --> hidden neuron 3	-8,6583
22	x4 --> hidden neuron 3	-1,4266
23	x5 --> hidden neuron 3	-12,1605
24	x6 --> hidden neuron 3	-3,3846
25	x7 --> hidden neuron 3	0,4699
26	x8 --> hidden neuron 3	5,5582
27	x9 --> hidden neuron 3	-18,9207
28	x1 --> hidden neuron 4	-44,9813
29	x2 --> hidden neuron 4	-6,3691
30	x3 --> hidden neuron 4	-6,6700

	Network weights	
Weight ID	Connections 4.MLP 9-5-2	Weight values 4.MLP 9-5-2
31	x4 --> hidden neuron 4	8,6082
32	x5 --> hidden neuron 4	-6,3382
33	x6 --> hidden neuron 4	21,2503
34	x7 --> hidden neuron 4	0,0703
35	x8 --> hidden neuron 4	0,9060
36	x9 --> hidden neuron 4	3,5797
37	x1 --> hidden neuron 5	-3,7488
38	x2 --> hidden neuron 5	-13,9347
39	x3 --> hidden neuron 5	-0,2131
40	x4 --> hidden neuron 5	1,1454
41	x5 --> hidden neuron 5	-13,8279
42	x6 --> hidden neuron 5	-9,2675
43	x7 --> hidden neuron 5	-1,7795
44	x8 --> hidden neuron 5	-0,9497
45	x9 --> hidden neuron 5	3,0873
46	input bias --> hidden neuron 1	11,3964
47	input bias --> hidden neuron 2	26,5653
48	input bias --> hidden neuron 3	20,8532
49	input bias --> hidden neuron 4	23,4448
50	input bias --> hidden neuron 5	9,4744
51	hidden neuron 1 --> y(0)	-0,6631
52	hidden neuron 2 --> y(0)	0,3032
53	hidden neuron 3 --> y(0)	4,9860
54	hidden neuron 4 --> y(0)	36,0276
55	hidden neuron 5 --> y(0)	-1,0766
56	hidden neuron 1 --> y(1)	0,0085
57	hidden neuron 2 --> y(1)	-0,4928
58	hidden neuron 3 --> y(1)	10,4615
59	hidden neuron 4 --> y(1)	-11,2608
60	hidden neuron 5 --> y(1)	2,9223
61	hidden bias --> y(0)	-15,8054
62	hidden bias --> y(1)	8,6566

Рисунок 5.28 – Вагові коефіцієнти нейронної мережі, отримані в пакеті «STATISTICA» (складено авторкою)

Розраховані значення використано для побудови математичної моделі нейронної мережі (5.21)–(5.27):

$$h_1^{(2)} = f(-16{,}3151x_1 + 4{,}3070x_2 - 4{,}5189x_3 - 0{,}5108x_4 + 4{,}2696x_5 + 7{,}3127x_6 + 2{,}5316x_7 + 0{,}5070x_8 + 0{,}4482x_9 + 11{,}3964), \quad (5.21)$$

$$h_2^{(2)} = f(-5{,}9908x_1 - 39{,}7783x_2 - 3{,}0862x_3 + 3{,}3070x_4 - 39{,}6615x_5 - 25{,}1488x_6 - 5{,}3583x_7 - 0{,}8634x_8 + 1{,}1390x_9 + 26{,}5653), \quad (5.22)$$

$$h_3^{(2)} = f(-6{,}6870x_1 - 12{,}1640x_2 - 8{,}6583x_3 - 1{,}4266x_4 - 12{,}1605x_5 - 3{,}3846x_6 + 0{,}4699x_7 + 5{,}5582x_8 - 18{,}9207x_9 + 20{,}8532), \quad (5.23)$$

$$h_4^{(2)} = f(-44{,}9813x_1 - 6{,}3691x_2 - 6{,}6700x_3 + 8{,}6082x_4 - 6{,}3382x_5 + 21{,}2503x_6 + 0{,}0703x_7 + 0{,}9060x_8 + 3{,}5797x_9 + 23{,}4448), \quad (5.24)$$

$$h_5^{(2)} = f(-3{,}7488x_1 - 13{,}9347x_2 - 0{,}2131x_3 + 1{,}1454x_4 - 13{,}8279x_5 - 9{,}2675x_6 - 1{,}7795x_7 - 0{,}9497x_8 + 3{,}0873x_9 + 9{,}4744), \quad (5.25)$$

$$y(1) = h_1^{(3)} = f\left(0{,}0085h_1^{(2)} - 0{,}4928h_2^{(2)} + 10{,}4615h_3^{(2)} - 11{,}2608h_4^{(2)} + 2{,}9223h_5^{(2)} + 8{,}6566\right), \quad (5.26)$$

$$y(0) = h_2^{(3)} = f\left(-0{,}6631h_1^{(2)} + 0{,}3032h_2^{(2)} + 4{,}9860h_3^{(2)} + 36{,}0276h_4^{(2)} - 1{,}0766h_3^{(2)} - 15{,}8054\right). \quad (5.27)$$

З використанням отриманої нейронної мережі побудовано прогноз ймовірності здійснення шахрайської операції з урахуванням заданих умов. Фрагмент отриманих результатів представлений на рисунку 5.29.

Case name	Predictions spreadsheet for y Samples: Train, Test, Validation **Sample**	y Target	y - Output 4. MLP 9-5-2
1	Test	0	0
2	Validation	1	1
3	Train	1	1
4	Train	0	0
5	Train	1	1
6	Test	0	0
7	Train	0	0
8	Train	1	1
9	Test	0	0
10	Train	1	1
11	Train	1	1
12	Train	0	0
13	Train	0	0
14	Test	0	0
15	Train	0	0

Рисунок 5.29 – Фрагмент прогнозних значень, отриманих за допомогою нейронної мережі (складено авторкою)

Матриця помилок побудованої мережі за трьома підвиборками показує гарні результати (рисунок 5.30).

	y (Classification summary) Samples: Train, Test, Validation			
		y-0	y-1	y-All
4.MLP 9-5-2	Total	3672,000	1328,000	5000,000
	Correct	3672,000	1328,000	5000,000
	Incorrect	0,000	0,000	0,000
	Correct (%)	100,000	100,000	100,000
	Incorrect (%)	0,000	0,000	0,000

Рисунок 5.30 – Фрагмент прогнозних значень, отриманих за допомогою нейронної мережі (складено авторкою)

Побудовану нейронну мережу можна застосовувати для подальшого аналізу операцій з картками для виявлення потенційних шахрайств з ними. Модель дає гарні результати, але потребує розвитку з урахуванням нових спостережень для подальшого її навчання та удосконалення.

Алгоритмічний рівень системи попередження кіберзагроз передбачає використання інтелектуального аналізу даних, що дозволить виявляти та попереджати шахрайські операції з картками клієнтів. Для максимального ефекту доцільно реалізувати алгоритм нейронної мережі та впровадити його у модуль моніторингу операцій в автоматизованій банківській системі. Його застосування дозволить проводити автоматичну перевірку операцій на етапі їх ініціювання клієнтом або потенційним зловмисником. В процесі перевірки здійснюватиметься відбір операцій у відповідності з ознаками, які характеризують їх як шахрайські.

Таким чином, для ефективної взаємодії фінансово-кредитних установ та їх клієнтів, а також для зменшення ймовірності отримання збитків від різного роду кібершахрайських операцій, необхідно застосовувати нові інструменти. В їх якості можуть виступати: моделі оптимізації бізнес-процесів, портрети потенційних шахраїв та жертв банківських шахрайств, а також інструменти Data Mining, а саме нейронні мережі. Їх використання було запропоновано для побудови трирівневої системи фінансових кіберзагроз, реалізованої для банківського сектору.

Так, оптимізаційні моделі забезпечують організаційний рівень, що дозволяє виявляти слабкі місця в системі інформаційного захисту. Вони були реалізовані для процесів ідентифікації клієнтів, перевірки транзакцій на предмет кіберзлочинів з боку зовнішнього користувача та інсайдерів, а також на предмет необхідності проведення фінансового моніторингу. Інформаційний рівень забезпечують портрети жертв та шахрая, які представляють собою моделі дерева рішень та дозволяють визначити ймовірність шахрайства у відповідності з рядом ознак. Їх було реалізовано для випадків кредитного шахрайства із врахуванням ознак віку, статі, соціального становища, але їх можна доповнити способами здійснення операцій, історією клієнта, місцем здійснення операції та іншими. Алгоритмічний рівень системи було реалізовано із використанням нейромережевого моделювання, яке дозволило побудувати модель виявлення ймовірності ознак кібершахрайств у транзакціях банків із кредитними картками.

Шахраї постійно вдосконалюють свої інструменти, відповідно банківські підрозділи кіберзахисту повинні швидко реагувати на ці зміни. Це можливо, якщо банки будуть використовувати математичні методи для розробки алгоритмів моніторингу, перевірки клієнтів та операцій на предмет виникнення ймовірності шахрайства. Отримані результати повинні накопичуватися та формувати банк даних, використання якого надасть можливість оперативно оновлювати інформацію щодо шахрайств та модернізовувати алгоритми. Комплексна реалізація запропонованої системи дозволить попереджати фінансові кіберзагрози, а її інтеграція із системою фінансового моніторингу, кібербезпеки та автоматизованої банківської системи забезпечуватиме синергетичний ефект від їх взаємодії.

Висновки до розділу 5

1. У підрозділі 5.1 дисертаційної роботи визначено важливість оцінювання ризиків, що асоціюються з втратою інформації у контексті забезпечення інформаційної безпеки. Було встановлено, що за статистикою, тривалість

періоду знаходження витоку інформації становить 206 днів, а періоду її відновлення після несанкціонованого витоку – 73 дні. У роботі запропоновано методологію експрес-оцінювання найбільш важливих факторів ризику втрати інформації залежно від обсягів допустимих збитків та частоти повторення відповідних інцидентів. Для цього всі інциденти, пов'язані з втратою інформації, згруповані п'ятьма групами (обумовлені діями персоналу, вірусними атаками, технічними несправностями, незаконними діями кіберзлочинців, некоректною роботою програмного забезпечення), для кожної з яких визначено набір релевантних факторів, які є каталізаторами цих інцидентів (загалом 66 факторів).

2. На основі системного поєднання теорії ймовірності та теорії множин у роботі побудовано карту ризиків (за матричним принципом), де грошова оцінка збитків від втрати інформації та частота повторення інцидентів ідентифікуються за такими рівнями: низьким, середнім, високим. Розроблені пропозиції можуть застосовуватися як в реальному і фінансовому секторах, так і в секторі публічного управління, що робить запропоновані розробки універсальними.

3. У підрозділі 5.2 запропоновано науково-методичний підхід, що базується на системно-динамічному імітаційному моделюванні (з використанням програмного середовища Vensim) та дозволяє порівняти декілька систем захисту інформації за такими параметрами: рівнем відкритості системи, наявністю можливостей для використання зовнішніх носіїв, можливостей для віддаленого й несанкціонованого доступу, для заборони завантаження інформації, для доступу до відкриття та запуску невідомих файлів, копіювання, зміни і знищення інформації тощо. Запропонований підхід апробовано на даних типових економічних агентів для обґрунтування доцільності запровадження блокчейн-технології щодо попередження та виявлення кіберінцидентів. У результаті проведених імітаційних експериментів змодельовано 128 патернів поведінки системи інформаційної безпеки, які оцінювалися за ризиком невиявлення кіберзагроз та рівнем уразливості системи, що підтвердило доцільність використання блокчейн-технології, оскільки середній ризик невиявлення нею кіберзагроз є меншим, ніж при використанні традиційної

системи захисту (0,49 та 0,63 відповідно), а також вона дозволяє скоротити рівень уразливості системи на 59,38 %.

4. У підрозділі 5.3 запропоновано трирівневу систему попередження кіберзагроз та продемонстровано ефективність її використання у фінансовому секторі національної економіки (для прикладу). Перший рівень цієї системи («організаційний») передбачає створення необхідних умов для ефективного функціонування ключових процесів захисту інформації, вчасного виявлення «вузьких» місць, що стають причиною неконтрольованого витоку інформації або втручання кіберзлочинців. У цьому контексті запропоновано науково-методичний підхід до моделювання та оптимізації бізнес-процесів у системі забезпечення інформаційної безпеки, що реалізовано шляхом побудови моделей ключових процесів інформаційного захисту в нотації BPMN 2.0 із використанням програмного забезпечення «Bizagi Modeller». Підхід передбачає таку послідовність заходів: 1) моделювання існуючих процесів захисту інформації; 2) проведення симуляційних експериментів залежно від витрат часу та ресурсів при здійсненні окремої операції та виявлення на цій основі «вузьких» місць; 3) моделювання процесів захисту інформації з урахуванням проведених оптимізаційних процедур та ліквідації виявлених недоліків; 4) проведення повторних симуляційних експериментів із метою підтвердження ефективності внесених змін до системи захисту інформації. Його було апробовано на прикладі банків України, для яких розроблено механізм поєднання технологій первинного фінансового моніторингу та кібербезпеки, що дозволило оптимізувати процеси автоматизованої ідентифікації й верифікації клієнтів, перевірки транзакцій на ознаки зовнішніх кібершахрайств та загроз із боку інсайдерів.

5. Другий рівень цієї системи («інформаційний») передбачає ефективне формування наборів даних за ключовими ознаками, що ідентифікують будь-яку операцію як кіберзлочинну. У роботі з використанням імовірнісних дерев рішень запропоновано будувати портрети кібершахраїв та жертв на основі статистичних даних щодо реальних випадків кіберзлочинів. Обґрунтовано, що ці дані повинні централізовано збирати органи державної статистики поряд із даними фінансової

звітності, підлягати аналізу та класифікації. Усе це повинне сприяти виявленню набору ключових ознак кіберінцидентів, із якими зіштовхуються різні економічні агенти залежно від типів їх інформаційних систем, характеру втраченої інформації, рівня фінансових втрат тощо. На підставі даних агентства звітності споживчого кредитування «Experian» проведено ідентифікацію кіберзлочинів стосовно кредитних операцій. Інформаційну базу цього дослідження сформували дані щодо персональних ознак кібершахраїв та їх жертв (вік, стать і соціальний статус), на основі яких оцінено їх імовірний розподіл за гілками дерева рішень. Моделювання засвідчило, що потенційними кредитними кіберзлочинцями є переважно чоловіки віком до 24 років, які здобули вищу освіту, або віком 25-29 років, які мають обмежений дохід та не мають власного житла, а потенційними жертвами – чоловіки віком 60+, які мають стабільний високий дохід.

6. Третій рівень цієї системи («алгоритмічний») передбачає створення алгоритмів попередження та виявлення ознак кіберзагроз, які дозволяють посилити захист інформації. За допомогою нейромережевого моделювання процесу виявлення ознак кібершахрайств (в аналітичному пакеті «STATISTICA») запропоновано обирати ключові ознаки, що ідентифікують конкретний вид кіберінциденту. Побудована нейронна мережа дозволяє аналізувати операції або процеси щодо наявності відповідної комбінації ознак, виявляти ті з них, які найімовірніше мають ознаки кіберзагроз та потребують підвищеної уваги. У роботі побудовано нейромережеву модель для набору з 5 000 транзакцій із банківськими кредитними картками, яка дозволила виявити кібершахрайські транзакції за такими ключовими ознаками, як частота та ліміт щоденного використання картки, обсяг транзакцій, інтервал часу між ними та ін. Перевірка моделі на адекватність показала 100 % збіг прогнозних результатів за трьома тестовими підвибірками.

Основні положення п’ятого розділу дисертаційної роботи опубліковано авторкою в роботах [160, 205, 227, 317, 318, 319, 380, 395, 396, 400, 401, 404, 405, 407, 408, 409].

ВИСНОВКИ

У дисертації подано розроблення нових та вдосконалення існуючих методологічних підходів і методичного інструментарію формування ефективної системи інформаційної безпеки з урахуванням її впливу на розвиток національної економіки в цілому та її окремих секторів. Одержані результати дослідження дозволили зробити такі висновки:

1. Аналіз наукових напрацювань щодо трактування поняття «інформаційна безпека» дозволив виявити існування двох підходів до її визначення, що характеризують її або через функціональне навантаження, або через суб'єктів та не враховують її багатокомпонентності та динамічності. Запропоноване в роботі нове визначення дозволило врахувати мету функціонування інформаційної безпеки, суб'єктно-об'єктну узгодженість її інструментів та механізмів впливу з урахуванням специфіки структури національної економіки. У результаті це сприяло формуванню концепції забезпечення інформаційної безпеки в системі управління національної економіки, що визначає передумови формування інформаційної безпеки, її наслідки, об'єкти, суб'єкти залежно від рівнів національної економіки, а також інструменти та механізми її забезпечення.

2. Динамічний аналіз кількості наукових публікацій засвідчив зростання зацікавленості проблематикою інформаційної безпеки лише за останні 20 років, що підтверджено 97 % обсягу публікацій за період 2000–2019 рр. порівняно з 3 % за період 1967–1999 рр. Дослідження інформаційної безпеки в розрізі предметних галузей економічного напрямку виявило відсутність домінування окремих наукових шкіл та наявність 7 векторів наукового вивчення проблематики інформаційної безпеки. Одержані результати дозволили виділити ключові її аспекти, що потребують поглибленого дослідження та вдосконалення для потреб національної економіки.

3. Аналіз взаємовпливів між показниками цифрової спроможності національної економіки і кібербезпеки та групами індикаторів інституційної

спроможності держави, економічного, соціального та фінансового розвитку національної економіки, зовнішньоекономічної діяльності, інноваційної активності, якості інформаційної інфраструктури дозволив одержати найбільш релевантні показники на основі статистично підтвердженого зв'язку, якими виявилися індикатори інституційної спроможності держави. Результати засвідчили існування впливу держаної політики на забезпечення системи інформаційної безпеки, а також її потенційних можливостей драйвера для національної економіки країни.

4. Запропонований інтегральний індекс інформаційної безпеки національної економіки дозволив сформувати рейтинг країн світу, внаслідок цього було виявлено 5 груп країн, яким відповідають рівні розвитку інформаційної безпеки національної економіки: дуже добре, добре, задовільно, погано, дуже погано. Україна ввійшла до переліку тих країн, рівень інформаційної безпеки національної економіки яких було оцінено як задовільно, що більшою мірою обумовлено розривами за субіндексами інституційної спроможності країни, ніж за субіндексами цифрової спроможності та кібербезпеки. Це дозволило сформувати відповідні таргети державної політики для підвищення рівня забезпечення інформаційної безпеки.

5. На основі проведеного кластерного аналізу і DEA-аналізу виявлено 7 кластерів країн за інтегральним рівнем їх інформаційної безпеки національної економіки та показниками інституційної та цифрової спроможності й кібербезпеки. У результаті визначено структурну не-ефективність для кожного кластеру країн, що показало недостатню забезпеченість поточного стану інформаційної безпеки національної економіки для країн 2-го, 4-го та 6-го кластерів, а також структурну неефективність усіх кластерів для досягнення максимального рівня інформаційної безпеки національної економіки. Для України забезпечення системи інформаційної безпеки національної економіки відбувається лише на рівні 63,7 %, що є наслідком неефективності блоку показників інституційної спроможності, які потребують їх покращання від 8,91 % до 88,57 %, що сприятиме максимальному зростанню ефективності системи

інформаційної безпеки національної економіки на 57,04 %.

6. Проведене дослідження закономірностей формування в національній економіці моделей забезпечення персональної інформаційної безпеки населення дозволило виявити 7 кластерів країн ЄС, сформованих за домінуючими заходами персональної інформаційної безпеки та наслідками її порушення. У результаті підтверджено, що існує вплив заходів органів державної влади на наслідки кіберінцидентів та існують залежності між рівнем добробуту, національних суспільних традицій, ментальних і культурних особливостей країни та заходів персональної безпеки, яким надає переваги населення європейських країн. Це сприятиме формуванню урядовими організаціями країн заходів, цілеспрямованих на підтримку цифрової освіти для населення та формування їх національних па-тернів забезпечення персональної інформаційної безпеки.

7. У роботі було доведено, що між показниками цифрової спроможності та кібербезпеки й ризиком відмивання коштів існує тісний зворотний зв'язок, що свідчить про важливу роль інформаційної безпеки в забезпеченні процесів протидії легалізації коштів. Визначений рівень привабливості країн для здійснення легалізації з боку українських контрагентів виявив, що найбільш привабливими країнами є ті, що мають низький рівень кібербезпеки. Результати щодо привабливості України для відмивання коштів з боку контрагентів інших країн дозволили визначити перелік тих, для яких вона є найбільш привабливою. Одержаний висновок сприятиме вдосконаленню регуляторної політики щодо підвищення міжнародних та національних вимог, особливо в частині перевірки на предмет додержання норм законодавства та ідентифікації джерел отримання доходів, а також конвергенції систем кібербезпеки й фінансового моніторингу для підвищення ефективності інформаційної безпеки.

8. Моделювання інформаційних активностей, ідентифікованих для кіберзагроз, хакерських атак, витоків інформації тощо в глобальному цифровому просторі дозволило виявити чотири «інформаційні бульбашки» в трирічній ретроспективі. Також було визначено, що середня тривалість періоду поширення дезінформації внаслідок глобальних кіберінцидентів – 7 днів, а стабілізація

цифрових економічних операцій після розриву бульбашки починається з 10-го дня. Одержані результати довели існування дестабілізаційних впливів інформаційного середовища на національної економіки країни, що сприятиме їх виявленню та попередженню колапсів у різних секторах національної економіки.

9. Використані методи багатоатрибутного прийняття рішень дозволили виявити таргети та напрямки реформування системи забезпечення інформаційної безпеки в Україні. Визначено, що найбільш критичним є система аналізу та інформації про кіберзагрози, менеджмент кіберкриз, діяльність державних органів України щодо здійснення її внеску в глобальну кібербезпеку та щодо організації військових кібероперацій. Це сприяло розробленню комплексу заходів державної політики забезпечення інформаційної безпеки національної економіки в цьому напрямку.

10. Обґрунтування пріоритетів формування державних секторальних та галузевих програм у напрямку забезпечення інформаційної безпеки національної економіки дозволило визначити, що найбільш уразливими до наслідків кіберзагроз є групи підприємств кількістю до 500 осіб. Також для кожної з п’яти галузей було встановлено граничний діапазон витрат на інформаційної безпеки, додержання якого є економічно доцільним. Так, для страхових компаній він може бути найбільшим, для постачальників послуг – найменшим. Це дозволило запропонувати систему державних заходів для забезпечення стандартизації та сертифікації, контролю й моніторингу у сфері інформаційної безпеки.

11. Для забезпечення стійкості розвитку країни необхідно додержуватися збалансованого розвитку всіх її сфер. Запропонована в роботі чотириполюсна барицентрична модель, побудована для країн світу з урахуванням рівня їх економічного, політичного, соціального розвитку та розвитку цифрової спроможності і кібербезпеки, дозволила проранжувати їх за рівнем збалансованості розвитку та виділити найбільш незбалансовані їх сфери. Також було виявлено, що Україна є аутсайдером серед країн, але найбільш перспективним чинником є композитний індикатор цифрової спроможності та кібербезпеки, потенціал якого є драйвером розвитку всіх інших сфер

національної економіки.

12. Запропонована методика експрес-оцінювання ризиків втрат інформації та даних незалежно від суб'єкта інформаційної безпеки дозволяє визначати найбільш імовірні каталізатори інцидентів з урахуванням частоти їх повторення та грошового оцінювання збитків від втрат інформації. Визначені 5 груп інцидентів та 66 факторів впливу на них можна використовувати як універсальні параметри для побудови карти ризиків. Розрахована ймовірність за її секторами дозволяє одержати потенційні ризикові фактори інцидентів та посилити управлінські заходи щодо забезпечення інформаційної безпеки саме для цього напрямку загроз.

13. Ребілдинг систем захисту необхідний в умовах зростання рівня загроз, які діюча система не визначає. Необґрунтована реалізація цього процесу може призвести до значних фінансових втрат. Запропонований у роботі підхід системно-динамічного моделювання дозволяє здійснити симуляцію варіантів реалізації новітніх технологій захисту порівняно з традиційними. Апробація методики для умов упровадження блокчейн-технології в систему інформаційної безпеки дозволила визначити її ефективність за такими параметрами: середнім ризиком невиявлення кіберзагроз побудованою на основі блокчейн-технології системою, який виявився меншим, ніж під час використання традиційної системи захисту (0,49 та 0,63 відповідно); рівень вразливості системи скоротиться на 59,38%.

14. Запропонована в роботі трирівнева система попередження фінансових кіберзагроз дозволяє: 1) здійснити моделювання та оптимізацію ключових бізнес-процесів захисту інформації виявлення «вузьких» місць, які є причиною неконтрольованого її витоку або втручання кіберзлочинців; 2) розробити портрети ймовірних жертв та кіберзлочинців та проводити ідентифікацію суб'єктів операцій за різними критеріями, що відповідають ознакам кіберзлочинів; 3) будувати нейронні мережі та за їх допомогою ідентифікувати операції з ознаками кіберзлочинів. Результати апробованих у фінансовому секторі рішень сприяли попередженню фінансових кіберзагроз у банківських транзакціях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 2014 Cost of Data Breach Study: Global Analysis. *Century Business Solutions* : website. URL: https://centurybizsolutions.net/wp-content/uploads/2014/12/IBM.pdf.

2. 2017 Cost of Data Breach Study. Global Overview. *IBM* : website. URL: https://www.ibm.com/downloads/cas/ZYKLN2E3.

3. 2018 Cost of a Data Breach Study: Global Overview. *IBM* : website. URL: https://www.ibm.com/downloads/cas/861MNWN2.

4. 2018 Social Progress Index. Social Progress Imperative. *Deloitte* : website. URL: https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/ deloitte-analytics/ Estudios/2018-Social-Progress-Index-brief.pdf.

5. 2019 Cost of a Data Breach Report. *All About Security* : website. URL: https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_ of_a_Data_Breach_Report_final.pdf.

6. 2020 Social Progress Index. *Social Progress Imperative* : website. URL: https://www.socialprogress.org/.

7. About The Index. 2020 Index of Economic Freedom. *The Heritage Foundation* : website. URL: https://www.heritage.org/index/about#:~:text=What %20is%20economic%20freedom%3F,in%20any%20way%20they%20please.

8. Akhmedov F., Zeitoun M.S. Optimising the value-at-risk model in banks in India to adequately quantify market risks in emerging markets. *International Journal of Economic Policy in Emerging Economies*. 2019. Vol. 12(4). P. 337 - 347. DOI: https://doi.org/10.1504/IJEPEE.2019.104623.

9. Akram S.M., Al-Kenani A.N., Alcantud J.C.R. Group Decision-Making Based on the VIKOR Method with Trapezoidal Bipolar Fuzzy Information. *Symmetry*. 2019. Vol. 11. P. 1313. DOI: https://doi.org/10.3390/sym11101313.

10. Aldhous P. A Security Breach Exposed More Than One Million DNA Profiles On A Major Genealogy Database. *BuzzFeedNews :* website. URL: https://www.buzzfeednews.com/article/peteraldhous/hackers-gedmatch-dna-privacy.

11. Alibeki H., Samsonov M. Stress testing and elements of consolidated supervision as key instruments for enhanced risk-oriented monitoring of banks' activities. *Financial Markets, Institutions and Risks*. 2017. Vol. 1(4). P. 37-46. DOI: https://doi.org/10.21272/fmir.1(4).37-46.2017.

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

13. Anderson R., Moore T. The economics of information security. *Science*. 2006. Vol. 314(5799). P. 610-613. DOI: https://doi.org/10.1126/science.1130992.

14. Anscombe T. Beware scams exploiting coronavirus fears. *WeLiveSecurity* : website. URL: https://www.welivesecurity.com/2020/03/13/beware-scams-exploiting-coronavirus-fears/.

15. Aryani D.N., Hussainey K. The determinants of risk disclosure in the Indonesian non-listed banks. *International Journal of Trade and Global Markets.* 2017. Vol. 10(1). P. 58 - 66. DOI: https://doi.org/10.1504/IJTGM.2017.082376.

16. Bangladesh may soon get $15.25 million of stolen reserve money. The *Economic Times*. 07 November 2016. URL: https://economictimes.indiatimes.com/news/international/world-news/bangladesh-may-soon-get-15-25-million-of-stolen-reserve-money/articleshow/55295915.cms.

17. Banker R.D., Charnes A., Cooper W.W. Some Models for Estimating Technical and Scale Inefficiencies in Data Envelopment Analysis. *Managment Science.* 1984. Vol. 30(9). P. 1031-1142. DOI: https://doi.org/10.1287/mnsc.30.9.1078.

18. Banking Is Only The Beginning: 58 Big Industries Blockchain Could Transform. *CBINSIGHTS* : web-site. URL: https://www.cbinsights.com/research/industries-disrupted-blockchain/.

19. Barmuta K., Ponkratov V. V., Maramygin M., Kuznetsov N. V., Ivlev V. Ivleva M. Mathematical model of optimizing the balance sheet structure of the Russian banking system with allowance for the foreign exchange risk levels. *Entrepreneurship*

and Sustainability Issues. 2019. Vol. 7(1). P. 484-497. DOI: https://doi.org/10.9770/jesi.2019.7.1(34).

20. Basel AML Index 2018. Report. *Basel Institute on Governance* : website. URL: https://baselgovernance.org/sites/default/files/2019-02/basel_aml_index_10_09_2018.pdf.

21. Basel AML Index. *Basel Institute on Governance* : website. URL: https://baselgovernance.org/basel-aml-index#:~:text=The%20Basel%20AML%20Index%20is,%2FTF)%20around%20the%20world.

22. Bekmuratov T.F., Ganiev A.A., Botirov F.B. Concept of establishing multi-agent intellectual automatically systems in the enterprise. *International Journal of Scientific and Technology Research.* 2020. № 9(4). P. 347-352.

23. 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.

24. 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.

25. Bilan Y., Brychko M., Buriak A., Vasilyeva T. Financial, business and trust cycles: The issues of synchronization | [Ciklusi financiranja, poslovanja i povjerenja: pitanja za sinkronizaciju]. *Zbornik Radova Ekonomskog Fakultet au Rijec*i. 2019. Vol. 37(1). P. 113-138. DOI: https://doi.org/10.18045/zbefri.2019.1.113.

26. Bilan Y., Đšuzmenko Đž., Boiko A. Research on the impact of industry 4.0 on entrepreneurship in various countries worldwide. In *Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019* : Education Excellence and Innovation Management through Vision 2020. P. 2373-2384. URL: https://ibima.org/accepted-paper/research-on-the-impact-of-industry-4-0-on-entrepreneurship-in-various-countries-worldwide/.

27. Bilan Y., Rubanov P., Vasylieva T., Lyeonov S. The influence of industry 4.0 on financial services: Determinants of alternative finance development | [Wpływ przemysłu 4.0 na usługi finansowe: determinanty rozwoju alternatywnych finansów]. *Polish Journal of Management Studies.* 2019. Vol. 19(1). P. 70-93. DOI: https://doi.org/10.17512/pjms.2019.19.1.06.

28. Blockchain. *TADVISER* : website. URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD_(Blockchain)#.D0.9A.D0.B8.D0.B1.D0.B5.D1.80.D0.B1.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D0.BE.D1.81.D1.82.D1.8C.

29. Blumbergs B. Technical Analysis of Advanced Threat Tactics Targeting Critical Information Infrastructure. *Cyber Security Review*. 2014. Winter. P. 1-12. URL: https://web.archive.org/web/20160319085736/https://ccdcoe.org/sites/default/files/multimedia/pdf/2014-Technical%20Analysis%20of%20Advanced%20Threat%20Tactics%20Targeting%20Critical%20Information%20Infrastructure.pdf.

30. Bodoni S. Mastercard Alerts Privacy Watchdogs After Loyalty Program Leak. *Bloomberg :* website. URL: https://www.bloomberg.com/news/articles/2019-08-23/mastercard-tells-belgian-german-privacy-watchdogs-of-breach.

31. Böhme R., Nowey T. Economic security metrics. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2008. № 4909. P. 176-187. DOI: https://doi.org/10.1007/978-3-540-68947-8_15.

32. Boiarko I., Samusevych Y. Role of intangible assets in company's value creation. *Actual Problems of Economics*. 2011. Vol. 117(3). P. 86-94. URL: https://www.researchgate.net/publication/292366060_Role_of_intangible_assets_in_company's_value_creation.

33. Boyko A., Roienko V. Risk assessment of using insurance companies in suspicious transactions. *Economic Annals-XXI*. 2014. Vol.11-12. P. 73-76. URL: http://soskin.info/userfiles/file/2014/11-12_2014/Boyko_Roienko.pdf.

34. Brahmana R., Tan J. H. Disclosing risk information by Malaysian firms: a trend and the determinants. *International Journal of Economic Policy in Emerging Economies*.2018. Vol. 11(5). P. 457 - 469. DOI: https://doi.org/10.1504/IJEPEE.2018.094804.

35. Breached Records More Than Doubled in H1 2018, Reveals Breach Level Index. *Digital Identity & Security Blog* : website. URL: https://blog.gemalto.com/security/2018/10/09/breached-records-more-than-doubled-in-h1-2018-reveals-breach-level-index/.

36. Bryant W.D. Cyberspace superiority. A conceptual model. *Air & Space Power Journal*. 2013. Vol. 29(2). P. 103-128.

37. Budanović N. The largest battlefield in history – 30 Cyber warfare statistics. *DataProt* : website. URL: https://dataprot.net/statistics/cyber-warfare-statistics/.

38. Buriak A., Artemenko A. Reputation risk in banking: application for Ukraine. *Financial Markets, Institutions and Risks*. 2018. Vol. 2(2). P. 100-110. DOI: https://doi.org/10.21272/fmir.2(2).100-110.2018.

39. Burke W., Oseni T., Jolfaei A., Gondal I. Cybersecurity Indexes for eHealth. In *Proceedings of the 2019 Australasian Computer Science Week Multiconference, ACSW 2019 (Australia, Sydney, January, 2019)*. ACM International Conference Proceeding Series, 2019. Vol. 17. P. 1-8. https://dl.acm.org/doi/10.1145/3290688.3290721.

40. Business Process Model and Notation (BPMN) Version 2.0. *Object Management Group* : the official website. URL: http://www.omg.org/spec/BPMN/2.0.

41. 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.

42. Cardholm L. Identifying the business value of information security. *Banking, Finance, and Accounting: Concepts, Methodologies, Tools, and*

Applications. Management Association, 2015. P. 1056-1079. DOI: https://doi.org/10.4018/978-1-4666-6268-1.ch058.

43. CB Insights says enterprise blockchain funding less than 20% of cryptocurrencies. But is it?. *Ledger Insights* : website. URL: https://www.ledgerinsights.com/cb-insights-enterprise-blockchain-funding/.

44. Chatterjeea P., Chakraborty S. A comparative analysis of VIKOR method and its variants. *Decision Science Letters*. 2016. № 5. P. 469–486. DOI: https://doi.org/10.5267/j.dsl.2016.5.004.

45. 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. Vol. 57(2). P. 245–285. DOI: https://doi.org/10.1007/s10115-017-1144-z.

46. Cherdantseva Y., Hilton J. Understanding Information Assurance and Security. In book: F. Almeida, and I. Portela (eds.), Organizational, Legal, and Technological Dimensions of IS Administrator. Publisher: IGI Global Publishing, 2013. P. 32. DOI: https://doi.org/10.4018/978-1-4666-4526-4.ch010.

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

48. Chyzhmar K., Dniprov O., Korotiuk O., Shapoval R., Sydorenko O. State information security as a challenge of information and computer technology development. *Journal of Security and Sustainability Issues*. 2020. Vol. 9(3). P. 819-828. DOI: https://doi.org/10.9770/jssi.2020.9.3(8).

49. Cimpanu C. Magento online stores hacked in largest campaign to date. *ZDNet* : website. URL : https://www.zdnet.com/article/magento-online-stores-hacked-in-largest-campaign-to-date/.

50. Cimpanu C. Exclusive: Details of 10.6 million MGM hotel guests posted on a hacking forum. *ZDNet* : website. URL :https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/.

51. Claims on central government, etc. (% GDP). *The World Bank* : website. URL: https://data.worldbank.org/indicator/FS.AST.CGOV.GD.ZS.

52. Clarke R.A. Cyber war. The next threat to national security and what to do about it. *New York: Ecco*. 2010.

53. Coelho R., De Simoni M., Prenio J Suptech applications for anti-money laundering. *FSI Insights on policy implementation*. 2019. Vol. 18. P. 1-18. URL: https://www.bis.org/fsi/publ/insights18.pdf.

54. Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010. *Center for Homeland Defense and Security* : website. URL: https://www.hsdl.org/?abstract&did=7447.

55. Corruption Perception Index 2018. *Trancparency International* : website. URL: https://www.transparency.org/files/content/pages/2018_CPI_Executive Summary.pdf.

56. Corruption perceptions - Transparency International - Country rankings. *The GlobalEconomy.com* : website. URL: https://www.theglobaleconomy.com/rankings/transparency_corruption/.

57. Cost of a Data Breach Report 2020. *IBM Security* : website. URL: https://www.ibm.com/downloads/cas/RZAX14GX.

58. Cost of Insider Threats: Global Report 2020. *IBM Security* : website. URL: https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/.

59. Cox J. GCHQ Says Hackers Have Likely Compromised UK Energy Sector Targets. *Vice Media Group* : website. URL: https://www.vice.com/en/article/9kwg4a/gchq-says-hackers-have-likely-compromised-uk-energy-sector-targets.

60. Crilley K. Information warfare: New battlefields Terrorists, propaganda and the Internet. *Aslib Proceedings.* 2001. Vol. 53(7). P. 250-264. DOI: https://doi.org/10.1108/EUM0000000007059.

61. Crime Index by Country 2018. *NUMBEO* : website. URL: https://www.numbeo.com/crime/rankings_by_country.jsp?title=2018.

62. Cyberthreat real-time map. *Kaspersky* : website. URL: https://cybermap.kaspersky.com/.

63. Dabbura I. K-means Clustering: Algorithm, Applications, Evaluation Methods, and Drawbacks. *Towards Data Science* : website. URL: https://towardsdatascience.com/k-means-clustering-algorithm-applications-evaluation-methods-and-drawbacks-aa03e644b48a.

64. Data Protection in a Multi-Cloud World. *DELL Technologies* : website. URL: https://www.dellemc.com/lv-lv/collaterals/unauth/infographic/products/data-protection/global-data-protection-index-2020-snapshot.pdf

65. Data Science K-means Clustering – In-depth Tutorial with Example. *DataFlair* : website. URL: https://data-flair.training/blogs/k-means-clustering-tutorial/.

66. Deane J.K., Goldberg D.M., Rakes T.R., Rees L.P. The effect of information security certification announcements on the market value of the firm. *Information Technology and Management.* 2019. № 20(3). P. 107-121. DOI: https://doi.org/10.1007/s10799-018-00297-3.

67. Democracy Index 2018: Me too? Political participation, protest and democracy. A report by The Economist Intelligence Unit. *The Economist* : website. URL: https://275rzy1ul4252pt1hv2dqyuf-wpengine.netdna-ssl.com/wp-content/uploads/2019/01/Democracy_Index_2018.pdf.

68. Democracy Index. *Gapminder* : website. URL: https://www.gapminder.org/data/documentation/democracy-index/.

69. Dennis J.B. A position paper on computing and communications. In *Proceedings of the 1st ACM Symposium on Operating Systems Principles, SOSP, 1 -4 October 1967.* 1967. P. 6.1-6.10. DOI: https://doi.org/10.1145/800001.811671.

70. Dincelli E. The role of national culture in shaping information security and privacy behaviors. *World Scientific Reference on Innovation:Volume 4: Innovation in Information Security.* USA : Arizona State University; Siegel D., 2018. P. 47-68. DOI: https://doi.org/10.1142/10209.

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

72. Dmitrov O.S., Goncharov K.G., Merenkova O.V., Medvid T.A., Boyko A.O., Vakhnyuk S.V. Simulation of commercial bank operational risk assessment [Modeliuvannia otsinky operatsiinoho ryzyku komertsiinoho banku]. Sumy: State Higher Education Institution "Ukrainian Banking Academy of the National Bank of Ukraine". 2010.

73. Dmytrov S., Medvid T. An approach to the use of indices-based analysis subject to money laundering and terrorist financing national risk assessment. *SocioEconomic Challenges*. 2017. Vol. 1(1). P. 35-47. DOI: https://doi.org/10.21272/sec.2017.1-04.

74. Doing Business 2018. Reforming to Create Jobs : A World Bank Group Flagship Report. *Doingbusiness.org* : website. URL: https://www.doingbusiness.org/content/dam/doingBusiness/media/Annual-Reports/English/DB2018-Full-Report.pdf.

75. Download VOSviewer. *VOSviewer* : website. URL: https://www.vosviewer.com/download.

76. Droege C. Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross.* 2013. Vol. 94(886). P. 533-578. DOI: https://doi.org/10.1017/S1816383113000246.

77. Duddu V. A survey of adversarial machine learning in cyber warfare. *Defence Science Journal*. 2018. Vol. 68(4). P. 356-366.

78. Dumas E. Mobile adware: The Silent Plague with No Origin. *CXOtoday.com :* website. URL: https://www.cxotoday.com/news-analysis/mobile-adware-the-silent-plague-with-no-origin/.

79. Dutta S., Lanvin B. The Network Readiness Index 2019: Towards a Future-Ready Society. *Networkreadinessindex.org* : website. URL: https://networkreadinessindex.org/wp-content/uploads/2020/03/The-Network-Readiness-Index-2019-New-version-March-2020.pdf.

80. Dvorský J., Schönfeld J., Kotásková A., Petráková Z. Evaluation of important credit risk factors in the SME segment. *Journal of International Studies*. 2018. Vol. 11(3). P. 204-216. DOI: https://doi.org/10.14254/2071-8330.2018/11-3/17.

81. Dykha M. V., Liubokhynets L., Tanasiienko N. P., Moroz S., Poplavska O. Elimination of the influence of investment, financial and operational risks on the organisation economic security. *Journal of Security and Sustainability*. 2019. Vol. 9(1). P. 13-26. DOI: https://doi.org/10.9770/jssi.2019.9.1(2).

82. Dziwok E. New approach to operational risk measurement in banks. *International Journal of Trade and Global Markets*. 2018. Vol. 11(4). P. 259 - 269. DOI: https://doi.org/10.1504/IJTGM.2018.097276.

83. E2: Uneven Economic Development. *Fragile States Index :* website. URL: https://fragilestatesindex.org/indicators/e2/.

84. Economic freedom, overall index - Country rankings. *The GlobalEconomy.com* : website. URL: https://www.theglobaleconomy.com/rankings/economic_freedom/.

85. Economic Impact of Cybercrime - No Slowing Down. *McAfee* : website. URL: https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/mcafee/economic-impact-of-cybercrime-not-slowing-down.pdf.

86. e-Governance Academy Foundation. (2020). National Cyber Security Index. *NCSI* : website. URL: https://ncsi.ega.ee/ncsi-index/.

87. Evana E., Metalia M., Mirfazli E., Georgieva D.V., Sastrodiharjo I., Business Ethics in ProvidingFinancial Statements: The Testing of Fraud Pentagon Theory on the Manufacturing Sector in Indonesia. *Business Ethics and Leadership.* 2019. Vol. 3(3). P. 68-77. DOI: https://doi.org/10.21272/bel.3(3).68-77.2019.

88. Fenton N., Neil M. Risk assessment and decision analysis with bayesian networks. In *Risk Assessment and Decision Analysis with Bayesian Networks*. CRC Press, 2012. P. 1-494. DOI: https://doi.org/10.1201/b21982.

89. Financial Development Index Database. *International Monetary Fund* : website. URL: https://data.imf.org/?sk=f8032e80-b36c-43b1-ac26-493c5b1cd33b.

90. Financial Secrecy Index. *Tax Justice Network* : website. URL: https://fsi.taxjustice.net/en/introduction/introducing-the-fsi.

91. Franceschi-Bicchierai L. Hackers Connected to NotPetya Ransomware Surface Online, Empty Bitcoin Wallet. *Vice* : website. URL: https://www.vice.com/en/article/8xagk4/hackers-connected-to-notpetya-ransomware-surface-online-empty-bitcoin-wallet.

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

93. Fu I., Ravichandran D. K Means Clustering of Sports Images. *Medium* : website. URL: https://medium.com/gumgum-tech/k-means-clustering-of-sports-images-4d2e1d8c4572.

94. Galinec D., Moznik D., Guberina B. Cybersecurity and cyber defence: national level strategic approach. *Automatika*. 2017. Vol. 58(3). P. 273-286. DOI: https://doi.org/10.1080/00051144.2017.1407022.

95. Gallagher S. FBI-DHS “amber” alert warns energy industry of attacks on nuke plant operators. *Ars Technica* : website. URL: https://arstechnica.com/information-technology/2017/07/dhs-fbi-warn-of-attempts-to-hack-nuclear-plants/.

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

97. Garcia A., Calle L., Raymundo C., Dominguez F., Moguerza J.M. Personal data protection maturity model for the micro financial sector in Peru. 4th International Conference on Computer and Technology Applications, ICCTA 2018, Istanbul, Turkey, 3 May 2018 through 5 May 2018. Istanbul, 2018. P. 20-24. DOI: https://doi.org/10.1109/CATA.2018.8398649.

98. GDP per capita (current US$). *The World Bank* : website. URL: https://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

99. Ghaleb A. M., Kaid H., Alsamhan A., Mian S. H., Hidri L. Assessment and Comparison of Various MCDM Approaches in the Selection of Manufacturing

Process. *Advances in Materials Science and Engineering*. 2020. DOI: https://doi.org/10.1155/2020/4039253.

100. Ghernouti-Hélie S. A national strategy for an effective cybersecurity approach and culture. *Fifth International Conference on Availability, Reliability and Security*, ARES 2010, Krakow, Poland, 15-18 February 2010. IEEE Computer Society, 2010. P. 370-373.

101. Gilbert D. Angela Merkel hacked: Bundestag computers targeted with malware by Russian cyberattack. *International Business Times* : website. URL: https://www.ibtimes.co.uk/angela-merkel-hacked-bundestag-computers-targeted-malware-by-russian-cybercriminals-1506131#.

102. Global Cybersecurity Index. *International Telecommunication Union* : website. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

103. Global Terrorism Index 2018. Measuring the impact of terrorism. *Institute for economics & peace :* URL: https://reliefweb.int/sites/reliefweb.int/files/resources/Global-Terrorism-Index-2018-1.pdf.

104. Global Web Statistics. *Statoperator* : website. URL: https://statoperator.com/.

105. Glossary of terms. *ISACA* : website. URL: http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf.

106. Gnatyuk S., Sydorenko V., Polozhentsev A., Fesenko A., Akatayev N., Zhilkishbayeva G. Method of cybersecurity level determining for the critical information infrastructure of the state. In *2nd International Workshop on Control, Optimisation and Analytical Processing of Social Networks, COAPSN 2020*, Lviv, Ukraine, 21 May 2020. CEUR Workshop Proceedings, 2020. Vol. 2616. P. 332-341.

107. Gordon L.A., Loeb M.P. The Economics of Information Security Investment. ACM Transactions on Information and System Security. 2002. № 5(4). P. 438-457. DOI: https://doi.org/10.1145/581271.581274.

108. Government effectiveness - Country rankings. *The GlobalEconomy.com* : website. URL: https://www.theglobaleconomy.com/rankings/wb_government_effectiveness/.

109. Government Effectiveness. *The World Bank* : website. URL: https://info.worldbank.org/governance/wgi/pdf/ge.pdf.

110. Hammerström L., Giebe C., Zwerenz D. Influence of Big Data & Analytics on Corporate Social Responsibility. *SocioEconomic Challenges.* 2019. Vol. 3(3). P. 47-60. DOI: https://doi.org/10.21272/sec.3(3).47-60.2019.

111. Happiness index - Country rankings. *The GlobalEconomy.com* : website. URL: https://www.theglobaleconomy.com/rankings/happiness/.

112. Harrington E. The Desirability Function. *Industrial Quality Control*. 1965. Vol. 21(10). P. 494-498.

113. Heckman K.E., Walsh M.J., Stech F.J., O'Boyle T.A., Dicato S.R., Herber A.F. Active cyber defense with denial and deception: A cyber-wargame experiment. *Computers and Security*. 2013. Vol. 37. P. 72-77. DOI: https://doi.org/10.1016/j.cose.2013.03.015.

114. Helísek M. Exchange Rate Mechanism II and the risk of currency crisis – empiricism and theory. *Journal of International Studies*. 2019. Vol. 12(1). P. 297-312. DOI: https://doi.org/10.14254/2071-8330.2019/12-1/20.

115. Hern A., Gibbs S. What is WannaCry ransomware and why is it attacking global computers? *The Guardian.* 2017. URL: https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20.

116. Hrytsenko L., Boiarko I., Ryabenkov O., Didenko O. Assessment of the Value Loss Risk in Response to the Enterprise's Innovative Transformations. *Marketing and Management of Innovations*. 2019. Vol. 1. P. 229-237. DOI: https://doi.org/10.21272/mmi.2019.1-19.

117. Hrytsenko L.L., Krasulya T.Y. Risk management at realization of infrastructure projects under public-private partnership. *Actual Problems of Economics.* 2011. Vol. 126(12). P. 85-90. URL: https://www.researchgate.net/

publication/298002936_Risk_management_at_realization_of_infrastructure_projects_under_public-private_partnership.

118. Hudáková M., Dvorský J. Assessing the risks and their sources in dependence on the rate of implementing the risk management process in the SMEs. *Equilib-rium. Quarterly Journal of Economics and Economic Policy*. 2018. Vol. 13(3). P. 543–567. DOI: https://doi.org/10.24136/eq.2018.027.

119. Hudakova M., Masar M., Luskova M., Patak M.R. The Dependence of Perceived Business Risks on the Size of SMEs. *Journal of Competitiveness*. 2018. Vol. 10(4). P. 54-69. DOI: https://doi.org/10.7441/joc.2018.04.04.

120. Human Development Index (HDI). Human Development Reports. *United Nations Development Programme* : website. URL: http://hdr.undp.org/en/indicators/137506.

121. Human Development Report 2019. Beyond income, beyond averages, beyond today: Inequalities in human development in the 21st century. Human Development Reports. *United Nations Development Programme* : website. URL: http://hdr.undp.org/sites/default/files/hdr2019.pdf.

122. Hwang C.L., Yoon K. Multiple Attribute Decision Making: Methods and Applications. New York: Springer-Verlag. 1981. DOI: 10.1007/978-3-642-48318-9.

123. Individuals - internet activities. *Eurostat* : website. URL: https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_ac_i/default/table?lang=en

124. Information Security Resources. *SANS* : website. URL: https://www.sans.org/information-security.

125. Information security. *Wikipedia* : website. URL: https://en.wikipedia.org/wiki/Information_security#cite_note-1.

126. Integration of internal processes. *Eurostat* : website. URL: https://ec.europa.eu/eurostat/databrowser/view/isoc_eb_iip/default/table?lang=en.

127. ISO/IEC 20000 IT Service Management – A Practical Guide. *ISO* : website. URL: https://www.iso.org/publication/PUB100441.html.

128. ISO/IEC 27000:2009(en) Information technology – Security techniques – Information security management systems – Overview and vocabulary. *ISO* : website. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-1:v1:en.

129. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. *ISO* : website. URL: https://www.iso.org/standard/54534.html.

130. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls. *ISO* : website. URL: https://www.iso.org/standard/54533.html.

131. ISO/IEC Standard 15443 - Information technology - Security techniques - A framework for IT security assurance. *The European Union Agency for Cybersecurity* : website. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-15443.

132. Jackson L.A., Al-Hamdani W. Economic acceptable risk assessment model. *5th Annual Conference on Information Security Curriculum Development, InfoSecCD '08*, Kennesaw, GA, United States, 26 September 2008 through 27 September 2008. Proceedings of the 5th Annual Conference on Information Security Curriculum Development, 2008. P. 36-39. DOI: https://doi.org/10.1145/1456625.1456636.

133. Jacobs P., Von Solms B., Grobler M. Towards a national cybersecurity capability development model. *16th European Conference on Cyber Warfare and Security, ECCWS 2017*, Dublin, Ireland, 2017. P. 582-592.

134. Jazri H., Zakaria O., Chikohora E. Measuring cybersecurity wellness index of critical organisations. *2018 IST-Africa Week Conference, IST-Africa 2018 (Botswana, Gaborone, May 2018).* Institute of Electrical and Electronics Engineers Inc., 2018. P. 1-8.

135. Jin H.-W. Analysis of factors affecting the benefits of demand information sharing. *E&M Economics and Management*. 2019. Vol. 22(3). P. 204-219. DOI: https://doi.org/10.15240/tul/001/2019-3-013.

136. Kadhim L.J., Al-sahrawardee H.M.S.M., Karoom C.B.M. The role of stress testing scenarios in reducing the banks- risks: an applied study. *Polish Journal of Management Studies*. 2019. Vol. 20(2). P. 279-289. DOI: https://doi.org/10.17512/pjms.2019.20.2.23.

137. Kalinowski S. Operating Risk of Polish Public Companies – Sectoral Differences. *Economics&Sociology*. 2017. Vol. 10(1). P. 22-34. DOI: https://doi.org/10.14254/2071- 789X.2017/10-1/2.

138. Kamaliah K., Marjuni N.-S., Mohamed N., Mohd-Sanusi Z., Anugerah R. Effectiveness of monitoring mechanisms and mitigation of fraud incidents in the public sector. *Administratie si Management Public*. 2018. Vol. 30. P. 82-95. DOI: https://doi.org/10.24818/amp/2018.30-06.

139. Karaoulanis A. Big Data, What Is It, Its Limits and Implications in Contemporary Life. *Business Ethics and Leadership*. 2018. Vol. 2(4). P. 108-114. DOI: https://doi.org/10.21272/bel.2(4).108-114.2018.

140. Kenney M. Cyber-Terrorism in a Post-Stuxnet World. *Orbis.* 2015. Vol. 59(1). P. 111-128. DOI: https://doi.org/10.1016/j.orbis.2014.11.009.

141. Kirilenko V.P., Alexeyev G.V. Political technologies and international conflicts in the information space of the Baltic Sea region. *Baltic Region.* 2018. Vol. 10(4). P. 20-38. DOI: https://doi.org/10.5922/2079-8555-2018-4-2.

142. Ključnikov A., Mura L., Sklenár D. Information security management in smes: Factors of success. *Entrepreneurship and Sustainability Issues.* 2019. Vol. 6(4). P. 2081-2094. DOI: https://doi.org/10.9770/jesi.2019.6.4(37).

143. Knapp K.J, Boulton W.R. Cyber-warfare threatens corporations: Expansion into commercial environments. *Information Systems Management.* 2006. Vol. 23(2). P. 76-87. DOI: https://doi.org/10.1201/1078.10580530/ 45925.23.2.20060301/92675.8.

144. Kohonen T. Self-Organized Formation of Topologically Correct Feature Maps. *Biological Cybernetics*. 1982. Vol. 43(1). P. 59-69. DOI: https://doi.org/10.1007/BF00337288.

145. Kokles M., Filanová J., Korček F. Application of fuzzy logic in the process of information security risk assessment. *27th International Business Information Management Association Conference - Innovation Management and Education Excellence Vision 2020: From Regional Development Sustainability to Global Economic Growth, IBIMA 2016*, Milan, Italy, 4-5 May 2016. International Business Information Management Association, IBIMA, 2016. P. 1078-1088.

146. 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.

147. Kolini F., Janczewski L. Clustering and topic modelling: A new approach for analysis of national cybersecurity strategies. *In Pacific Asia Conference on Information Systems (PACIS).* Association For Information Systems. 2017.

148. Kollár C., Zsuzsanna Bellász Z. V. Terrorism and the information security of media content with special regard to ISIS, the Balkans and Russia. *SocioEconomic Challenges.* 2017. Vol. 1(1). P. 13-19. DOI: https://doi.org/10.21272/sec.2017.1-02.

149. Kolupaieva I., Pustovhar S., Suprun O., Shevchenko O. Diagnostics of systemic risk impact on the enterprise capacity for financial risk neutralization: the case of Ukrainian metallurgical enterprises. *Oeconomia Copernicana*. 2019. Vol. 10(3). P. 471-491. DOI: https://doi.org/10.24136/oc.2019.023.

150. Kosevich E. Cyber security strategies of Latin America countries | [Estrategias de seguridad cibernética en los países de América Latina]. *Iberoamerica (Russian Federation).* 2020. Vol. 1. P. 137-159. DOI: https://doi.org/10.37656/S20768400-2020-1-07.

151. Kostyuchenko N., Starinskyi M., Tiutiunyk I., Kobushko I. Methodical approach to the assessment of risks connected with the legalization of the proceeds of crime. *Montenegrin Journal of Economics*. 2018. Vol. 14(4). P. 023-043. DOI: https://doi.org/10.14254/1800-5845/2018.14-4.2.

152. Kostyuk N. International and domestic challenges to comprehensive national cybersecurity: A case study of the Czech Republic. *Journal of Strategic Security*. 2014. Vol. 7(1). P. 68-82. DOI: https://doi.org/10.5038/1944-0472.7.1.6.

153. Kozmenko O.V., Pakhnenko O.M. Financial methods of catastrophe risks management. *Actual Problems of Economics*. 2011. Vol. 118(4). P. 217-223. URL: https://www.researchgate.net/publication/289809836_Financial_methods_of_catastrophe_risks_management.

154. Kshetri N. An opinion on the 'Report on Securing and Growing the Digital Economy. *IEEE Security and Privacy*. 2017. № 15(1). P. 80-85. DOI: https://doi.org/10.1109/MSP.2017.10.

155. Kshetri N., Murugesan S. EU and US cybersecurity strategies and their impact on businesses and consumers. *Computer*. 2013. Vol. 46(10). P. 84-88. DOI: https://doi.org/10.1109/MC.2013.350.

156. Kuzmenko O., Bozhenko A. Optimization of the risk level of net retention in the insurance market. *Economic Annals-XXI.* 2014. Vol. 11-12. P. 76-79. URL: http://soskin.info/userfiles/file/2014/11-12_2014/Kuzmenko_Bozhenko.pdf.

157. Launching the Contract for the Web. *World Wide Web Foundation* : website. URL: https://webfoundation.org/2019/11/launching-the-contract-for-the-web/.

158. Lazaroiu G., KovachovaM., Kliesticova J., Kubla P., Valaskova K., Dengov V. Data governance and automated individual decision-making in the digital privacy General Data Protection Regulation. *Administratie si Management Public.* 2018. Vol. 31. P. 132-141. DOI: https://doi.org/10.24818/amp/2018.31-09.

159. Lee D. 2020. Cathay Pacific fined £500,000 by British privacy watchdog for 2018 data breach but avoids potentially heftier penalty under European regulation. *SCMP* : website. URL: https://www.scmp.com/news/hong-kong/transport/article/3065071/cathay-pacific-fined-ps500000-british-privacy-watchdog.

160. Leonov S., Yarovenko H., Boiko A., Dotsenko T. Information system for monitoring banking transactions related to money laundering. *CEUR Workshop*

Proceedings. 2019. Vol. 2422. P. 297-307. URL: http://ceur-ws.org/Vol-2422/paper24.pdf.

161. Leonov S.V., Vasilyeva T.A., Shvindina H. O. Methodological approach to design the organizational development evaluation system. *Scientific Bulletin of Polissia*. 2017. Vol. 3(11)(2). P. 51-56. DOI: 10.25140/2410-9576-2017-2-3(11)-51-56.

162. Levchenko V., Boyko A., BozhenkoV., Mynenko S. Money laundering risk in developing and transitive economies: Analysis of cyclic component of time series. *Business: Theory and Practice*. 2019. Vol. 20. P. 492-508. DOI: https://doi.org/10.3846/btp.2019.46.

163. Li J. Network information security challenges and relevant strategic thinking as highlighted by "PRISM". *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2015. № 9483. P. 147-156. DOI: https://doi.org/10.1007/978-3-319-27051-7_13.

164. Limba T., Stankevičius A., Andrulevičius A. Towards sustainable cryptocurrency: risk mitigations from a perspective of national security. *Journal of Security and Sustainability*. 2019. Vol. 9(2). P. 375-389. DOI: https://doi.org/10.9770/jssi.2019.9.2(2).

165. List of Least Developed Countries (as of December 2020). *The United Nations* : website. URL: https://www.un.org/development/desa/dpad/least-developed-country-category/ldcs-at-a-glance.html.

166. Liu C., Shi H., Wu L., Guo M. The short-term and long-term trade-off between risk and return: chaos vs rationality. *Journal of Business Economics & Management*. 2020. Vol. 21(1). P. 23-43. DOI: https://doi.org/10.3846/jbem.2019.11349.

167. Loshytskyi M., Kostenko O., Koropatnik I., Tereshchuk G., Karelin V. Organizational competence of NATO information security policy. *Journal of Security and Sustainability Issues*. 2020. Vol. 9(3). P. 735-746. DOI: https://doi.org/10.9770/JSSI.2020.9.3(1).

168. Lyeonov S., Liuta O. Actual problems of finance teaching in Ukraine in the post-crisis period. In *The Financial Crisis: Implications for Research and Teaching*. s.l.:Springer, Cham. 2016. P. 145-152. DOI: https://doi.org/10.1007/978-3-319-20588-5_8.

169. Lyeonov S., Kuzmenko O., Yarovenko H., Dotsenko T. The Innovative Approach to Increasing Cybersecurity of Transactions Through Counteraction to Money Laundering. *Marketing and Management of Innovations*. 2019. № 3. P. 308-326.

170. Lynett M. A History of Information Security From Past to Present. *Hybrid Document Systems* : website. URL: https://blog.mesltd.ca/a-history-of-information-security-from-past-to-present.

171. MacKay B., Munro I. Information Warfare and New Organizational Landscapes: An Inquiry into the ExxonMobil-Greenpeace Dispute over Climate Change. *Organization Studies.* 2012. Vol. 33(11). P. 1507-1536. DOI: https://doi.org/10.1177/0170840612463318.

172. MacQueen J.B. Some methods for classification and analysis of multivariate observations. In *5-th Berkeley Symposium on Mathematical Statistics and Probability*. USA, Berkeley, The University of California. 1967. P. 281-297. URL: http://www.cs.cmu.edu/~bhiksha/courses/mlsp.fall2010/class14/macqueen.pdf.

173. Mardani A., Zavadskas E.K., Govindan K., Amat Senin A., Jusoh, A. VIKOR technique: A systematic review of the state of the art literature on methodologies and applications. *Sustainability.* 2016. Vol. 8(1). P. 37. DOI: https://doi.org/10.3390/su8010037.

174. Martins N., Da Veiga A. An Information security culture model validated with structural equation modelling. In *9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015,* Lesvos, Greece, 1-3 July 2015. University of Plymouth, 2015. P. 11-21.

175. Mencher Eh. M., Zemshman A. Ja. Osnovy planirovaniya eksperimenta s elementami matematicheskoy statistiki v issledovanii po vinogradstvu [Basics of

planning an experiment with elements of mathematical statistics in a study on viticulture]. Kishinev: Shtiintsa, 1986.

176. Miller K.E. A Situational Multi-Attribute Attitude Model. *Advances in Consumer Research*. 1975. Vol. 2. P. 455-464.

177. Misra S., Singh R., Rohith Mohan S.V. Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. *Sensors*. 2010. Vol. 10(4). P. 3444-3479. DOI: https://doi.org/10.3390/s100403444.

178. Morgan S. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. Cybercrime Magazine : website. URL: https://cybersecurityventures.com/cybersecurity-almanac-2019/.

179. Morrow S., Crabtree T. The future of cybercrime & security. Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024. *Juniper Research :* website. URL: https://www.juniperresearch.com/researchstore/key-vertical-markets/cybercrime-cybersecurity-research-report?utm_campaign=pr1_thefutureof cybercrime_technology_aug19&utm_source=businesswire&utm_medium=pr.

180. Munteanu A. Information security risk assessment: The qualitative versus quantitative dilemma. In *6th International Business Information Management Association Conference, IBIMA 2006*, Bonn, Germany, 19-21 June 2006. International Business Information Management Association, IBIMA, 2006. P. 227-232.

181. Murphey D. A history of information security. *IFSEC GLOBAL* : website. URL: https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/#:~:text=It%20was%20during%20the%201960s,how%20to%20work%20a%20computer.

182. Nakashima E. Russian government hackers penetrated DNC, stole opposition research on Trump. *The Washington Post*. 14 June 2016. URL: https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html.

183. Nardelli A. The EU's Embassy In Russia Was Hacked But The EU Kept It A Secret. *BuzzFeedNews* : website. URL: https://www.buzzfeednewscom/ article/albertonardelli/eu-embassy-moscow-hack-russia.

184. Nasr A. K., Alaei S., Bakhshi F., Rasoulyan F., Tayaran H., Farahi M. How enterprise risk management (ERM) can affect on short-term and long-term firm performance: evidence from the Iranian banking system. *Entrepreneurship and Sustainability Issues*. 2019. Vol. 7(2). P. 1387-1403. DOI: https://doi.org/10.9770/jesi.2019.7.2(41).

185. National Cyber Security Index. *e-Governance Academy* : website. URL: https://ncsi.ega.ee/ncsi-index/.

186. 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/#:~:text=However%2C%20experts%20deem% 20the%20following,%2C%20India%2C%20and%20Hong%20Kong.

187. Nitsenko V., Mardani A., Streimikis J., Ishchenko M., Chaikovsky M., Stoyanova-Koval S., Arutiunian R. Automatic Information System of Risk Assessment for Agricultural Enterprises of Ukraine. *Montenegrin Journal of Economics.* 2019. Vol. 15(2). P. 139-152. DOI: https://doi.org/10.14254/1800-5845/2019.15-2.11.

188. Nocoń A., Pyka I. Sectoral analysis of the effectiveness of bank risk capital in the Visegrad Group countries. *Journal of Business Economics & Management.* 2019. Vol. 20(3). P. 424-445. DOI: https://doi.org/10.3846/jbem.2019.9606.

189. Noel S., Harley E., Tam K.H., Limiero M., Share M. CyGraph: Graph-Based Analytics and Visualization for Cybersecurity. *Handbook of Statistics*. 2016. Vol. 35. P. 117-167. DOI: https://doi.org/10.1016/bs.host.2016.07.001.

190. O'Neill J., Wilson D., Purushothaman R., Stupnytska A. How Solid are the BRICs? Global Economics Paper No: 134. *GS Global Economic Website. Economic Research from the GS Institutional Portal* : website. URL: https://www.goldmansachs.com/insights/archive/archive-pdfs/how-solid.pdf.

191. Omirzhanov Y., Baimagambetova Z., Tusupova A., Omirtay R., Uteuliev S. On the national security correlation with freedom of speech in Kazakhstan. *Journal of Advanced Research in Law and Economic.* 2017. Vol. 8(3). P. 980-986. DOI: https://doi.org/10.14505/jarle.v8.3(25).35.

192. Opricovic S. T. G.-H. The Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS. *European Journal of Operational Research*. 2004. Vol. 156(2). P. 445–455.

193. Percentage of the ICT sector in GDP. *Eurostat* : website. URL: https://ec.europa.eu/eurostat/databrowser/view/isoc_bde15ag/default/table?lang=en.

194. Podaras A. Risk-based control of the negative effect of discontinued automated processes – a case from the agricultural domain. *E&M Economics and Management.* 2017. Vol. 20(4). P. 251-261. DOI: https://doi.org/10.15240/tul/001/2017-4-017.

195. Pokrovskaia N.N. Tax, financial and social regulatory mechanisms within the knowledge-driven economy. Blockchain algorithms and fog computing for the efficient regulation. In *20th IEEE International Conference on Soft Computing and Measurements, SCM 2017,* St. Petersburg, Russian Federation, 24-26 May 2017. Institute of Electrical and Electronics Engineers Inc., 2017. P. 709-712. DOI: https://doi.org/10.1109/SCM.2017.7970698.

196. Polak J. Determining Probabilities for a Commercial Risk Model of Czech Exports to China with Respect to Cultural Differences and in Financial Management. *Journal of Competitiveness*. 2019. Vol. 11(3). P. 109-127. DOI: https://doi.org/10.7441/joc.2019.03.07.

197. Political stability - Country rankings. *The GlobalEconomy.com* : website. URL: https://www.theglobaleconomy.com/rankings/wb_political_stability/.

198. Popova L., Korostelkina I., Dedkova E., Korostelkin M. Information Risks and Threats of the Digital Economy of the XXI Century: Objective Prerequisites and Management Mechanisms. In Antipova T., Rocha Á. (Eds) *Digital Science 2019. DSIC 2019.* Advances in Intelligent Systems and Computing, 2019. Vol. 1114. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-37737-3_17.

199. Pryima S., Dayong Y., Anishenko O., Petrushenko Y., Vorontsova A. Lifelong learning progress monitoring as a tool for local development management. *Problems and Perspectives in Management*. 2018. Vol. 16(3). P. 1-13. DOI: https://doi.org/10.21511/ppm.16(3).2018.01.

200. #FraudStats. *Experian* : website. URL: https://www.experian.co.uk/identity-and-fraud/fraud-statistics/.

201. Riley D. Microsoft exposes 250M customer service records via misconfigured Elasticsearch database. *SiliconANGLE :* website. URL: https://siliconangle.com/2020/01/22/microsoft-exposes-250m-customer-service-records-via-misconfigured-elasticsearch-database/.

202. Riley D. Payment card records stolen in latest attack targeting municipal payments system. *SiliconANGLE :* website. URL: https://siliconangle.com/2019/09/22/payment-card-records-stolen-latest-attack-targeting-municipal-payments-system/.

203. Robinson M., Jones K., Janicke H. Cyber warfare: Issues and challenges. *Computers and Security.* 2015. Vol. 49. P. 70-94. DOI: https://doi.org/10.1016/j.cose.2014.11.007.

204. Ryu Y.U., Rhee H.-S. Evaluation of intrusion detection systems under a resource constraint. *ACM Transactions on Information and System Security*. 2008. Vol. 11(4). Article number 20. DOI: https://doi.org/10.1145/1380564.1380566.

205. Sadigov M., Kuzmenko O., Yarovenko H. Blockchain technology based system-dynamic simulation modeling of enterprise's cyber security system. *Economic and Social Development :* Book of Proceedings Vol. 1/4, 55th International Scientific Conference on Economic and Social Development Development, 2020. P. 399-408. URL: https://www.esd-conference.com/upload/book_of_proceedings/Book_of_Proceedings_esdBaku2020_Vol1_Online.pdf.

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

207. Sayed Hussin S.A.H., Iskandar T.M., Saleh N.M., Jaffar R. Professional Skepticism and Auditors' Assessment of Misstatement Risks: The Moderating Effect

of Experience and Time Budget Pressure. *Economics & Sociology*. 2017. Vol. 10(4). P. 225-250. DOI: https://doi.org/10.14254/2071-789X.2017/10-4/17.

208. Schreier F. On Cyberwarfare. *The Geneva Centre for the Democratic Control of Armed Forces* : website. URL: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf. ‘

209. Schwab K. The Global Competitiveness Report 2018. *World Economic Forum* : website. URL: http://www3.weforum.org/docs/GCR2018/05FullReport/ TheGlobalCompetitivenessReport2018.pdf.

210. Sedov L.I. Similarity and Dimensional Methods in Mechanics. 4th ed. M. Holt (Ed.). New York: Academic Press, 1959.

211. Sheen J.N. Fuzzy economic decision-models for information security investment. In *9th WSEAS International Conference on Instrumentation, Measurement, Circuits and Systems, IMCAS '10*, Hangzhou, China, 11-13 April 2010. China Jiliang University, 2010. P. 141-147.

212. Shi Y., Wen Q. A value based security risk assessment method. In *4th International Conference on Multimedia and Security, MINES 2012*, Nanjing, Jiangsu, China, 2-4 November 2012. Nanjing University of Science and Technology, NSFC, 2012. P. 49-51. DOI: https://doi.org/ 10.1109/MINES.2012.72.

213. Shkarlet S., Lytvynov V., Dorosh M., Trunova E., Voitsekhovska M. The model of information security culture level estimation of organization. In *14th International Scientific-Practical Conference, MODS 2019,* Chernihiv, Ukraine; 24-26 June 2019. Advances in Intelligent Systems and Computing, 2019. Vol. 1019. P. 249-258. DOI: https://doi.org/10.1007/978-3-030-25741-5_25.

214. Short Circuit: How a Robotics Vendor Exposed Confidential Data for Major Manufacturing Companies. *UpGuard* : website. URL: https://www.upguard.com/breaches/short-circuit-how-a-robotics-vendor-exposed-confidential-data-for-major-manufacturing-companies.

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

216. Śliwiński P., Łobza M. The impact of global risk on the performance of socially responsible and conventional stock indices. *Equilibrium. Quarterly Journal of Economics and Economic Policy*. 2017. Vol. 12(4). P. 657–674. DOI: https://doi.org/10.24136/eq.v12i4.34.

217. Smith T. Hacker jailed for revenge sewage attacks. *The Register* : website. URL: https://www.theregister.com/2001/10/31/hacker_jailed_for_revenge_sewage/.

218. Sonny Z. National security in Malaysia's digital economy: Redefinition, reaction and legal reform. *Journal of Applied Sciences Research.* 2011. № 7 (special issue). P. 2316-2325.

219. Sorokivska O.A. Economic security of ukrainian enterprises under information war. *Actual Problems of Economics*. 2015. Vol. 174(12). P. 198-202.

220. Special Eurobarometer 404: Cyber security. *EU Open Data Portal* : website. URL: https://data.europa.eu/euodp/en/data/dataset/S1073_79_4_404.

221. Special Eurobarometer 499: Europeans’ attitudes towards cyber security. *EU Open Data Portal* : website. URL: https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.

222. Special Eurobarometer 499: Report. Europeans’ attitudes towards cyber security. URL: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/89100.

223. STATISTICA products. *StatSoft* : website. URL: http://statsoft.ru/products/.

224. Stewart P., Wolf J. Old worm won't die after 2008 attack on military. *The Thomson Reuters*. 2011. URL: https://www.reuters.com/article/us-usa-cybersecurity-worm-idUSTRE75F5TB20110617.

225. Štitilis D., Pakutinskas P., Malinauskaite I. EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. *Security*

Journal. 2017. Vol. 30(4). P. 1151-1168. DOI: https://doi.org/10.1057/s41284-016-0083-9.

226. Stoll M. An information security model for implementing the new ISO 27001. *Handbook of Research on Emerging Developments in Data Privacy*. *IGI Global.* 2014. P. 2016-238. DOI: https://doi.org/10.4018/978-1-4666-7381-6.ch011.

227. Subeh Musa A., Yarovenko H. Data Mining of Operations with Card Accounts of Bank Clients. *Financial Markets, Institutions and Risks*. 2017. № 1(4). P. 87-95.

228. Suniantara I. K. P., Putra I. G. E. W. Comparison of VIKOR and TOPSIS Methods in Multiresponse Taguchi Optimization. *Journal of Education Research and Evaluation.* 2019. Vol. 2(3). P. 106-113. URL: https://ejournal.undiksha.ac.id/index.php/JERE.

229. Tallau L.J., Gupta M., Sharman R. Information security investment decisions: Evaluating the Balanced Scorecard method. *International Journal of Business Information Systems.* 2010. № 5(1). P. 34-57. DOI: https://doi.org/10.1504/IJBIS.2010.029479.

230. Targett E. 2020. Decathlon Leaks 123 Million Records via Insecure Elasticsearch Server. *TECHMONITOR* : website. URL: https://www.cbronline.com/news/decathlon-leaks.

231. Taylor G.I. The formation of a blast wave by a very intense explosion. *Proceedings of the Royal Society A*. 1950. Vol. 201. P. 159-174. DOI: https://doi.org/10.1098/rspa.1950.0049.

232. Teoh C.S., Mahmood A.K. National cyber security strategies for digital economy. *Journal of Theoretical and Applied Information Technology*. 2017. Vol. 9(13). P. 6510-6522.

233. Tewari M. Event risk covenants, design parameters and agency issues: a comparative study of high yield versus investment grade bonds. *Business: Theory and Practice*. 2018. Vol. 19. P. 331-341. DOI: https://doi.org/10.3846/btp.2018.33.

234. The ICT Development Index (IDI): conceptual framework and methodology. *International Telecommunication Union* : website. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis/methodology.aspx.

235. The Legatum Prosperity Index. *The Legatum Institute* : website. URL: https://www.prosperity.com/about/resources.

236. Topa I., Karyda M. From theory to practice: guidelines for enhancing information security management. *Information and Computer Security.* 2019. №27(3). P. 326-342. DOI: https://doi.org/10.1108/ICS-09-2018-0108.

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

238. Tsiakis T., Stephanides G. The economic approach of information security. *Computers and Security*. 2005. № 24(2). P. 105-108. DOI: https://doi.org/10.1016/j.cose.2005.02.001.

239. Umadevi P., Divya, E. Money laundering detection using TFA system. *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.

240. 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.

241. Uneven economic development - Country rankings. *The GlobalEconomy.com* : website. URL: https://www.theglobaleconomy.com/rankings/ uneven_economic_development_index/#:~:text=Definition%3A%20The%20Uneven %20economic%20development,inequality%20in%20the%20country's%20economy.

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

243. Valaskova K., Kliestik T., Kovacova M. Management of financial risks in Slovak enterprises using regression analysis. *Oeconomia Copernicana*. 2018. Vol. 9(1). P. 105-121. DOI: https://doi.org/10.24136/oc.2018.006.

244. Vasilieva T., Lieonov S., Makarenko I., Sirkovska N. Sustainability information disclosure as an instrument of marketing communication with stakeholders: markets, social and economic aspects. *Marketing and Management of Innovations*. 2017. Vol. 4. P. 350 - 357. DOI: https://doi.org/10.21272/mmi.2017.4-31.

245. Vasilyeva T., Kozyriev V. Scientific and methodical approaches to determining the center-orientation of financial conglomerates with the factor and cluster analysis. *Business Ethics and Leadership*. 2017. Vol. 1(1). P. 5-15. DOI: https://doi.org/10.21272/bel.2017.1-01.

246. Vasilyeva T., Kuzmenko O., Bozhenko V., Kolotilina O. Assessment of the dynamics of bifurcation transformations in the economy. *CEUR Workshop Proceedings*. 2019. Vol. 2422. P. 134-146. URL: http://ceur-ws.org/Vol-2422/paper11.pdf.

247. Vasilyeva T.A., Makarenko I.A. Modern innovations in corporate reporting. *Marketing and Management of Innovations*. 2017. Vol. 1. P. 115 - 125. DOI: https://doi.org/10.21272/mmi.2017.1-10.

248. Vasyl'eva T. A., Leonov S. V., Makarenko I. O. Modern methodical approaches to the evaluation of corporate reporting transparency. *Scientific Bulletin of Polissia*. 2017. Vol. 1(9)(2). P. 185-190. URL: http://nvp.stu.cn.ua/uk/component/k2/item/681-vasyl%E2%80%99eva-t-a-leonov-s-v-makarenko-i-o-modern-methodical-approaches-to-the-evaluation-of-corporate-reporting-transparency.html.

249. Vasylieva T. A., Lieonov S. V., Petrushenko Yu. M., Vorontsova A. S. Investments in the system of lifelong education as an effective factor of socio-economic development. *Financial and Credit Activity-Problems of Theory and Practice*. 2017. Vol. 2(23). P. 426-436. DOI: https://doi.org/10.18371/fcaptp.v2i23.121202.

250. Vasylyeva T.A., Leonov S.V., Bohma S.D. The impact of implicit bank consolidation on systemic risk in the banking system of Ukraine. *Actual Problems of Economics*. 2014. Vol. 159(9). P. 384-389. DOI: https://doi.org/10.2139/ssrn.2538382.

251. Ventana Systems. *Vensim* : website. URL: http://vensim.com.

252. Vosstanovlenie informacii. Prichiny poteri informacii. *hdd.lviv.ua* : website. URL: https://hdd.lviv.ua/publikatsii/prichiny-poteri-informatsii.

253. Vorontsova A., Lyeonov S., Vasylieva T., Artyukhov A. Innovations in the financing of lifelong learning system: expenditure optimization model. *Marketing and Management of Innovations*. 2018. Vol. 2. P. 218-231. DOI: https://doi.org/10.21272/mmi.2018.2-18.

254. Wang B., Li Y., Zhao S., Chen H., Jin Y., Ding Y. Key Technologies on Blockchain Based Distributed Energy Transaction. *Dianli Xitong Zidonghua/Automation of Electric Power Systems*. 2019. № 43(14). P. 53-64. DOI: https://doi.org/10.7500/AEPS20181203010.

255. War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?". *The Economist* : website. URL: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.

256. Weiner R. Hacker who sent ‘kill list’ of U.S. military personnel to ISIS: ‘I feel so bad’. *The Washington Post* : website. URL: https://www.washingtonpost.com/local/public-safety/hacker-who-sent-kill-list-of-us-military-personnel-to-islamic-state-i-feel-so-bad/2016/09/23/dc0ba0ea-8196-11e6-b002-307601806392_story.html.

257. World Development Indicators. *The world Bank* : website. URL: https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on.

258. World Economic Outlook. October 2018. Challenges to Steady Growth. *International Monetary Fund* : website. URL: https://www.imf.org/~/media/Files/Publications/WEO/2018/October/English/main-report/Text.ashx.

259. Wu Y., Feng G., Fung R.Y.K. Comparison of information security decisions under different security and business environments. *Journal of the Operational Research Society.* 2018. № 69(5). P. 747-761. DOI: https://doi.org/10.1057/s41274-017-0263-y.

260. X-Force Threat Intelligence Index 2020. *Kommersant* : website. URL: https://www.kommersant.ru/docs/2018/IBMXForceThreatIntelIndex2020.pdf.

261. Yarovenko H. Evaluating the threat to national information security. *Problems and Perspectives in Management.* 2020. Vol. 18(3). P. 195-210.

262. Yarovenko H. Research of relationship between information security and country development factors. *Theoretical and empirical scientific research: concept and trends :* Collection of scientific papers «ΛΌГОΣ» with Proceedings of the International Scientific and Practical Conference, July 24, 2020. Oxford, UK : Oxford Sciences Ltd. & European Scientific Platform, 2020. Vol. 1. P. 37-38.

263. Yarovenko H., Kuzmenko O., Stumpo M. DEA-Analysis Of The Effectiveness Of The Country's Information Security System. *SocioEconomic Challenges.* 2020. 4(3). P. 142-153.

264. Yarovenko H., Kuzmenko O., Stumpo M. Strategy for Determining Country Ranking by Level of Cybersecurity. *Financial Markets, Institutions and Risks*. 2020. 4(3). P. 124-137.

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

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

267. Yunis M.M., Koong K.S. A conceptual model for the development of a national cybersecurity index: An integrated framework. *21st Americas Conference on Information Systems, AMCIS 2015 (Puerto Rico, El Conquistador Resort and*

Convention CenterFajardo). AMCIS 2015. URL: https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/44/.

268. Zhang R., Xue R., Liu L. Security and privacy on blockchain. *ACM Computing Surveys*. 2019. Vol. 52(3). P. 1-34.

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

270. Аналітична економія: макроекономіка і мікроекономіка : навч. посіб. : у 2 кн. Кн. 1 : Вступ до аналітичної економії / за ред. С. Панчишина, П. Остоверха. Київ : Знання, 2006. 723 с.

271. Артамонова Я.С. Информационная безопасность российского общества: теоретические основания и практика политического обеспечения: дис. … доктора политических наук / Московский государственный областной университет. М., 2014. 359 с.

272. Бараненко Р.В., Задорожна А.Ю. Кібервійна як новий вид протистояння держав. *Південноукраїнський правничий часопис*. 2017. №1. С. 53-56. URL: http://www.sulj.oduvs.od.ua/archive/2017/1/18.pdf.

273. Барр Р. Политическая экономия : в 2-х т. Т. 1; пер. с фр. М. : Междунар. отношения, 1995. 608 с.

274. Білоцерковець В.В., Завгородня О.О., Лебедєва В.К. та ін. Національна економіка: навч. посіб. для студ. вищ. навч. закл. / за ред. В.М. Тарасевича. К. : Центр учбової літератури, 2009. 280 с.

275. Бланк И.А. Инвестиционный менеджмент. К. : Эльга-Н, Ника – Центр, 2001. 448 с.

276. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник. Київ : ООО «Д.В.К.», 2004. 508 с.

277. Боднар І.Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки*. 2014. №1. С. 68-75. URL: https://core.ac.uk/download/pdf/141443493.pdf.

278. Бойко А. Забезпечення стійкості національної економіки. *Зовнішня торгівля: економіка, фінанси, право.* 2017. №4. С. 16-27.

279. Бронникова Т. Оценка эффективности внедрения информационной системы управления предприятием. Измеримые цели и контроль их достижения. *Экономика и жизнь.* 2008. № 47. URL: http://www.topsbi.ru/about-the-company/press-centr/publikacii/ocenka_effektivnosti_vnedreniya_informacionnoy_sistemy_upravleniya_predpriyatiem/.

280. Булкін С.М. Ударно-хвильова модель поширення фінансової кризи. *Прометей: регіональний збірник наукових праць з економіки*. 2016. № 1 (46). С. 132–140.

281. Бункина М.К. Национальная экономика : учебник для вузов. М. : Издательство «Палеотип» : Издательский Дом «Деловая литература» : Издательство «Логос», 2002. 488 с.

282. Валовий внутрішній продукт (у фактичних цінах). *Держстат України* : вебсайт. URL: http://ukrstat.gov.ua/operativ/operativ2003/vvp/vvp_kv/vvp_kv_u/ arh_vvp_kv.html.

283. Вашай Ю.В., Самедова Л.Р. Інформаційна безпека та її вплив на стан економічної безпеки держави. *Глобальні та національні проблеми економіки.* 2018. № 22. С. 3-6. URL: http://global-national.in.ua/archive/22-2018/3.pdf.

284. 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.

285. Голубев В. Кибертерроризм как новая форма терроризма. *Центр исследования проблем компьютерной преступност*и : вебсайт. URL: http://www.crime-research.ru/library/Gol_tem3.htm.

286. Градов А.П. Национальная экономика. СПб. : Питер, 2005. 240 с.

287. Гринів Л. С., Кічурчак М. В. Національна економіка. Львів : Магнолія-2006, 2009. 464 с.

288. Гринчуцька С.В. Конспект лекцій з курсу «Національна економіка» для студентів за спеціальностями напряму підготовки 0501 «Економіка і підприємництво» всіх форм навчання. Тернопіль : ПМП “Тайп”, 2010. 132 с. URL: http://elartu.tntu.edu.ua/bitstream/lib/22558/5/NacEkon-Konspekt_lekcij-2010.pdf.

289. Дергалюк Б.В. Структурні елементи економіки та їх пропорції. *Підприємництво та інновації*. 2019. № 7. С. 52-55. DOI: https://doi.org/10.37320/2415-3583/7.8.

290. Діордіца І.В. Поняття та зміст кібершпигунства. *Наукові праці Національного університету “Одеська юридична академія”*. 2020. № 26. С. 49-55. DOI: https://doi.org/10.32837/npnuola.v26i0.660.

291. Загорський В., Борощук Є., Жолобчук І. Забезпечення сталого розвитку національної економіки: соціальні та екологічні аспекти. *Збірник наукових праць «Ефективність державного управління».* 2015. № 44. С. 9-17.

292. Загроза. Великий тлумачний словник сучасної мови. *Slovnyk.me* : вебсайт. URL: https://slovnyk.me/dict/vts/%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B0.

293. Загроза. Фізико-технічний словник-мінімум. *Slovnyk.me* : вебсайт. URL: https://slovnyk.me/dict/phystech_terms/%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B0.

294. Задоя А.А., Петруня Ю.Е. Основы экономики. Київ : Вища шк. : Знання, 1998. 478 с.

295. Закон України № 2163-VIII від 05.10.2017 (редакція станом на 24.10.2020) «Про основні засади забезпечення кібербезпеки України». *Верховна Рада України* : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

296. Закон України № 2297-VI від 01.06.2010 (редакція станом на 20.03.2020) «Про захист персональних даних». *Верховна Рада України* : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

297. Закон України № 2657-XII від 02.10.1992 (редакція станом на 16.07.2020) «Про інформацію». *Верховна Рада України* : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

298. 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.

299. Закон України № 3855-XII від 21.01.1994 (редакція станом на 24.10.2020) «Про державну таємницю». *Верховна Рада України* : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

300. Закон України № 537-V від 09.01.2007 «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». *Верховна Рада України* : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text.

301. Закон України № 74/98-ВР від 04.02.1998 (редакція станом на 16.10.2020) «Про Національну програму інформатизації». *Верховна Рада України* : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text.

302. Закон України № 80/94-ВР від 05.07.1994 (редакція станом на 04.07.2020) «Про захист інформації в інформаційно-телекомунікаційних системах». *Верховна Рада України* : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

303. Золотар О.О. Інформаційна безпека людини: теорія і практика. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

304. Золотогоров В.Г. Экономика. Мн. : Интерпрессерсис: Книжный дом, 2003. 720 с.

305. Зубок М.І. Інформаційна безпека в підприємницькій діяльності. К. : ГНОЗІС, 2015. 216 с.

306. Информационная безопасность в компании. *TADVISER* : вебсайт. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2_%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D0%B8#Dell_Technologies:_82.25_.D0.BA.D0.BE.D0.BC.D0.BF.D0.B0.D0.BD.D0.B8.D0.B9_.D0.BF.D0.BE.D1.81.D1.82.D1.80.D0.B0.D0.B4.D0.B0.D0.BB.D0.B8_.D0.BE.D1.82_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.B0.D1.82.D0.B0.D0.BA_.D0.B8_.D0.BF.D1.80.D0.BE.D0.B8.D1.81.D1.88.D0.B5.D1.81.D1.82.D0.B2.D0.B8.D0.B9.

307. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Гуманітарні візії*. 2016. № 2(1). С. 27-32.

308. Інструкція з проведення аналізу ризиків у Державній прикордонній службі України, затверджено Наказом Міністерства внутрішніх справ України № 1007 від 11.12.2017, зареєстровано в Міністерстві юстиції України № 91/31543 від 22.01.2018. *Верховна Рада України* : вебсайт. URL: https://zakon.rada.gov.ua/laws/show/z0091-18#Text.

309. Карінцева О.І. Оптимальна структура національної економіки як запорука сталого розвитку держави. *Проблеми економіки*. 2018. № 1(35). С. 62-68. URL: https://www.problecon.com/export_pdf/problems-of-economy-2018-1_0-pages-62_68.pdf.

310. Клімова О.І. Структурні зміни в економіці: основні поняття та види. *Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки*. 2009. № 24(1). С. 60–65.

311. Козьменко О., Кузьменко О. Моделювання рівноваги перестрахових ринків у Німеччині, Франції та Україні: порівняльні характеристики. *Інвестиційний менеджмент та фінансові інновації*. 2011. № 2. С. 8-16.

312. Козьменко О., Меренкова О., Бойко А. Аналіз структури та динаміки ринку в Україні, Росії та членах Європейської федерації страхування та перестрахування. *Проблеми та перспективи в управлінні міжнародними дослідженнями*. 2009. № 7(1). С. 29-39.

313. Концепція інформаційної безпеки України: проект. *OSCE* : вебсайт. URL: https://www.osce.org/files/f/documents/0/2/175056.pdf.

314. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: дис. доктора юрид. наук : 12.00.07. Одеса, 2004. 427 с.

315. Круша П. В. Національна економіка. К. : Каравела: Піча Ю. В., 2008. 416 с.

316. Кузьменко О. В., Бойко А. О., Яровенко Г. М., Доценко Т. В. Сценарії реформування національної системи фінансового моніторингу. *Економіка та держава.* 2020. № 1. С. 9-15.

317. Кузьменко О. В., Яровенко Г. М., Бойко А. О., Миненко С. В. Розробка інтерфейсів автоматизованого модулю фінансового моніторингу. *Інвестиції: практика та досвід.* 2020. № 1. С. 11-18.

318. Кузьменко О. В., Яровенко Г. М., Левченко В. П., Миненко С. В. Автоматизація процесу фінансового моніторингу легалізації коштів, отриманих незаконним шляхом. *Науковий журнал «Наукові записки Національного університету «Острозька академія» серія «Економіка»*. 2019. № 43. С. 162-171.

319. Кузьменко О.В., Яровенко Г.М., Бойко А.О., Миненко С.В. Інформаційна система фінансового моніторингу: особливості розробки та реалізації в сучасних умовах протидії легалізації кримінальних доходів. Суми : Видавництво «Ярославна», 2019. 145 с.

320. Кузьмін О. Є., Пирог О. В. Секторна модель розвитку національного господарства України в умовах постіндустріального суспільства. *Бізнесінформ.* 2013. №7. С. 8-13. URL: http://www.business-inform.net/export_pdf/business-inform-2013-7_0-pages-8_13.pdf.

321. Кузьмін О., Когут У., Процик І., Вербицька Г. Національна економіка. Львів : Львівська політехніка, 2011. 303 с.

322. Кулініч О.М. Сталий розвиток національної економіки як ознака цивілізаційних процесів XXI століття. *Актуальні проблеми економіки*. 2012. № 1(127). С. 25-31.

323. Курбан О.В. Сучасні інформаційні війни у мережевому он-лайнпросторі. Київ : ВІКНУ, 2016. 286 с.

324. Лопатинський Ю.М. Меглей В.І. Концепція сталого розвитку як фактор конкурентоспроможності національної економіки. *Науковий вісник Чернівецького університету*. 2016. № 777-778. С. 35-40.

325. Любохинець Л.С., Поплавська О.В. Світова практика забезпечення інформаційної безпеки в сучасному глобалізованому середовищі. *Науково-виробничий журнал «Бізнес-навігатор».* 2017. № 4-1 (43). С. 93-97.

326. Мейер М.В., Маршал В. Оценка эффективности бизнеса. М. : ООО «Вершина», 2004. 272 с.

327. Мельникова В., Мельникова О., Сідлярук Т., Тур І., Шведова Г. Національна економіка. Київ : Центр навчальної літератури, 2012. 248 с.

328. Микитенко Т.В., Петровська І.О., Рогов П.Д. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2014. №1. С. 24-31. URL: http://znp-cvsd.nuou.org.ua/article/view/126694/121598.

329. Микитенко Т.В., Петровська І.О., Рогов П.Д., Гаркуша А.О. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.* 2016. № 2. С. 24-31.

330. Міхальова К.В. Науково-методичні засади сталого соціально-економічного розвитку України. *Інноваційна економіка*. 2013. № 11. С. 40-46.

331. Мочерний С.В., Ларіна Я.С., Устенко О.А., Юрій С.І. Економічний енциклопедичний словник. Львів : Світ, 2005. 616 с.

332. Мудра І., Сінькова Є. Інструменти інформаційної війни проти України в Інтернет-ЗМІ. *Вісник Національного університету «Львівська політехніка». Серія: Журналістські науки*. 2017. № 883. С. 39–44. DOI: https://doi.org/10.23939/sjs2017.01.042.

333. Нашинець-Наумова А. Організація системи захисту інформації суб'єктів господарювання. *Підприємництво, господарство і право*. 2016. №2. С. 110-116. URL: http://www.pgp-journal.kiev.ua/archive/2016/02/23.pdf.

334. Некрасов В. Блекаут по-київськи: чим загрожує кібератака на енергомережу Києва і хто за нею стоїть. *Економічна правда*. 2017. URL: https://www.epravda.com.ua/publications/2017/06/15/626036/.

335. Некрасов В. Україна програє кібервійну. Хакери атакують державні фінанси. *Економічна правда*. 2016. URL: https://www.epravda.com.ua/publications/2016/12/9/613957/.

336. Нехай В.А., Нехай В.В. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету*. 2017. № 24-1. С. 137-140.

337. Нортон Д., Каплан Р. Сбалансированная система показателей. От стратегии к действию. М. : ОлимпБизнес, 2010. 320 с.

338. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент*. 2008. № 4. С. 135-141. URL: http://nbuv.gov.ua/UJRN/PoMe_2008_4_16.

339. Отчет о стоимости утечки данных 2020. *IBM Security* : офіційний вебсайт. URL: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ru/pdf.

340. Панарин И. Н. Информационная война и выборы. М. : ОАО «Издательский Дом «Городец»», 2003. 416 с.

341. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. № 5. С.122-134.

342. Петров В.П., Петров С.В. Информационная безопасность человека и общества. М. : ЭНАС, 2007. 334 с.

343. Пилипенко С.М. Теоретичні засади оцінки ефективності діяльності підприємства. *Глобальні та національні проблеми економіки*. 2016. № 10. С. 452-456. URL: http://global-national.in.ua/archive/10-2016/94.pdf.

344. Пирог О. В. Адаптація структури національної економіки України до вимог постіндустріального суспільства. *Вісник Національного університету «Львівська політехніка»* : *Проблеми економіки та управління*. 2011. № 698. С. 93–103.

345. Платформа Loginom. Скачать Deductor. *BaseGroup Labs* : вебсайт. URL: https://basegroup.ru/deductor/download.

346. Половцев О.В. Методологічні підходи моделювання динаміки соціальних систем. *Теорія та практика державного управління і місцевого самоврядування.* 2014. № 1. URL: http://el-zbirn-du.at.ua/2014_1/19.pdf.

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

348. 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.

349. Поченчук Г.М. Інституціональний вимір структурних характеристик економічної системи. *Проблеми системного підходу в економіці*. 2017. № 6 (62). С. 25–32.

350. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. № 537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.

351. Проданова І.І. Національна економіка як система взаємопов’язаних середовищ: показники результативності їх функціонування. *Глобальні та національні проблеми економіки*. 2016. № 11. С. 205-210. URL: http://global-national.in.ua/archive/11-2016/45.pdf.

352. Прушківська Е.В. Еволюція концепцій структурування національної економіки. *Проблеми економіки*. 2013. № 2. С. 87-94.

353. Решетило В.П. Національна економіка. Харків : ХНАМГ, 2009. 386 с.

354. Російсько-українська кібервійна. *Wikipedia* : вебсайт. URL: https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%B0_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B2%D1%96%D0%B9%D0%BD%D0%B0.

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

356. Савченко П.В. Национальная экономика. М. : Экономистъ, 2005. 813 с.

357. Світлична В.Ю. Інформаційна безпека: сутність та порядок реалізації. *Молодий вчений.* 2014. №11(14). С. 97-100.

358. Сердюк В.Н. Системно-динамическое имматационное моделирование стратегического развития машиностроительного предприятия. *Экономика и организация управления.* 2013. № 1-2. С. 90-101.

359. Січко Т. Методи моделювання бізнес-процесів підприємства засобами системного аналізу. *Галицький економічний вісник.* 2016. №2(51). С. 190-201.

360. Скірка Н.Я. Структура економіки: сутність, основні завдання та типи. *Науковий вісник НЛТУУ : збірник науково-технічних праць.* 2008. № 18(5). С. 205-217.

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

362. Старостенко Г.Г., Онишко С.В., Поснова Т.В. Національна економіка. К. : Ліра-К, 2011. 432 с.

363. Старостіна А., Прушківська Е. Економічний зміст поняття національної економіки та її структури в умовах економічної нестабільності. *Економіст*. 2013. № 6. С. 29-32.

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

365. Указ Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»». *Президент України* : офіційний вебсайт. URL: https://www.president.gov.ua/documents/962016-19836.

366. Указ Президента України від 25 лютого 2017 року № 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». *Президент України* : офіційний вебсайт. URL: https://www.president.gov.ua/documents/472017-21374.

367. Україна 2030Е – країна з розвинутою цифровою економікою. *Український інститут майбутнього* : вебсайт. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html.

368. Філіпішина Л.М. Інтегральна оцінка стійкості розвитку промислових підприємств. *Економіка та управління підприємствами*. 2017. № 19. С. 280-285.

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

370. Ходжаян А. Макроекономічні умови стійкого розвитку національної економіки. *Теоретичні та прикладні питання економіки*. 2011. №26. С. 128-141.

371. Цанько О. Принципи сталого розвитку і проблеми формування державної інвестиційної політики. *Ефективність державного управління*. 2017. №4(53), Ч.2. С. 189-196.

372. Цифрова адженда України – 2020 («Цифровий порядок денний» – 2020). Концептуальні засади (версія 1.0): Першочергові сфери, ініціативи,

проекти «цифровізації» України до 2020 року. *Торгово-промислова палата України* : вебсайт. URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf.

373. Чухно А. Производственно-технологическая структура экономики: сущность и пути перестройки. *Экономика Украины*. 1995. № 7. С. 4–15.

374. Чухно А.А. Економічна теорія. К. : ДННУ АФУ, 2010. № 1. 512 с.

375. Шамрін Р.В. Імітаційне моделювання економічних систем: програмні засоби та напрями їх вдосконалення. *Економіка та держава*. 2016. № 1. С. 35-39.

376. Шевченко Л. С. Економічна безпека держави: сутність та напрями формування. Харків : Право, 2009. 312 с.

377. Шевчук Я.В. Динамічні моделі розвитку міст і регіонів як середовища формування автотранспортної інфраструктури. *Економіка і управління.* 2011. № 3. С. 128-133.

378. Шинкарук Л.В. Структурні трансформації в економіці України: динаміка, суперечності та вплив на економічний розвиток. Київ : НАН України, ДУ «Ін-т екон. та прогнозув. НАН України», 2015. 304 с.

379. Юськів Б.М. Опорний конспект лекцій з дисципліни “Інформаційні війни”. Рівне : РІС КСУ, 2003. 55 с.

380. Яровенко Г. М. Автоматизація як перспективний напрям розвитку зовнішнього аудиту. *Інвестиції: практика та досвід.* 2012. № 4. С. 34-38.

381. Яровенко Г. М. Аналіз видів загроз та їх наслідків щодо забезпечення інформаційної безпеки держави. *Вісник Хмельницького національного університету*. *Економічні науки.* 2018. № 6(3). С. 103-109.

382. Яровенко Г. М. Аналіз макропоказників, що характеризують рівень складових інформаційної безпеки. *Вісник Хмельницького національного університету*. *Економічні науки.* 2019. № 4(3). С. 47-54.

383. Яровенко Г.М. Аспекти автоматизації фінансового контролю підприємств. *Вісник Української академії банківської справи*. 2004. № 2(17) С. 89-96. URL: https://essuir.sumdu.edu.ua/handle/123456789/54128.

384. Яровенко Г. М. Бібліометричний аналіз досліджень інформаційної безпеки в розрізі розвитку національної економіки. *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки»*. 2020. № 8(40). С. 53-63.

385. Яровенко Г. М. Визначення джерел ефективності в гомоморфній та ізоморфній системах. *Перспективи стабільного економічного розвитку та економічної безпеки України та її регіонів*: зб. матеріалиів доповідей Міжнар. наук.-практ. конф., 8 трав. 2015 р. Ужгород: Видавничий дім «Гельветика», 2015. Ч.3. С. 131-133.

386. Яровенко Г. М. Використання карт Кохонена для аналізу рівня інформаційної безпеки країн з урахуванням їх розвитку. *Економічний простір*. 2020. № 157. С. 118-124.

387. Яровенко Г. М. Використання математичних методів та моделей у забезпеченні ефективності корпоративних інформаційних систем. *Актуальні проблеми теорії та практики менеджменту* : зб. матеріалів міжнар. наук.-практ. конф., 16-17 серп. 2013 р. Сімферополь, 2013. С. 92-94.

388. Яровенко Г. М. Вплив рівня економічного розвитку країни на залежність використання персональних засобів інформаційної безпеки та наслідків кіберзлочинів. *Вісник Сумського державного університету. Серія «Економіка»*. 2020. № 1. С.188-198.

389. 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.

390. Яровенко Г. М. Метод оцінки економічної ефективності автоматизованих інформаційних систем на основі статистики результатів впроваджень. *Формування фінансової системи в умовах глобалізації* : XXIV Міжнар. наук.-практ. конф., 9-10 серп. 2013 р. Київ, 2013. С. 71-74.

391. Яровенко Г. М. Методика визначення витрат на обробку інформації при впровадженні автоматизованої системи управління. *Сучасні шляхи*

стабілізації економічного стану країни : матеріали Міжнар. наук.-практ. конф., 1-2 квіт. 2016 р. Д. : НО «Перспектива». 2016. Ч.2. С. 99-101.

392. Яровенко Г. М. Моделювання в бухгалтерському обліку як засіб підвищення ефективності його автоматизації. *Інвестиції: практика та досвід.* 2012. № 6. С. 100-104.

393. Яровенко Г. М. Моделювання та автоматизація обліку, контролю, аудиту. Суми : Видавництво: ПП Вінниченко М.Д., ФОП Литовченко Є.Б., 2016. 156 с.

394. Яровенко Г. М. Наслідки інформаційних війн як фактор економічної дестабілізації країни. *Міжнародний науковий журнал "Інтернаука". Серія: "Економічні науки"*. 2020. № 9(1). С. 94-103.

395. Яровенко Г. М. Розробка інформаційної моделі виявлення ознак шахрайств у банках. *Інвестиції: практика та досвід.* 2018. № 14. С. 23-28.

396. Яровенко Г. М. Системний підхід до побудови інформаційної моделі виявлення передумов виникнення шахрайств в банках. *Актуальні проблеми моделювання та управління соціально-економічними системами в умовах глобалізації* : матеріали міжнар. наук.-практ. конф. Дрогобич, 2018. С. 66-69.

397. Яровенко Г. М. Системний підхід до формалізації поняття «Інформаційна безпека». *Причорноморські економічні студії*. 2018. № 34. С. 239-244.

398. Яровенко Г. М. Тенденції розвитку національної економіки в умовах її цифровізації. *Причорноморські економічні студії*. 2019. № 39(1). С. 159-164.

399. Яровенко Г. М. Формування інформації для оцінки джерел ефективності використання автоматизованої інформаційної системи підприємства. *Економіка, менеджмент, фінанси: теоретичні та практичні аспекти розвитку*: зб. тез наук. робіт учасн. Міжнар. наук.-практ. конф., 22-23 трав. 2015. К. : Аналітичний центр "Нова Економіка". 2015. № 2. С. 101-102.

400. Яровенко Г. М., Бояджян М. М. Аналіз наслідків кібершахрайств в банківській системі України. *Економіка та суспільство*. 2018. № 18. С. 836-843. URL: http://economyandsociety.in.ua/journals/18_ukr/116.pdf.

401. Яровенко Г. М., Бояджян М. М. Концептуальна модель виявлення ознак кібершахрайств в банках. *Сучасні міжнародні економічні відносини: становлення та шляхи перспективного розвитку* : зб. тез наук. робіт учасн. Всеукр. наук.-практ. конф., 9-10 лют. 2018 р. О. : ЦЕДР, 2018. С. 98-100.

402. Яровенко Г. М., Бояджян М. М. Оцінка впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері. *Проблеми та перспективи розвитку фінансово-кредитної системи України* : зб. матеріалів III Всеукр. наук.-практ. on-line конф., 22-23 листоп. 2018 р. Суми : ННІ БТ «УАБС» СумДУ, 2018. С. 294-297.

403. Яровенко Г. М., Доценко Т. В., Кушнерьов О. С. Формування інтегрального індексу загрози національної економіки. *Вісник Сумського державного університету. Серія «Економіка*. 2020. № 2. С. 16-28.

404. Яровенко Г. М., Ковач В. О. Моделювання портретів потенційних шахрая та жертви банківських шахрайств. *Ефективна економіка.* 2018. № 10. URL: http://www.economy.nayka.com.ua/pdf/10_2018/63.pdf.

405. Яровенко Г. М., Ковач В. О. Перспективи застосування технології блокчейн в системах забезпечення кібербезпеки банків. *Підприємництво та інновації.* 2020. № 12. С. 206-214.

406. Яровенко Г. М., Колотіліна О. В. Оцінка ризиків соціо-економіко-політичного розвитку України. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Економіка і управління*. 2020. Т. 31 (70), № 4. С. 151-159.

407. Яровенко Г. М., Коркішко А. В. Моделювання ймовірності виникнення шахрайських операцій з кредитними картками. *Збірник наукових праць "Проблеми і перспективи розвитку банківської системи України"*. 2015. № 41. С. 237-248.

408. Яровенко Г. М., Нечепоренко І. Д. Сучасні технології кіберзахисту щодо виявлення шахрайств, які здійснюються персоналом банку. *Проблеми та перспективи розвитку фінансово-кредитної системи України* : зб. матеріалів IV

Всеукр. наук.-практ. on-line конф., 21–22 листоп. 2019 р. Суми : Сумський державний університет, 2019. № 2. С. 149-153.

409. Яровенко Г. М., Сковронська А. І., Бояджян М. М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу. *Ефективна економіка.* 2018. № 7. URL: http://www.economy. nayka.com.ua/pdf/7_2018/39.pdf.

410. Яровенко Г. М., Титаренко А. К. Методи дослідження ринку автоматизованих інформаційних систем. *Ефективна економіка*. 2011. № 6. URL: http:// www.economy.nayka.com.ua/index.php?operation=1&iid=590.

ДОДАТКИ

Додаток А

Результати проведеного канонічного аналізу для обґрунтування складу індикаторів рівня інформаційної безпеки країни

N=159	Canonical Analysis Summary (Kanonich_analyse.sta) Canonical R: .78758 Chi²(20)=164.33 p=0.0000	
	Left Set	Right Set
No. of variables	5	4
Variance extracted	95.2907%	100.000%
Total redundancy	47.4678%	23.8074%
Variables: 1	Global Cybersecurity Index	Life expectancy
2	ICT Development Index	Wage and salaried workers
3	Networked Readiness Index	GINI index
4	National Cyber Security Index	Unemployment
5	Digital Development Level	

Рисунок А.1 – Підсумки канонічного аналізу для групи соціального розвитку та цифрової спроможності національної економіки і кібербезпеки (складено авторкою)

N=159	Canonical Analysis Summary (Kanonich_analyse.sta) Canonical R: .51239 Chi²(10)=53.294 p=0.0000	
	Left Set	Right Set
No. of variables	5	2
Variance extracted	77.1474%	100.000%
Total redundancy	18.1029%	18.4117%
Variables: 1	Global Cybersecurity Index	Statistical Capacity score
2	ICT Development Index	Secure Internet servers
3	Networked Readiness Index	
4	National Cyber Security Index	
5	Digital Development Level	

Рисунок А.2 – Підсумки канонічного аналізу для групи якості інформаційної інфраструктури та цифрової спроможності національної економіки і кібербезпеки (складено авторкою)

N=159	Canonical Analysis Summary (Kanonich_analyse.sta) Canonical R: .94334 Chi²(40)=387.04 p=0.0000 Left Set	Right Set
No. of variables	5	8
Variance extracted	100.000%	80.8815%
Total redundancy	67.7978%	24.7199%
Variables: 1	Global Cybersecurity Index	Mobile cellular subscriptions
2	ICT Development Index	Individuals using the Internet
3	Networked Readiness Index	Charges for the use of intellectual property, payments
4	National Cyber Security Index	Charges for the use of intellectual property, receipts
5	Digital Development Level	High-technology exports
6		Patent applications, nonresidents
7		Patent applications, residents
8		Scientific and technical journal articles

Рисунок А.3 – Підсумки канонічного аналізу для групи інноваційної активності та цифрової спроможності національної економіки і кібербезпеки (складено авторкою)

N=159	Canonical Analysis Summary (Kanonich_analyse.sta) Canonical R: .59613 Chi²(25)=87.693 p=0.0000 Left Set	Right Set
No. of variables	5	5
Variance extracted	100.000%	100.000%
Total redundancy	27.1537%	10.5896%
Variables: 1	Global Cybersecurity Index	Portfolio investment
2	ICT Development Index	Total reserves
3	Networked Readiness Index	Foreign direct investment, net inflows
4	National Cyber Security Index	Inflation, GDP deflator
5	Digital Development Level	Tax revenue

Рисунок А.4 – Підсумки канонічного аналізу для групи фінансового розвитку та цифрової спроможності національної економіки і кібербезпеки (складено авторкою)

N=159	Canonical Analysis Summary (Kanonich_analyse.sta) Canonical R: .58151 Chi²(20)=91.891 p=0.0000 **Left Set**	Right Set
No. of variables	5	4
Variance extracted	96.6724%	100.000%
Total redundancy	25.3595%	15.4336%
Variables: 1	Global Cybersecurity Index	Current account balance
2	ICT Development Index	Exports of goods and services
3	Networked Readiness Index	External debt stocks, total
4	National Cyber Security Index	Imports of goods and services
5	Digital Development Level	

Рисунок А.5 – Підсумки канонічного аналізу для групи зовнішньоекономічної діяльності та цифрової спроможності національної економіки і кібербезпеки (складено авторкою)

Таблиця А.1 – Результати розрахунку канонічної змінної Y

Країна	Y	Країна	Y
Afghanistan	16,7359	Bulgaria	71,9362
Albania	60,2857	Burundi	20,8163
Algeria	43,5984	Cambodia	36,5978
Angola	14,3314	Cameroon	37,5856
Antigua and Barbuda	39,8953	Canada	87,7559
Argentina	62,3530	Chad	20,7440
Armenia	60,9449	Chile	67,3052
Australia	89,3958	China	67,7325
Austria	87,4518	Colombia	61,6298
Azerbaijan	66,8116	Congo (Democratic Republic)	9,5797
Bahamas	43,4191	Costa Rica	60,4839
Bahrain	74,3251	Côte d'Ivoire	44,3552
Bangladesh	42,5263	Croatia	80,1432
Barbados	47,6940	Cuba	29,1530
Belarus	62,5513	Cyprus	75,5856
Belgium	87,8734	Czech Republic	76,8452
Belize	24,9182	Denmark	93,2345
Benin	38,8680	Dominica	33,7401
Bhutan	40,9221	Dominican Republic	51,4340
Bolivia	41,1101	Ecuador	52,3719
Bosnia and Herzegovina	50,7083	Egypt	61,2733
Botswana	49,6236	El Salvador	39,7216
Brazil	64,2759	Estonia	92,0202
Brunei Darussalam	56,9775	Ethiopia	32,6330

Продовження таблиці А.1

Країна	Y	Країна	Y
Finland	92,1464	Morocco	52,4387
France	91,4458	Mozambique	29,6779
Georgia	71,5473	Myanmar	31,4877
Germany	91,8052	Namibia	37,5162
Ghana	48,3913	Nepal	37,5013
Greece	73,4903	Netherlands	94,3303
Grenada	38,1795	New Zealand	87,0997
Guatemala	40,8039	Nicaragua	33,4127
Guyana	36,3313	Nigeria	47,9159
Haiti	22,2315	North Macedonia	70,3294
Honduras	34,7755	Norway	92,2913
Hungary	76,9267	Oman	72,3600
Iceland	81,2147	Pakistan	41,4294
India	54,7381	Panama	55,9806
Indonesia	60,5038	Papua New Guinea	4,3288
Iran (Islamic Republic of)	58,6683	Paraguay	54,7934
Ireland	85,3442	Peru	53,2517
Israel	85,4172	Philippines	58,2068
Italy	79,2576	Poland	78,0520
Jamaica	52,6229	Portugal	79,8108
Japan	90,6837	Qatar	82,3665
Jordan	61,0674	Romania	68,8399
Kazakhstan	74,7939	Russian Federation	78,7886
Kenya	52,4317	Rwanda	48,1095
Kiribati	13,8332	Saint Kitts and Nevis	44,3754
Korea (Republic of)	92,4358	Saint Lucia	29,8889
Kyrgyzstan	45,1616	Saint Vincent and the Grenadines	36,7262
Lao PDR	36,0130	Samoa	28,0974
Latvia	79,8916	Saudi Arabia	79,0300
Liberia	27,3660	Senegal	37,4882
Libya	29,6036	Serbia	70,9599
Lithuania	85,3595	Seychelles	48,5490
Luxembourg	91,6642	Sierra Leone	3,6219
Madagascar	26,3096	Singapore	93,7283
Malawi	29,6732	Slovakia	77,2922
Malaysia	79,9071	Slovenia	77,0943
Mali	27,9969	Solomon Islands	13,8036
Malta	74,0682	South Africa	60,1992
Mauritania	26,1800	South Sudan	1,7439
Mauritius	72,5041	Spain	87,2350
Mexico	60,4690	Sudan	22,7299
Moldova	68,0941	Suriname	34,4044
Mongolia	54,8762	Sweden	89,5564

Продовження таблиці А.1

Країна	Y	Країна	Y
Montenegro	67,0858	Switzerland	92,4152
Syrian Arab Republic	26,3032	United Arab Emirates	80,2378
Tajikistan	31,6171	United Kingdom	95,0016
Tanzania, United Republic of	38,3699	United States	93,7026
Thailand	68,2211	Uruguay	73,7736
Tonga	32,1908	Uzbekistan	46,9127
Trinidad and Tobago	52,8664	Vanuatu	19,5680
Tunisia	55,8496	Venezuela	50,6988
Turkey	73,3268	Vietnam	57,8975
Turkmenistan	3,1619	Yemen	1,0329
Tuvalu	1,6479	Zambia	41,3882
Uganda	44,4958	Zimbabwe	33,5650
Ukraine	66,7997	X	X

Таблиця А.2 – Результати розрахунку канонічної змінної X

Країна	X	Країна	X
Afghanistan	-0,7351	Canada	1,5945
Albania	0,3820	Chad	-1,2353
Algeria	-0,5049	Chile	1,2401
Angola	-1,0540	China	0,7194
Antigua and Barbuda	-0,1884	Colombia	0,4067
Argentina	-0,0118	Congo (Democratic Republic of the)	-1,1456
Armenia	0,3354	Costa Rica	0,2625
Australia	1,5891	Côte d'Ivoire	-0,2665
Austria	1,3336	Croatia	0,4374
Azerbaijan	0,2859	Cuba	-1,0618
Bahamas	0,0608	Cyprus	1,0565
Bahrain	0,6289	Czech Republic	1,0326
Bangladesh	-0,5557	Denmark	1,6913
Barbados	-0,0705	Dominica	-0,8924
Belarus	-0,5560	Dominican Republic	-0,2106
Belgium	1,0975	Ecuador	-0,3748
Belize	-0,8400	Egypt	-0,4784
Benin	-0,5682	El Salvador	-0,1561
Bhutan	-0,6553	Estonia	1,2188
Bolivia	-0,3185	Ethiopia	-0,5339
Bosnia and Herzegovina	-0,4943	Finland	1,8322
Botswana	-0,0060	France	1,5922
Brazil	-0,3875	Georgia	1,0182
Brunei Darussalam	1,1074	Germany	1,6070
Bulgaria	0,5037	Ghana	-0,2633
Burundi	-0,9811	Greece	0,5088
Cambodia	-0,3125	Grenada	-0,8695

Продовження таблиці А.2

Країна	X	Країна	X
Cameroon	-0,3726	Guatemala	-0,3374
Guyana	-0,3720	Nigeria	-0,5154
Haiti	-2,0608	North Macedonia	0,5378
Honduras	-0,4464	Norway	1,6941
Hungary	0,5400	Oman	0,0272
Iceland	1,0930	Pakistan	-0,0435
India	0,5959	Panama	0,2710
Indonesia	0,4644	Papua New Guinea	-0,4516
Iran (Islamic Republic of)	-0,2555	Paraguay	-0,2768
Ireland	1,3501	Peru	0,2351
Israel	1,8192	Philippines	0,6380
Italy	0,5717	Poland	0,7270
Jamaica	0,6695	Portugal	1,0709
Japan	1,5822	Qatar	0,4390
Jordan	0,1921	Romania	-0,1428
Kazakhstan	0,3144	Russian Federation	0,2496
Kenya	0,0830	Rwanda	0,0320
Kiribati	-1,1060	Saint Kitts and Nevis	0,4534
Korea (Republic of)	1,3597	Saint Lucia	-0,1843
Kyrgyzstan	-0,2724	Saint Vincent and the Grenadines	-0,2212
Lao PDR	-0,7931	Samoa	0,0186
Latvia	1,3945	Saudi Arabia	0,3707
Liberia	-1,5406	Senegal	-0,3104
Libya	-1,7152	Serbia	0,2665
Lithuania	1,2480	Seychelles	0,0851
Luxembourg	1,5206	Sierra Leone	-1,4735
Madagascar	-1,0959	Singapore	2,1485
Malawi	-0,7525	Slovakia	0,7845
Malaysia	1,3270	Slovenia	0,9573
Mali	-0,5348	Solomon Islands	-1,6701
Malta	1,0221	South Africa	0,5782
Mauritania	-0,6522	South Sudan	-2,2790
Mauritius	1,0454	Spain	1,1888
Mexico	0,4207	Sudan	-1,4716
Moldova	-0,1811	Suriname	-0,9864
Mongolia	-0,3257	Sweden	1,6986
Montenegro	0,2544	Switzerland	1,8690
Morocco	-0,1664	Syrian Arab Republic	-1,1689
Mozambique	-0,7324	Tajikistan	-0,8928
Myanmar	-0,9064	Tanzania, United Republic of	-0,7836
Namibia	-0,2216	Thailand	0,8104
Nepal	-0,9246	Tonga	-0,2324
Netherlands	1,8781	Trinidad and Tobago	0,2836
New Zealand	1,3927	Tunisia	-0,0311

Продовження таблиці А.2

Країна	X	Країна	X
Nicaragua	-0,5238	Turkey	0,5104
Turkmenistan	-1,4024	Uzbekistan	-0,5147
Tuvalu	-1,5344	Vanuatu	-0,9983
Uganda	-0,2410	Venezuela	-1,6779
Ukraine	0,3062	Vietnam	-0,0393
United Arab Emirates	1,3988	Yemen	-1,7179
United Kingdom	1,4682	Zambia	-0,6185
United States	1,7664	Zimbabwe	-1,2993
Uruguay	0,0661	X	X

Додаток Б

Результати розрахунків інтегрального індексу інформаційної безпеки національної економіки

Таблиця Б.1 – Розрахунки нормалізованих значень індикаторів інституційної спроможності та їх значень, приведених до безрозмірної шкали бажаності Харрінгтона

Назва країни	Нормалізовані значення індикаторів інституційної спроможності					Значення індикаторів, приведені до безрозмірної шкали бажаності Харрінгтона				
	ОКК*	ОЕУ*	ОПС*	ОЯР*	ОВП*	ОКК	ОЕУ	ОПС	ОЯР	ОВП
Afghanistan	0,181	0,174	0,059	0,229	0,150	0,434	0,431	0,390	0,451	0,423
Albania	0,371	0,518	0,611	0,560	0,397	0,501	0,551	0,581	0,565	0,511
Algeria	0,344	0,376	0,319	0,206	0,307	0,492	0,503	0,483	0,443	0,479
Angola	0,239	0,243	0,433	0,254	0,251	0,455	0,456	0,523	0,460	0,459
Antigua and Barbuda	0,568	0,487	0,691	0,593	0,597	0,567	0,541	0,606	0,575	0,577
Argentina	0,478	0,495	0,520	0,426	0,435	0,538	0,544	0,552	0,520	0,524
Armenia	0,412	0,482	0,408	0,557	0,458	0,516	0,539	0,514	0,564	0,531
Australia	0,860	0,834	0,743	0,874	0,852	0,655	0,648	0,621	0,659	0,653
Austria	0,832	0,812	0,731	0,824	0,872	0,647	0,642	0,618	0,645	0,658
Azerbaijan	0,302	0,463	0,341	0,392	0,347	0,477	0,533	0,491	0,509	0,493
Bahamas	0,757	0,626	0,722	0,527	0,522	0,625	0,586	0,615	0,554	0,552
Bahrain	0,462	0,535	0,309	0,602	0,602	0,533	0,557	0,480	0,578	0,578
Bangladesh	0,286	0,305	0,268	0,289	0,338	0,472	0,479	0,465	0,473	0,490
Barbados	0,805	0,598	0,732	0,625	0,597	0,639	0,577	0,618	0,585	0,577
Belarus	0,451	0,411	0,604	0,326	0,295	0,529	0,515	0,579	0,486	0,475
Belgium	0,820	0,763	0,618	0,773	0,802	0,644	0,627	0,583	0,630	0,638

Продовження таблиці Б.1

Назва країни	Нормалізовані значення індикаторів інституційної спроможності					Значення індикаторів, приведені до безрозмірної шкали бажаності Харрінгтона				
	ОКК*	ОЕУ*	ОПС*	ОЯР*	ОВП*	ОКК	ОЕУ	ОПС	ОЯР	ОВП
Belize	0,464	0,340	0,518	0,326	0,297	0,533	0,491	0,551	0,486	0,476
Benin	0,404	0,347	0,480	0,402	0,330	0,513	0,493	0,539	0,512	0,487
Bhutan	0,839	0,581	0,767	0,403	0,635	0,649	0,572	0,629	0,513	0,589
Bolivia	0,347	0,406	0,452	0,275	0,232	0,493	0,514	0,529	0,468	0,452
Bosnia and Herzegovina	0,359	0,334	0,414	0,435	0,437	0,497	0,489	0,516	0,524	0,524
Botswana	0,679	0,575	0,744	0,604	0,615	0,602	0,570	0,622	0,579	0,582
Brazil	0,395	0,375	0,423	0,409	0,426	0,510	0,503	0,520	0,514	0,520
Brunei Darussalam	0,689	0,778	0,785	0,659	0,654	0,605	0,632	0,634	0,596	0,594
Bulgaria	0,461	0,559	0,620	0,633	0,489	0,532	0,564	0,584	0,588	0,542
Burundi	0,188	0,179	0,170	0,257	0,174	0,437	0,434	0,430	0,462	0,432
Cambodia	0,208	0,346	0,542	0,362	0,238	0,444	0,493	0,559	0,498	0,455
Cameroon	0,239	0,294	0,205	0,295	0,245	0,455	0,475	0,443	0,475	0,457
Canada	0,868	0,850	0,746	0,841	0,859	0,657	0,652	0,622	0,650	0,655
Chad	0,194	0,163	0,188	0,233	0,205	0,439	0,428	0,437	0,453	0,443
Chile	0,734	0,746	0,621	0,792	0,757	0,619	0,622	0,584	0,636	0,626
China	0,431	0,611	0,448	0,454	0,445	0,522	0,581	0,528	0,530	0,527
Colombia	0,424	0,466	0,315	0,572	0,393	0,520	0,534	0,482	0,569	0,509
Congo (Democratic Republic)	0,180	0,160	0,107	0,173	0,136	0,434	0,426	0,407	0,431	0,418
Costa Rica	0,634	0,586	0,636	0,610	0,618	0,588	0,573	0,589	0,581	0,583
Côte d'Ivoire	0,376	0,346	0,289	0,439	0,352	0,503	0,493	0,473	0,525	0,495
Croatia	0,532	0,606	0,700	0,602	0,580	0,556	0,579	0,609	0,578	0,571
Cuba	0,541	0,426	0,675	0,175	0,384	0,559	0,520	0,601	0,432	0,506
Cyprus	0,655	0,713	0,649	0,731	0,682	0,595	0,613	0,593	0,618	0,603
Czech Republic	0,623	0,713	0,755	0,778	0,744	0,585	0,613	0,625	0,632	0,622
Denmark	0,896	0,870	0,740	0,843	0,867	0,665	0,658	0,620	0,650	0,657

Продовження таблиці Б.1

Назва країни	Нормалізовані значення індикаторів інституційної спроможності					Значення індикаторів, приведені до безрозмірної шкали бажаності Харрінгтона				
	ОКК*	ОЕУ*	ОПС*	ОЯР*	ОВП*	ОКК	ОЕУ	ОПС	ОЯР	ОВП
Dominica	0,633	0,414	0,768	0,509	0,651	0,588	0,516	0,629	0,548	0,594
Dominican Republic	0,319	0,387	0,523	0,468	0,396	0,483	0,507	0,553	0,535	0,510
Ecuador	0,361	0,421	0,495	0,276	0,340	0,498	0,519	0,544	0,468	0,491
Egypt	0,356	0,342	0,242	0,281	0,392	0,496	0,492	0,456	0,470	0,509
El Salvador	0,355	0,375	0,429	0,478	0,297	0,496	0,503	0,521	0,538	0,476
Estonia	0,819	0,767	0,663	0,827	0,780	0,644	0,629	0,597	0,646	0,632
Ethiopia	0,379	0,337	0,210	0,259	0,388	0,504	0,490	0,445	0,462	0,508
Finland	0,902	0,882	0,733	0,857	0,890	0,667	0,661	0,618	0,654	0,663
France	0,789	0,816	0,542	0,762	0,813	0,635	0,643	0,559	0,627	0,642
Georgia	0,670	0,644	0,406	0,752	0,580	0,599	0,591	0,514	0,624	0,571
Germany	0,876	0,837	0,664	0,853	0,841	0,659	0,649	0,598	0,653	0,650
Ghana	0,470	0,434	0,522	0,468	0,515	0,535	0,523	0,553	0,534	0,550
Greece	0,482	0,576	0,538	0,564	0,536	0,539	0,570	0,558	0,566	0,557
Grenada	0,593	0,423	0,747	0,414	0,576	0,575	0,520	0,623	0,516	0,570
Guatemala	0,303	0,320	0,378	0,438	0,251	0,478	0,484	0,504	0,525	0,459
Guyana	0,442	0,419	0,470	0,355	0,415	0,526	0,518	0,535	0,496	0,517
Haiti	0,218	0,116	0,357	0,213	0,255	0,448	0,411	0,497	0,446	0,461
Honduras	0,349	0,334	0,375	0,370	0,256	0,494	0,489	0,503	0,501	0,461
Hungary	0,512	0,613	0,697	0,639	0,636	0,549	0,582	0,608	0,590	0,589
Iceland	0,864	0,814	0,819	0,804	0,853	0,656	0,642	0,644	0,639	0,653
India	0,452	0,562	0,284	0,441	0,503	0,529	0,565	0,471	0,526	0,546
Indonesia	0,436	0,535	0,380	0,470	0,416	0,524	0,557	0,505	0,535	0,517
Iran (Islamic Republic of)	0,275	0,379	0,217	0,201	0,326	0,468	0,504	0,447	0,441	0,486
Ireland	0,825	0,807	0,754	0,831	0,817	0,645	0,640	0,625	0,647	0,643
Israel	0,687	0,770	0,289	0,775	0,733	0,605	0,629	0,473	0,631	0,619

Продовження таблиці Б.1

Назва країни	Нормалізовані значення індикаторів інституційної спроможності					Значення індикаторів, приведені до безрозмірної шкали бажаності Харрінгтона				
	ОКК*	ОЕУ*	ОПС*	ОЯР*	ОВП*	ОКК	ОЕУ	ОПС	ОЯР	ОВП
Italy	0,558	0,595	0,593	0,656	0,560	0,564	0,576	0,576	0,595	0,565
Jamaica	0,458	0,615	0,636	0,560	0,436	0,531	0,582	0,589	0,565	0,524
Japan	0,807	0,845	0,759	0,790	0,827	0,640	0,651	0,626	0,635	0,646
Jordan	0,537	0,518	0,418	0,510	0,557	0,557	0,551	0,518	0,548	0,564
Kazakhstan	0,375	0,494	0,515	0,524	0,388	0,503	0,543	0,550	0,553	0,507
Kenya	0,297	0,384	0,242	0,430	0,393	0,476	0,506	0,456	0,522	0,509
Kiribati	0,583	0,418	0,754	0,301	0,621	0,572	0,518	0,625	0,477	0,584
Korea (Republic of)	0,647	0,765	0,650	0,747	0,779	0,592	0,628	0,593	0,623	0,632
Kyrgyzstan	0,276	0,336	0,368	0,399	0,279	0,468	0,489	0,501	0,511	0,469
Lao PDR	0,270	0,322	0,619	0,297	0,293	0,466	0,484	0,584	0,476	0,474
Latvia	0,581	0,738	0,620	0,765	0,726	0,572	0,620	0,584	0,628	0,616
Liberia	0,297	0,192	0,465	0,260	0,263	0,476	0,438	0,534	0,462	0,463
Libya	0,173	0,123	0,079	0,084	0,136	0,431	0,413	0,397	0,399	0,418
Lithuania	0,622	0,744	0,697	0,750	0,726	0,585	0,622	0,608	0,624	0,616
Luxembourg	0,891	0,858	0,813	0,854	0,864	0,663	0,654	0,642	0,653	0,656
Madagascar	0,267	0,224	0,383	0,309	0,299	0,465	0,450	0,506	0,480	0,476
Malawi	0,320	0,309	0,431	0,323	0,400	0,484	0,480	0,522	0,485	0,512
Malaysia	0,577	0,745	0,575	0,658	0,652	0,570	0,622	0,570	0,596	0,594
Mali	0,331	0,252	0,114	0,351	0,303	0,488	0,460	0,410	0,495	0,478
Malta	0,641	0,723	0,800	0,791	0,745	0,590	0,616	0,638	0,635	0,622
Mauritania	0,307	0,310	0,348	0,293	0,327	0,479	0,480	0,493	0,474	0,486
Mauritius	0,566	0,703	0,722	0,733	0,688	0,567	0,610	0,615	0,619	0,605
Mexico	0,295	0,449	0,370	0,527	0,330	0,475	0,528	0,501	0,554	0,487
Moldova (Republic of)	0,324	0,370	0,425	0,476	0,392	0,485	0,501	0,520	0,537	0,509
Mongolia	0,393	0,428	0,705	0,481	0,429	0,509	0,521	0,610	0,539	0,521

Продовження таблиці Б.1

Назва країни	Нормалізовані значення індикаторів інституційної спроможності					Значення індикаторів, приведені до безрозмірної шкали бажаності Харрінгтона				
	ОКК*	ОЕУ*	ОПС*	ОЯР*	ОВП*	ОКК	ОЕУ	ОПС	ОЯР	ОВП
Montenegro	0,505	0,523	0,542	0,581	0,522	0,547	0,553	0,559	0,572	0,553
Morocco	0,445	0,435	0,430	0,426	0,461	0,527	0,523	0,522	0,520	0,532
Mozambique	0,312	0,278	0,321	0,311	0,252	0,481	0,469	0,484	0,481	0,460
Myanmar	0,355	0,239	0,216	0,305	0,254	0,496	0,455	0,447	0,479	0,460
Namibia	0,584	0,516	0,675	0,475	0,560	0,572	0,551	0,601	0,537	0,565
Nepal	0,336	0,272	0,358	0,307	0,376	0,489	0,467	0,497	0,479	0,503
Netherlands	0,883	0,867	0,721	0,884	0,865	0,661	0,657	0,615	0,662	0,656
New Zealand	0,899	0,844	0,838	0,880	0,872	0,666	0,651	0,649	0,660	0,658
Nicaragua	0,255	0,293	0,317	0,320	0,253	0,461	0,474	0,483	0,484	0,460
Nigeria	0,258	0,248	0,100	0,278	0,285	0,462	0,458	0,405	0,469	0,471
North Macedonia	0,408	0,512	0,464	0,621	0,424	0,514	0,549	0,533	0,584	0,520
Norway	0,891	0,871	0,776	0,854	0,882	0,663	0,658	0,631	0,653	0,661
Oman	0,561	0,537	0,675	0,568	0,614	0,565	0,557	0,601	0,567	0,582
Pakistan	0,310	0,331	0,093	0,329	0,330	0,480	0,488	0,402	0,487	0,487
Panama	0,360	0,483	0,585	0,591	0,481	0,498	0,540	0,573	0,575	0,539
Papua New Guinea	0,292	0,321	0,348	0,353	0,310	0,474	0,484	0,494	0,495	0,480
Paraguay	0,298	0,358	0,484	0,456	0,361	0,476	0,497	0,540	0,531	0,498
Peru	0,366	0,425	0,448	0,619	0,367	0,500	0,520	0,528	0,584	0,500
Philippines	0,365	0,501	0,251	0,500	0,376	0,500	0,546	0,459	0,545	0,503
Poland	0,655	0,655	0,650	0,703	0,605	0,595	0,595	0,593	0,609	0,579
Portugal	0,701	0,770	0,774	0,705	0,762	0,609	0,629	0,631	0,610	0,627
Qatar	0,674	0,648	0,680	0,619	0,678	0,601	0,593	0,603	0,583	0,602
Romania	0,468	0,423	0,530	0,601	0,580	0,535	0,520	0,555	0,578	0,571
Russian Federation	0,299	0,473	0,387	0,353	0,299	0,476	0,536	0,507	0,495	0,476
Rwanda	0,641	0,542	0,544	0,510	0,527	0,590	0,559	0,560	0,548	0,554

Продовження таблиці Б.1

Назва країни	Нормалізовані значення індикаторів інституційної спроможності					Значення індикаторів, приведені до безрозмірної шкали бажаності Харрінгтона				
	ОКК*	ОЕУ*	ОПС*	ОЯР*	ОВП*	ОКК	ОЕУ	ОПС	ОЯР	ОВП
Saint Kitts and Nevis	0,611	0,629	0,688	0,618	0,631	0,581	0,587	0,605	0,583	0,587
Saint Lucia	0,631	0,539	0,750	0,562	0,637	0,587	0,558	0,624	0,565	0,589
Saint Vincent and the Grenadines	0,683	0,539	0,718	0,554	0,606	0,604	0,558	0,614	0,563	0,580
Samoa	0,655	0,638	0,782	0,459	0,698	0,595	0,590	0,633	0,531	0,608
Saudi Arabia	0,589	0,572	0,383	0,476	0,533	0,574	0,569	0,506	0,537	0,556
Senegal	0,493	0,420	0,492	0,461	0,443	0,543	0,518	0,542	0,532	0,526
Serbia	0,407	0,517	0,536	0,490	0,459	0,514	0,551	0,557	0,542	0,532
Seychelles	0,669	0,617	0,685	0,450	0,548	0,599	0,583	0,604	0,529	0,561
Sierra Leone	0,378	0,226	0,507	0,273	0,309	0,504	0,450	0,547	0,467	0,480
Singapore	0,899	0,907	0,834	0,896	0,868	0,666	0,668	0,648	0,665	0,657
Slovakia	0,589	0,666	0,696	0,687	0,630	0,574	0,598	0,607	0,605	0,587
Slovenia	0,705	0,755	0,730	0,661	0,746	0,610	0,625	0,618	0,597	0,622
Solomon Islands	0,498	0,242	0,591	0,286	0,438	0,545	0,456	0,575	0,472	0,525
South Africa	0,494	0,576	0,444	0,532	0,470	0,543	0,570	0,526	0,556	0,535
South Sudan	0,149	0,070	0,079	0,102	0,116	0,423	0,394	0,397	0,405	0,410
Spain	0,649	0,730	0,579	0,716	0,728	0,593	0,618	0,571	0,614	0,617
Sudan	0,192	0,151	0,138	0,151	0,237	0,438	0,423	0,419	0,423	0,454
Suriname	0,446	0,326	0,534	0,332	0,480	0,527	0,486	0,557	0,488	0,539
Sweden	0,896	0,865	0,731	0,859	0,874	0,665	0,656	0,618	0,655	0,659
Switzerland	0,883	0,888	0,809	0,857	0,878	0,661	0,663	0,641	0,654	0,660
Syrian Arab Republic	0,162	0,144	0,060	0,130	0,107	0,427	0,421	0,390	0,416	0,407
Tajikistan	0,193	0,234	0,335	0,245	0,208	0,439	0,453	0,489	0,457	0,444
Tanzania, United Republic of	0,388	0,303	0,374	0,337	0,358	0,508	0,478	0,502	0,490	0,497
Thailand	0,400	0,579	0,333	0,517	0,503	0,512	0,571	0,488	0,551	0,546
Tonga	0,481	0,525	0,724	0,399	0,595	0,539	0,553	0,616	0,511	0,576

Продовження таблиці Б.1

Назва країни	Нормалізовані значення індикаторів інституційної спроможності					Значення індикаторів, приведені до безрозмірної шкали бажаності Харрінгтона				
	ОКК*	ОЕУ*	ОПС*	ОЯР*	ОВП*	ОКК	ОЕУ	ОПС	ОЯР	ОВП
Trinidad and Tobago	0,420	0,538	0,578	0,483	0,466	0,518	0,558	0,571	0,540	0,534
Tunisia	0,486	0,461	0,295	0,384	0,507	0,540	0,532	0,475	0,506	0,547
Turkey	0,415	0,490	0,213	0,476	0,415	0,517	0,542	0,446	0,537	0,517
Turkmenistan	0,203	0,244	0,513	0,108	0,181	0,442	0,457	0,549	0,408	0,434
Tuvalu	0,506	0,317	0,821	0,347	0,630	0,547	0,483	0,644	0,493	0,587
Uganda	0,260	0,337	0,342	0,424	0,421	0,462	0,490	0,492	0,520	0,519
Ukraine	0,293	0,383	0,139	0,432	0,320	0,474	0,506	0,419	0,522	0,484
United Arab Emirates	0,760	0,809	0,695	0,714	0,694	0,627	0,641	0,607	0,613	0,607
United Kingdom	0,862	0,794	0,527	0,854	0,842	0,656	0,636	0,554	0,653	0,650
United States	0,790	0,831	0,634	0,829	0,815	0,635	0,647	0,588	0,646	0,642
Uruguay	0,781	0,630	0,757	0,615	0,647	0,632	0,587	0,625	0,582	0,592
Uzbekistan	0,254	0,351	0,442	0,234	0,246	0,460	0,495	0,526	0,453	0,458
Vanuatu	0,458	0,364	0,715	0,369	0,582	0,531	0,499	0,613	0,501	0,572
Venezuela	0,185	0,156	0,210	0,079	0,081	0,436	0,425	0,445	0,397	0,398
Vietnam	0,379	0,488	0,566	0,391	0,496	0,504	0,541	0,567	0,508	0,544
Yemen	0,161	0,085	0,046	0,164	0,135	0,427	0,399	0,385	0,428	0,417
Zambia	0,340	0,348	0,551	0,377	0,409	0,491	0,494	0,562	0,504	0,515
Zimbabwe	0,223	0,216	0,339	0,157	0,210	0,449	0,447	0,490	0,425	0,445

* ОКК – Оцінка контролю корупції; ОЕУ – Оцінка ефективності уряду; ОПС – Оцінка політичної стабільності та відсутності насильства / тероризму; ОЯР – Оцінка якості регуляторів; ОВП – Оцінка верховенства права

Таблиця Б.2 – Розрахунки нормалізованих значень індикаторів цифрової спроможності національної економіки та кібербезпеки, а також їх значень, приведених до безрозмірної шкали бажаності Харрінгтона

Назва країни	Нормалізовані значення індикаторів цифрової спроможності національної економіки та кібербезпеки					Значення індикаторів цифрової спроможності національної економіки та кібербезпеки, приведені до безрозмірної шкали бажаності Харрінгтона				
	ГІК*	ІР ІКТ*	ІМГ*	РЦР*	НІК*	ГІК	ІР ІКТ	ІМГ	РЦР	НІК
Afghanistan	0,255	0,219	0,140	0,164	0,258	0,461	0,448	0,419	0,428	0,462
Albania	0,614	0,506	0,576	0,508	0,531	0,582	0,547	0,570	0,548	0,556
Algeria	0,310	0,464	0,482	0,419	0,278	0,480	0,533	0,539	0,518	0,469
Angola	0,206	0,212	0,140	0,163	0,238	0,443	0,445	0,419	0,428	0,455
Antigua and Barbuda	0,303	0,568	0,140	0,551	0,258	0,478	0,567	0,419	0,562	0,462
Argentina	0,428	0,675	0,557	0,599	0,595	0,521	0,601	0,564	0,577	0,576
Armenia	0,505	0,578	0,621	0,580	0,429	0,547	0,571	0,584	0,571	0,521
Australia	0,794	0,789	0,764	0,794	0,700	0,636	0,635	0,628	0,636	0,609
Austria	0,759	0,774	0,750	0,779	0,770	0,626	0,631	0,624	0,632	0,629
Azerbaijan	0,630	0,618	0,621	0,606	0,493	0,587	0,583	0,584	0,580	0,543
Bahamas	0,236	0,647	0,140	0,645	0,355	0,454	0,593	0,419	0,592	0,496
Bahrain	0,581	0,744	0,721	0,741	0,379	0,572	0,622	0,615	0,621	0,504
Bangladesh	0,530	0,257	0,491	0,307	0,404	0,555	0,461	0,542	0,479	0,513
Barbados	0,248	0,719	0,140	0,729	0,288	0,458	0,614	0,419	0,617	0,473
Belarus	0,572	0,744	0,140	0,751	0,643	0,569	0,622	0,419	0,624	0,591
Belgium	0,746	0,760	0,750	0,770	0,867	0,622	0,626	0,624	0,629	0,657
Belize	0,224	0,363	0,140	0,316	0,211	0,449	0,499	0,419	0,482	0,445
Benin	0,496	0,212	0,435	0,250	0,582	0,544	0,445	0,523	0,459	0,572
Bhutan	0,255	0,363	0,557	0,412	0,310	0,461	0,499	0,564	0,516	0,480

Продовження таблиці Б.2

Назва країни	Нормалізовані значення індикаторів цифрової спроможності національної економіки та кібербезпеки					Значення індикаторів цифрової спроможності національної економіки та кібербезпеки, приведені до безрозмірної шкали бажаності Харрінгтона				
	ГІК*	ІР ІКТ*	ІМГ*	РЦР*	НІК*	ГІК	ІР ІКТ	ІМГ	РЦР	НІК
Bolivia	0,230	0,423	0,491	0,406	0,404	0,452	0,519	0,542	0,514	0,513
Bosnia and Herzegovina	0,268	0,537	0,529	0,497	0,607	0,465	0,557	0,555	0,544	0,580
Botswana	0,454	0,454	0,519	0,440	0,344	0,530	0,530	0,552	0,525	0,492
Brazil	0,572	0,608	0,585	0,576	0,582	0,569	0,580	0,573	0,570	0,572
Brunei Darussalam	0,605	0,675	0,140	0,671	0,467	0,579	0,601	0,419	0,600	0,534
Bulgaria	0,683	0,685	0,603	0,628	0,631	0,604	0,604	0,579	0,586	0,588
Burundi	0,201	0,186	0,371	0,200	0,195	0,441	0,436	0,502	0,441	0,439
Cambodia	0,242	0,326	0,510	0,355	0,288	0,456	0,486	0,549	0,496	0,473
Cameroon	0,445	0,249	0,453	0,278	0,344	0,527	0,459	0,530	0,469	0,492
Canada	0,794	0,760	0,771	0,780	0,678	0,636	0,626	0,630	0,632	0,602
Chad	0,206	0,173	0,345	0,182	0,310	0,443	0,431	0,493	0,434	0,480
Chile	0,454	0,657	0,664	0,652	0,678	0,530	0,595	0,598	0,594	0,602
China	0,759	0,558	0,612	0,562	0,467	0,626	0,564	0,581	0,566	0,534
Colombia	0,564	0,537	0,603	0,539	0,582	0,566	0,557	0,579	0,558	0,572
Congo (Democratic Republic of the)	0,160	0,192	0,140	0,139	0,195	0,427	0,438	0,419	0,419	0,439
Costa Rica	0,281	0,638	0,647	0,636	0,643	0,470	0,590	0,592	0,589	0,591
Côte d'Ivoire	0,471	0,308	0,510	0,348	0,429	0,535	0,479	0,549	0,493	0,521
Croatia	0,765	0,711	0,621	0,665	0,855	0,628	0,612	0,584	0,598	0,654
Cuba	0,488	0,290	0,140	0,238	0,268	0,541	0,473	0,419	0,455	0,465
Cyprus	0,630	0,760	0,664	0,715	0,531	0,587	0,626	0,598	0,613	0,556
Czech Republic	0,564	0,711	0,673	0,691	0,894	0,566	0,612	0,600	0,606	0,664

Продовження таблиці Б.2

Назва країни	Нормалізовані значення індикаторів цифрової спроможності національної економіки та кібербезпеки					Значення індикаторів цифрової спроможності національної економіки та кібербезпеки, приведені до безрозмірної шкали бажаності Харрінгтона				
	ГІК*	ІР ІКТ*	ІМГ*	РЦР*	НІК*	ГІК	ІР ІКТ	ІМГ	РЦР	НІК
Denmark	0,771	0,821	0,771	0,817	0,849	0,630	0,644	0,630	0,643	0,652
Dominica	0,165	0,568	0,140	0,549	0,203	0,428	0,567	0,419	0,561	0,442
Dominican Republic	0,445	0,443	0,529	0,444	0,531	0,527	0,526	0,555	0,526	0,556
Ecuador	0,395	0,475	0,576	0,490	0,467	0,510	0,537	0,570	0,542	0,534
Egypt	0,765	0,454	0,548	0,460	0,467	0,628	0,530	0,561	0,532	0,534
El Salvador	0,218	0,373	0,548	0,411	0,321	0,447	0,502	0,561	0,515	0,484
Estonia	0,805	0,782	0,750	0,784	0,889	0,640	0,633	0,624	0,633	0,663
Ethiopia	0,325	0,198	0,463	0,250	0,442	0,485	0,440	0,533	0,459	0,526
Finland	0,777	0,767	0,808	0,808	0,849	0,631	0,629	0,640	0,640	0,652
France	0,810	0,789	0,743	0,782	0,855	0,641	0,635	0,621	0,633	0,654
Georgia	0,777	0,578	0,621	0,582	0,643	0,631	0,571	0,584	0,572	0,591
Germany	0,771	0,802	0,771	0,805	0,842	0,630	0,639	0,630	0,640	0,650
Ghana	0,454	0,403	0,519	0,408	0,429	0,530	0,512	0,552	0,514	0,521
Greece	0,530	0,711	0,603	0,649	0,908	0,555	0,612	0,579	0,593	0,668
Grenada	0,230	0,578	0,140	0,562	0,278	0,452	0,571	0,419	0,566	0,469
Guatemala	0,303	0,335	0,519	0,367	0,404	0,478	0,489	0,552	0,500	0,513
Guyana	0,224	0,335	0,529	0,381	0,220	0,449	0,489	0,555	0,505	0,448
Haiti	0,180	0,198	0,389	0,216	0,248	0,434	0,440	0,508	0,447	0,458
Honduras	0,175	0,326	0,548	0,380	0,248	0,432	0,486	0,561	0,505	0,458
Hungary	0,746	0,685	0,639	0,656	0,741	0,622	0,604	0,590	0,595	0,621
Iceland	0,462	0,839	0,764	0,822	0,582	0,533	0,649	0,628	0,644	0,572
India	0,683	0,299	0,557	0,373	0,700	0,604	0,476	0,564	0,502	0,609

Продовження таблиці Б.2

Назва країни	Нормалізовані значення індикаторів цифрової спроможності національної економіки та кібербезпеки					Значення індикаторів цифрової спроможності національної економіки та кібербезпеки, приведені до безрозмірної шкали бажаності Харрінгтона				
	ГІК*	ІР ІКТ*	ІМГ*	РЦР*	НІК*	ГІК	ІР ІКТ	ІМГ	РЦР	НІК
Indonesia	0,726	0,423	0,585	0,468	0,506	0,616	0,519	0,573	0,534	0,547
Iran (Islamic Republic of)	0,622	0,558	0,548	0,518	0,278	0,584	0,564	0,561	0,551	0,469
Ireland	0,726	0,774	0,743	0,773	0,731	0,616	0,631	0,621	0,630	0,618
Israel	0,726	0,767	0,750	0,773	0,741	0,616	0,629	0,624	0,630	0,621
Italy	0,765	0,693	0,639	0,662	0,820	0,628	0,607	0,590	0,597	0,644
Jamaica	0,428	0,475	0,576	0,490	0,404	0,521	0,537	0,570	0,542	0,513
Japan	0,789	0,802	0,771	0,807	0,721	0,635	0,639	0,630	0,640	0,615
Jordan	0,556	0,598	0,612	0,586	0,278	0,563	0,577	0,581	0,573	0,469
Kazakhstan	0,726	0,675	0,664	0,664	0,570	0,616	0,601	0,598	0,598	0,568
Kenya	0,705	0,290	0,557	0,367	0,467	0,610	0,473	0,564	0,500	0,534
Kiribati	0,170	0,234	0,140	0,179	0,211	0,430	0,453	0,419	0,433	0,445
Korea (Republic of)	0,783	0,833	0,771	0,822	0,721	0,633	0,648	0,630	0,644	0,615
Kyrgyzstan	0,303	0,433	0,548	0,444	0,321	0,478	0,523	0,561	0,527	0,484
Lao PDR	0,268	0,290	0,510	0,335	0,299	0,465	0,473	0,549	0,489	0,476
Latvia	0,705	0,719	0,689	0,704	0,788	0,610	0,614	0,605	0,610	0,635
Liberia	0,275	0,109	0,425	0,348	0,321	0,468	0,408	0,520	0,493	0,484
Libya	0,275	0,403	0,140	0,360	0,248	0,468	0,512	0,419	0,498	0,458
Lithuania	0,805	0,711	0,697	0,707	0,879	0,640	0,612	0,608	0,611	0,660
Luxembourg	0,794	0,809	0,777	0,814	0,721	0,636	0,641	0,632	0,642	0,615
Madagascar	0,268	0,198	0,398	0,220	0,268	0,465	0,440	0,511	0,448	0,465
Malawi	0,325	0,198	0,416	0,229	0,332	0,485	0,440	0,517	0,451	0,488

Продовження таблиці Б.2

Назва країни	Нормалізовані значення індикаторів цифрової спроможності національної економіки та кібербезпеки					Значення індикаторів цифрової спроможності національної економіки та кібербезпеки, приведені до безрозмірної шкали бажаності Харрінгтона				
	ГІК*	ІР ІКТ*	ІМГ*	РЦР*	НІК*	ГІК	ІР ІКТ	ІМГ	РЦР	НІК
Malaysia	0,794	0,638	0,697	0,665	0,796	0,636	0,590	0,608	0,598	0,637
Mali	0,201	0,234	0,435	0,260	0,321	0,441	0,453	0,523	0,463	0,484
Malta	0,488	0,767	0,689	0,733	0,619	0,541	0,629	0,605	0,619	0,584
Mauritania	0,212	0,241	0,389	0,239	0,258	0,445	0,456	0,508	0,455	0,462
Mauritius	0,789	0,588	0,639	0,596	0,595	0,635	0,574	0,590	0,576	0,576
Mexico	0,614	0,516	0,585	0,518	0,480	0,582	0,551	0,573	0,551	0,539
Moldova (Republic of)	0,638	0,647	0,585	0,596	0,619	0,589	0,593	0,573	0,576	0,584
Mongolia	0,479	0,495	0,621	0,532	0,258	0,538	0,544	0,584	0,556	0,462
Montenegro	0,622	0,638	0,621	0,620	0,454	0,584	0,590	0,584	0,584	0,530
Morocco	0,445	0,475	0,576	0,486	0,355	0,527	0,537	0,570	0,540	0,496
Mozambique	0,242	0,241	0,453	0,275	0,238	0,456	0,456	0,530	0,468	0,455
Myanmar	0,248	0,299	0,416	0,287	0,248	0,458	0,476	0,517	0,472	0,458
Namibia	0,190	0,383	0,529	0,407	0,258	0,437	0,506	0,555	0,514	0,462
Nepal	0,310	0,290	0,482	0,318	0,404	0,480	0,473	0,539	0,483	0,513
Netherlands	0,794	0,809	0,790	0,820	0,849	0,636	0,641	0,635	0,644	0,652
New Zealand	0,733	0,796	0,764	0,797	0,667	0,618	0,637	0,628	0,637	0,598
Nicaragua	0,224	0,326	0,425	0,308	0,344	0,449	0,486	0,520	0,480	0,492
Nigeria	0,630	0,265	0,482	0,303	0,655	0,587	0,464	0,539	0,478	0,595
North Macedonia	0,739	0,598	0,639	0,603	0,519	0,620	0,577	0,590	0,579	0,551
Norway	0,794	0,809	0,790	0,819	0,721	0,636	0,641	0,635	0,643	0,615
Oman	0,783	0,638	0,621	0,619	0,454	0,633	0,590	0,584	0,584	0,530
Pakistan	0,428	0,249	0,510	0,309	0,544	0,521	0,459	0,549	0,480	0,560

Продовження таблиці Б.2

Назва країни	Нормалізовані значення індикаторів цифрової спроможності національної економіки та кібербезпеки					Значення індикаторів цифрової спроможності національної економіки та кібербезпеки, приведені до безрозмірної шкали бажаності Харрінгтона				
	ГІК*	ІР ІКТ*	ІМГ*	РЦР*	НІК*	ГІК	ІР ІКТ	ІМГ	РЦР	НІК
Panama	0,395	0,485	0,621	0,529	0,595	0,510	0,540	0,584	0,555	0,576
Papua New Guinea	0,224	0,109	0,140	0,070	0,268	0,449	0,408	0,419	0,394	0,465
Paraguay	0,589	0,413	0,510	0,407	0,678	0,574	0,516	0,549	0,514	0,602
Peru	0,420	0,485	0,557	0,482	0,519	0,518	0,540	0,564	0,539	0,551
Philippines	0,622	0,464	0,585	0,488	0,442	0,584	0,533	0,573	0,541	0,526
Poland	0,752	0,685	0,647	0,661	0,779	0,624	0,604	0,592	0,597	0,632
Portugal	0,712	0,702	0,697	0,704	0,788	0,612	0,609	0,608	0,610	0,635
Qatar	0,777	0,711	0,728	0,729	0,667	0,631	0,612	0,617	0,617	0,598
Romania	0,564	0,647	0,603	0,606	0,788	0,566	0,593	0,579	0,580	0,635
Russian Federation	0,765	0,702	0,647	0,671	0,741	0,628	0,609	0,592	0,600	0,621
Rwanda	0,668	0,234	0,576	0,334	0,392	0,599	0,453	0,570	0,489	0,509
Saint Kitts and Nevis	0,190	0,711	0,140	0,722	0,248	0,437	0,612	0,419	0,615	0,458
Saint Lucia	0,206	0,454	0,140	0,420	0,238	0,443	0,530	0,419	0,518	0,455
Saint Vincent and the Grenadines	0,248	0,547	0,140	0,531	0,238	0,458	0,561	0,419	0,555	0,455
Samoa	0,395	0,326	0,140	0,275	0,211	0,510	0,486	0,419	0,468	0,445
Saudi Arabia	0,789	0,666	0,689	0,673	0,689	0,635	0,598	0,605	0,600	0,605
Senegal	0,347	0,273	0,510	0,321	0,288	0,493	0,467	0,549	0,484	0,473
Serbia	0,622	0,657	0,585	0,605	0,828	0,584	0,595	0,573	0,579	0,646
Seychelles	0,310	0,495	0,585	0,510	0,248	0,480	0,544	0,573	0,549	0,458
Sierra Leone	0,230	0,109	0,140	0,070	0,203	0,452	0,408	0,419	0,394	0,442
Singapore	0,800	0,782	0,808	0,814	0,842	0,638	0,633	0,640	0,642	0,650

Продовження таблиці Б.2

Назва країни	Нормалізовані значення індикаторів цифрової спроможності національної економіки та кібербезпеки					Значення індикаторів цифрової спроможності національної економіки та кібербезпеки, приведені до безрозмірної шкали бажаності Харрінгтона				
	ГІК*	ІР ІКТ*	ІМГ*	РЦР*	НІК*	ГІК	ІР ІКТ	ІМГ	РЦР	НІК
Slovakia	0,691	0,702	0,639	0,663	0,835	0,606	0,609	0,590	0,597	0,648
Slovenia	0,668	0,728	0,673	0,702	0,678	0,599	0,617	0,600	0,609	0,602
Solomon Islands	0,185	0,226	0,140	0,175	0,195	0,436	0,450	0,419	0,432	0,439
South Africa	0,630	0,495	0,612	0,523	0,392	0,587	0,544	0,581	0,553	0,509
South Sudan	0,190	0,109	0,140	0,070	0,187	0,437	0,408	0,419	0,394	0,436
Spain	0,800	0,760	0,689	0,730	0,879	0,638	0,626	0,605	0,618	0,660
Sudan	0,332	0,265	0,140	0,208	0,258	0,488	0,464	0,419	0,444	0,462
Suriname	0,212	0,516	0,140	0,483	0,321	0,445	0,551	0,419	0,540	0,484
Sweden	0,746	0,802	0,790	0,817	0,678	0,622	0,639	0,635	0,643	0,602
Switzerland	0,733	0,821	0,790	0,829	0,820	0,618	0,644	0,635	0,646	0,644
Syrian Arab Republic	0,295	0,326	0,140	0,279	0,288	0,475	0,486	0,419	0,469	0,473
Tajikistan	0,310	0,109	0,491	0,430	0,278	0,480	0,408	0,542	0,522	0,469
Tanzania, United Republic of	0,622	0,205	0,435	0,244	0,268	0,584	0,443	0,523	0,457	0,465
Thailand	0,739	0,568	0,612	0,566	0,544	0,620	0,567	0,581	0,567	0,560
Tonga	0,275	0,423	0,140	0,386	0,355	0,468	0,519	0,419	0,507	0,496
Trinidad and Tobago	0,261	0,598	0,603	0,580	0,332	0,463	0,577	0,579	0,571	0,488
Tunisia	0,539	0,475	0,576	0,489	0,429	0,558	0,537	0,570	0,541	0,521
Turkey	0,771	0,608	0,639	0,608	0,655	0,630	0,580	0,590	0,580	0,595
Turkmenistan	0,218	0,109	0,140	0,070	0,203	0,447	0,408	0,419	0,394	0,442
Tuvalu	0,185	0,109	0,140	0,070	0,195	0,436	0,408	0,419	0,394	0,439
Uganda	0,605	0,234	0,463	0,275	0,619	0,579	0,453	0,533	0,468	0,584

Продовження таблиці Б.2

Назва країни	Нормалізовані значення індикаторів цифрової спроможності національної економіки та кібербезпеки					Значення індикаторів цифрової спроможності національної економіки та кібербезпеки, приведені до безрозмірної шкали бажаності Харрінгтона				
	ГІК*	ІР ІКТ*	ІМГ*	РЦР*	НІК*	ГІК	ІР ІКТ	ІМГ	РЦР	НІК
Ukraine	0,638	0,558	0,612	0,563	0,731	0,589	0,564	0,581	0,566	0,618
United Arab Emirates	0,746	0,711	0,743	0,736	0,519	0,622	0,612	0,621	0,619	0,551
United Kingdom	0,816	0,821	0,777	0,820	0,828	0,643	0,644	0,632	0,644	0,646
United States	0,816	0,789	0,790	0,808	0,835	0,643	0,635	0,635	0,640	0,648
Uruguay	0,653	0,711	0,647	0,676	0,595	0,594	0,612	0,592	0,601	0,576
Uzbekistan	0,645	0,485	0,140	0,453	0,429	0,592	0,540	0,419	0,529	0,521
Vanuatu	0,206	0,282	0,140	0,230	0,248	0,443	0,470	0,419	0,452	0,458
Venezuela	0,379	0,516	0,510	0,467	0,442	0,504	0,551	0,549	0,534	0,526
Vietnam	0,661	0,433	0,576	0,465	0,454	0,597	0,523	0,570	0,534	0,530
Yemen	0,160	0,109	0,140	0,070	0,229	0,427	0,408	0,419	0,394	0,451
Zambia	0,454	0,257	0,482	0,300	0,531	0,530	0,461	0,539	0,477	0,556
Zimbabwe	0,261	0,290	0,453	0,305	0,288	0,463	0,473	0,530	0,479	0,473

** ГІК – Глобальний індекс кібербезпеки; ІР ІКТ – Індексом розвитку інформаційних та комунікаційних технологій; ІМГ – Індекс мережевої готовності; РЦР – Рівень цифрового розвитку; НІК – Національний індекс кібербезпеки*

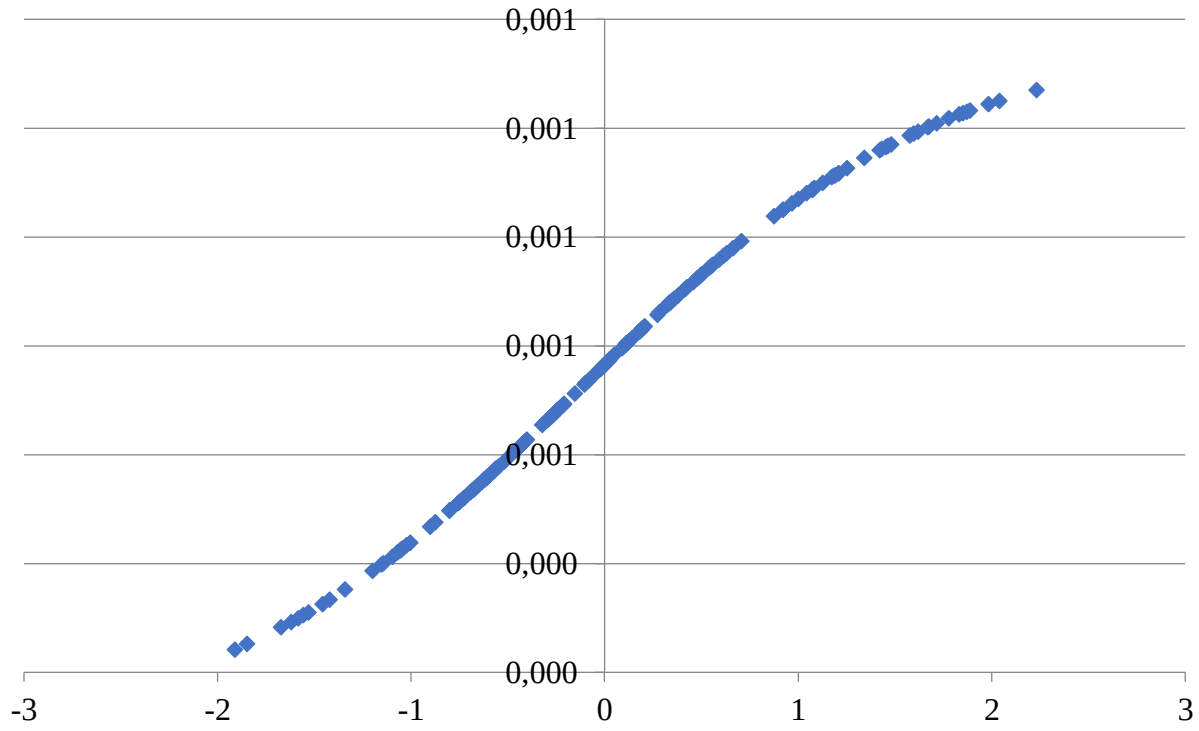


Рисунок Б.1 – Графік кривої першого типу для індикатора «Оцінка ефективності уряду (складено авторкою)

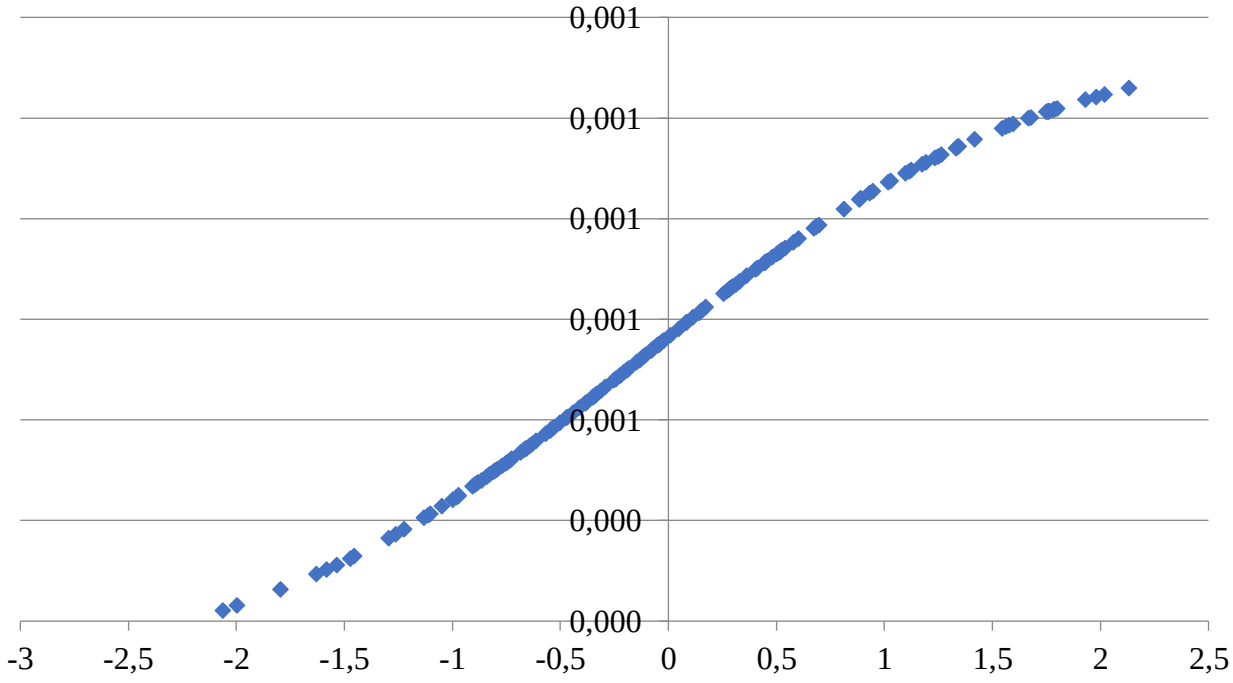


Рисунок Б.2 – Графік кривої першого типу для індикатора «Оцінка якості регуляторів» (складено авторкою)

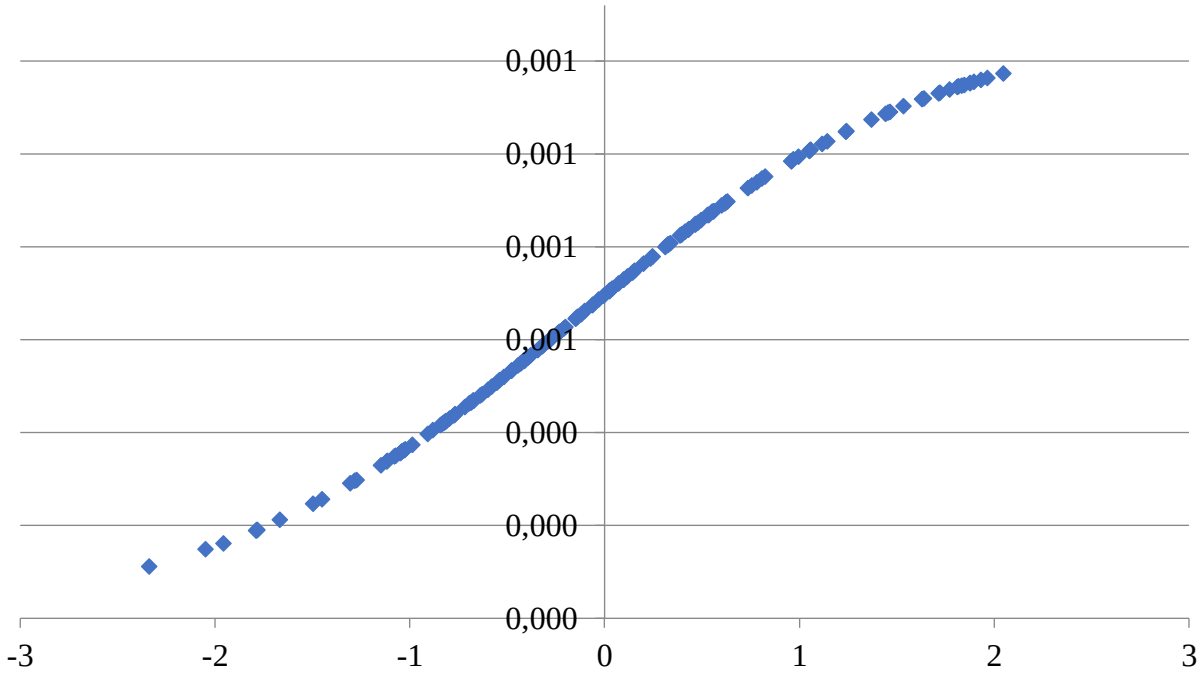


Рисунок Б.3 – Графік кривої першого типу для індикатора «Оцінка верховенства права» (складено авторкою)

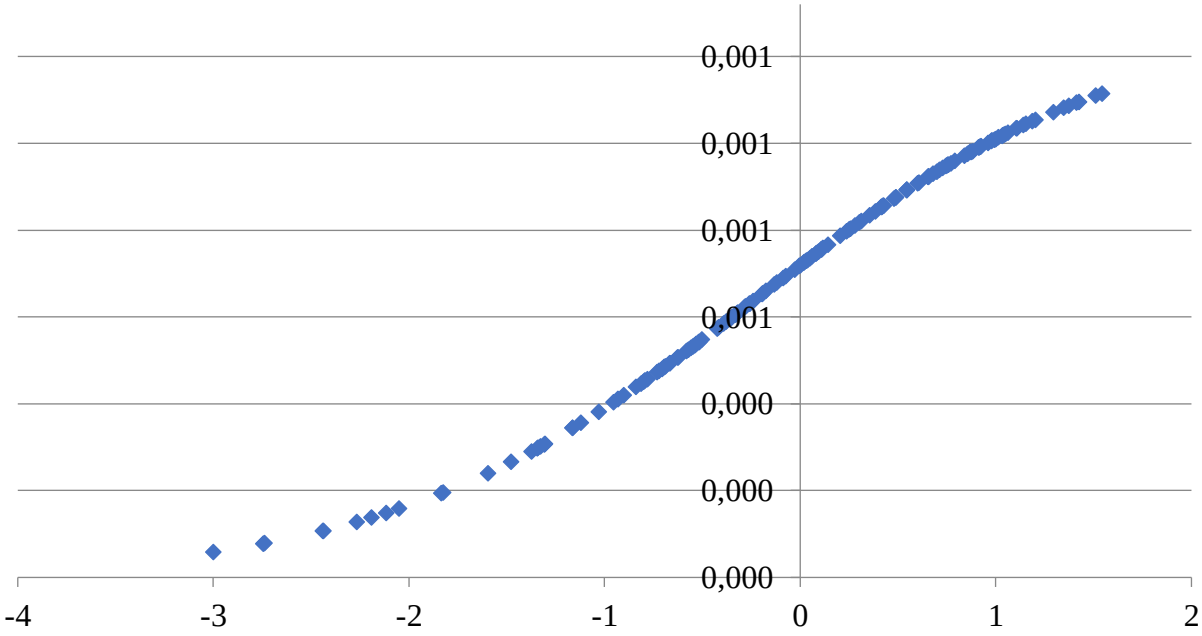


Рисунок Б.4 – Графік кривої першого типу для індикатора «Оцінка політичної стабільності та відсутності насилля / тероризму (складено авторкою)

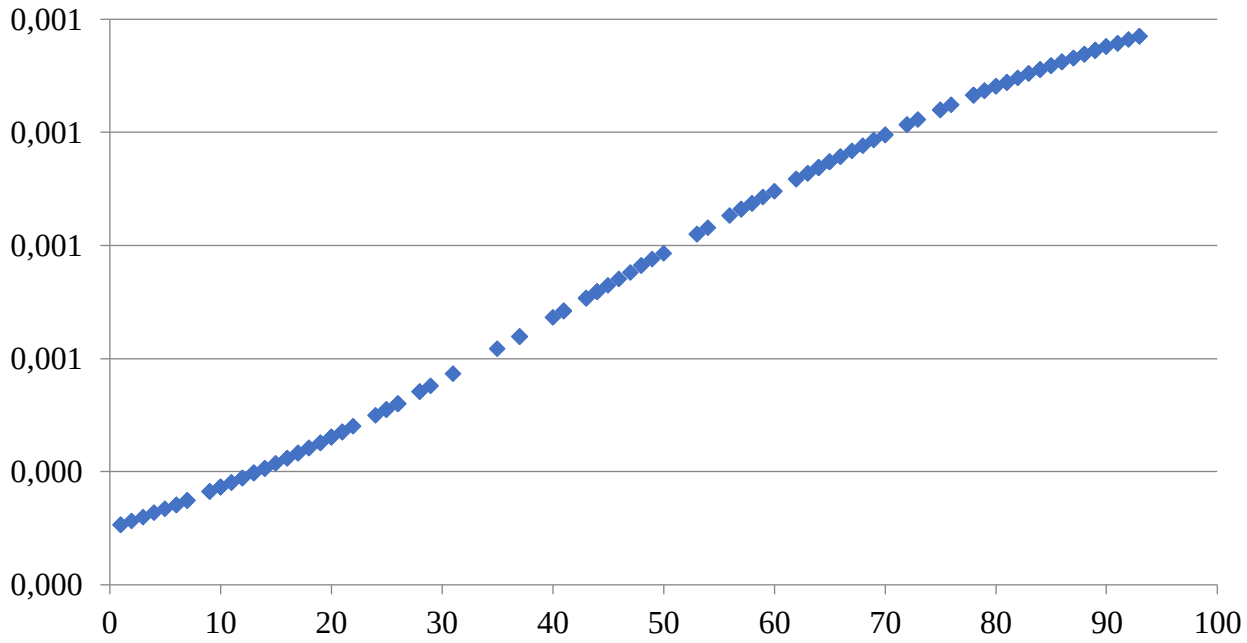


Рисунок Б.5 – Графік кривої першого типу для індикатора «Глобальний індекс кібербезпеки» (складено авторкою)

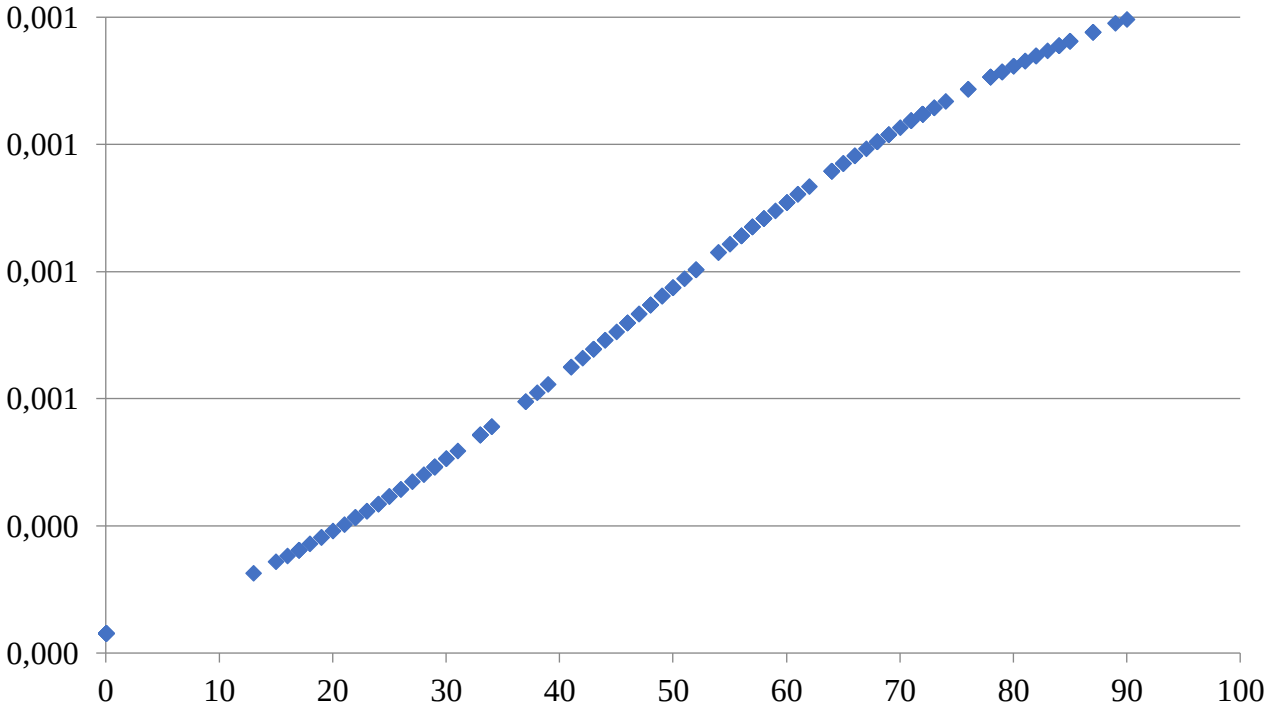


Рисунок Б.6 – Графік кривої першого типу для індикатора «Індекс розвитку ІКТ» (складено авторкою)

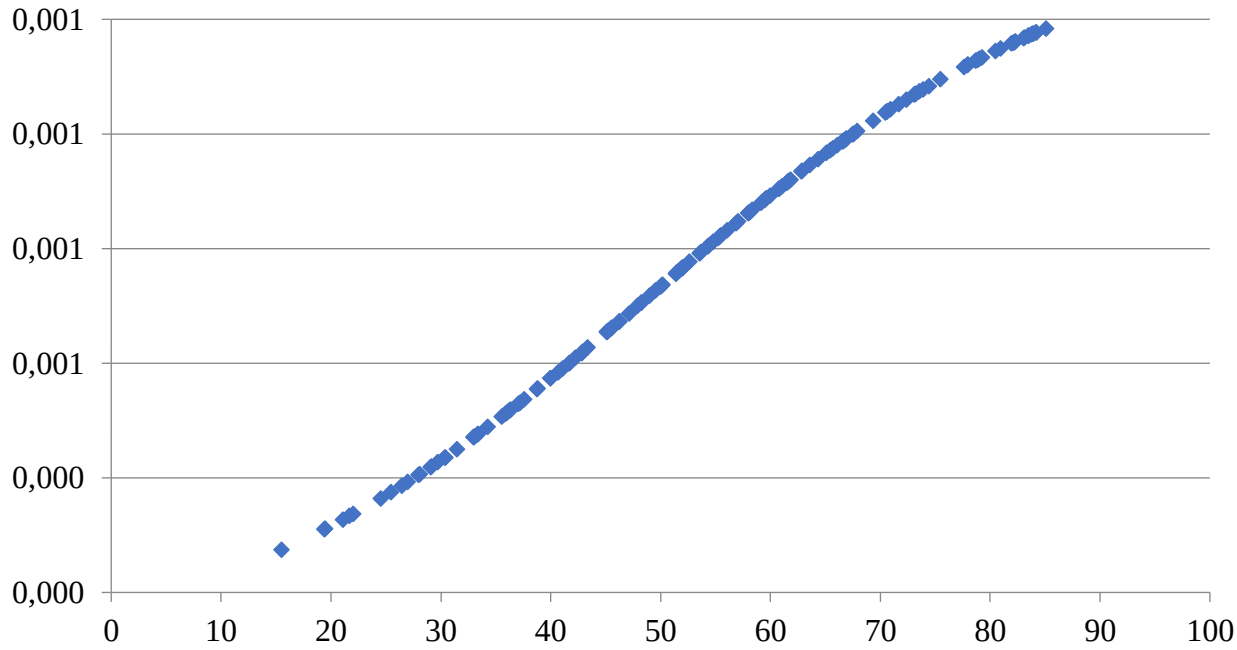


Рисунок Б.7 – Графік кривої першого типу для індикатора «Рівень цифрового розвитку» (складено авторкою)

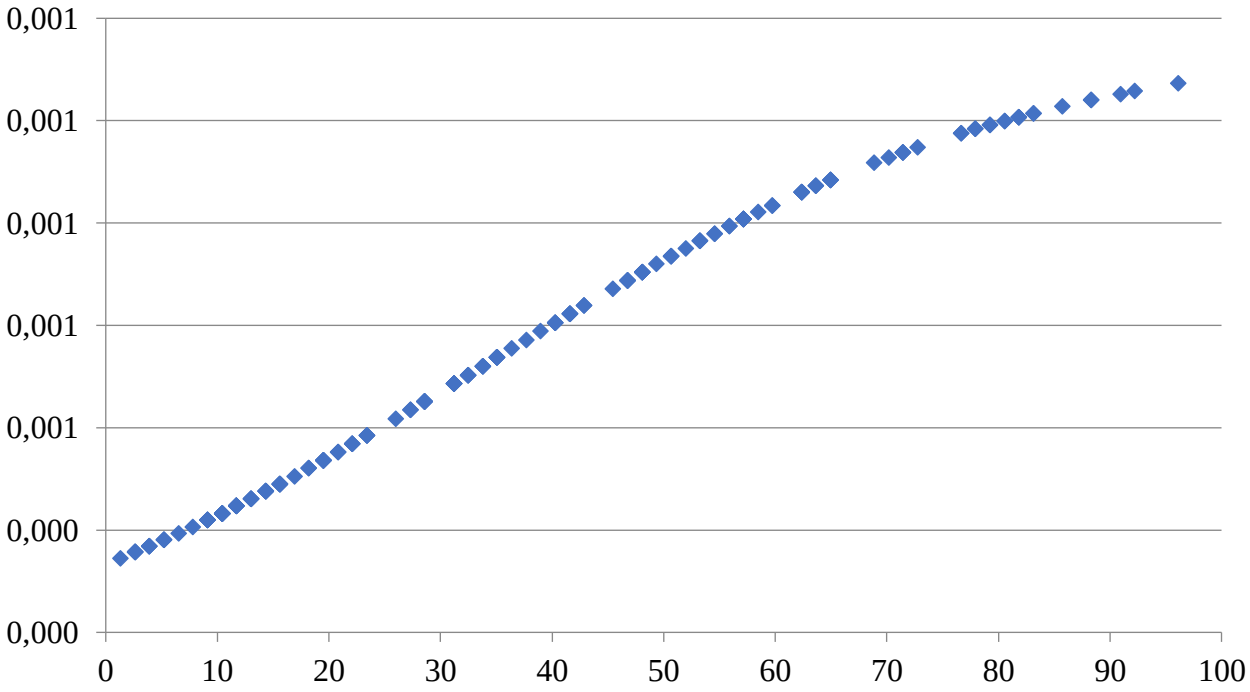


Рисунок Б.8 – Графік кривої другого типу для індикатора «Національний індекс кібербезпеки» (складено авторкою)

Таблиця Б.3 – Розрахунки значень перетворення Харрінгтона-Менчера та визначення інтегрального показника інформаційної безпеки національної економіки

Назва країни	ОКК	ОЕУ	ОПС	ОЯР	ОВП	ГІК	ІР ІКТ	ІМГ	РЦР	НІК	$IIBNE_i$
Afghanistan	0,001	0,002	0,001	0,005	0,001	0,003	0,003	0,001	0,002	0,963	0,011
Albania	0,043	0,611	0,934	0,751	0,182	0,915	0,633	0,998	0,723	0,996	0,652
Algeria	0,023	0,133	0,098	0,003	0,033	0,012	0,458	0,997	0,374	0,973	0,185
Angola	0,002	0,008	0,463	0,009	0,009	0,001	0,002	0,001	0,002	0,947	0,018
Antigua and Barbuda	0,668	0,496	0,983	0,831	0,844	0,010	0,830	0,001	0,840	0,963	0,262
Argentina	0,304	0,527	0,770	0,270	0,305	0,227	0,971	0,998	0,921	0,997	0,637
Armenia	0,105	0,478	0,364	0,742	0,391	0,579	0,853	0,998	0,894	0,993	0,685
Australia	0,998	0,996	0,994	0,999	0,998	0,998	0,997	0,999	0,998	0,998	0,998
Austria	0,996	0,994	0,992	0,996	0,999	0,996	0,996	0,999	0,997	0,999	0,997
Azerbaijan	0,008	0,403	0,145	0,166	0,076	0,937	0,921	0,998	0,929	0,995	0,488
Bahamas	0,981	0,884	0,990	0,647	0,634	0,002	0,952	0,001	0,963	0,988	0,232
Bahrain	0,245	0,668	0,080	0,849	0,853	0,851	0,992	0,999	0,994	0,990	0,788
Bangladesh	0,005	0,034	0,033	0,022	0,063	0,689	0,008	0,997	0,058	0,992	0,146
Barbados	0,993	0,835	0,992	0,889	0,845	0,002	0,988	0,001	0,992	0,976	0,249
Belarus	0,207	0,225	0,927	0,049	0,025	0,830	0,992	0,001	0,995	0,998	0,246
Belgium	0,995	0,986	0,942	0,990	0,994	0,995	0,995	0,999	0,997	0,999	0,994
Belize	0,253	0,070	0,767	0,049	0,026	0,001	0,104	0,001	0,071	0,890	0,072
Benin	0,089	0,079	0,646	0,194	0,053	0,539	0,002	0,996	0,015	0,997	0,179
Bhutan	0,996	0,797	0,996	0,198	0,908	0,003	0,104	0,998	0,344	0,982	0,342
Bolivia	0,024	0,209	0,540	0,016	0,006	0,001	0,285	0,997	0,322	0,992	0,156
Bosnia and Herzegovina	0,033	0,062	0,390	0,302	0,311	0,004	0,744	0,998	0,686	0,997	0,295
Botswana	0,927	0,781	0,994	0,853	0,877	0,335	0,413	0,997	0,461	0,987	0,727

Продовження таблиці Б.3

Назва країни	ОКК	ОЕУ	ОПС	ОЯР	ОВП	ГІК	ІР ІКТ	ІМГ	РЦР	НІК	$IIBNE_i$
Brazil	0,074	0,131	0,425	0,213	0,272	0,830	0,908	0,998	0,888	0,997	0,571
Brunei Darussalam	0,938	0,989	0,997	0,932	0,930	0,902	0,971	0,001	0,977	0,995	0,463
Bulgaria	0,241	0,739	0,943	0,901	0,512	0,979	0,975	0,998	0,950	0,998	0,850
Burundi	0,001	0,002	0,003	0,010	0,002	0,001	0,001	0,994	0,004	0,740	0,024
Cambodia	0,001	0,078	0,826	0,100	0,006	0,002	0,045	0,997	0,152	0,976	0,112
Cameroon	0,002	0,027	0,007	0,025	0,008	0,297	0,006	0,996	0,030	0,987	0,096
Canada	0,998	0,997	0,994	0,997	0,998	0,998	0,995	0,999	0,997	0,998	0,998
Chad	0,001	0,002	0,005	0,006	0,003	0,001	0,001	0,993	0,003	0,982	0,023
Chile	0,971	0,981	0,944	0,993	0,987	0,335	0,959	0,999	0,967	0,998	0,884
China	0,149	0,859	0,522	0,369	0,341	0,996	0,805	0,998	0,862	0,995	0,729
Colombia	0,131	0,418	0,090	0,782	0,172	0,807	0,744	0,998	0,811	0,997	0,631
Congo (Democratic Republic of the)	0,001	0,001	0,001	0,002	0,001	0,001	0,002	0,001	0,001	0,740	0,008
Costa Rica	0,856	0,808	0,956	0,864	0,882	0,005	0,943	0,998	0,957	0,998	0,561
Côte d'Ivoire	0,049	0,077	0,053	0,316	0,083	0,415	0,029	0,997	0,132	0,993	0,261
Croatia	0,527	0,849	0,986	0,849	0,806	0,997	0,985	0,998	0,974	0,999	0,925
Cuba	0,562	0,270	0,977	0,002	0,149	0,498	0,018	0,001	0,011	0,969	0,094
Cyprus	0,893	0,968	0,965	0,979	0,955	0,937	0,995	0,999	0,990	0,996	0,977
Czech Republic	0,831	0,968	0,995	0,991	0,984	0,807	0,985	0,999	0,984	0,999	0,961
Denmark	0,999	0,998	0,993	0,997	0,999	0,997	0,999	0,999	0,999	0,999	0,999
Dominica	0,853	0,234	0,996	0,583	0,927	0,001	0,830	0,001	0,834	0,843	0,184
Dominican Republic	0,012	0,157	0,780	0,426	0,180	0,297	0,369	0,998	0,477	0,996	0,424
Ecuador	0,034	0,257	0,697	0,016	0,066	0,119	0,503	0,998	0,660	0,995	0,336
Egypt	0,030	0,073	0,018	0,018	0,169	0,997	0,413	0,998	0,543	0,995	0,338
El Salvador	0,029	0,131	0,447	0,464	0,026	0,001	0,126	0,998	0,342	0,984	0,191

Продовження таблиці Б.3

Назва країни	ОКК	ОЕУ	ОПС	ОЯР	ОВП	ГІК	ІР ІКТ	ІМГ	РЦР	НІК	$IIBNE_i$
Estonia	0,994	0,987	0,972	0,996	0,992	0,999	0,997	0,999	0,998	0,999	0,996
Ethiopia	0,052	0,066	0,008	0,011	0,159	0,019	0,002	0,997	0,015	0,994	0,088
Finland	0,999	0,999	0,992	0,998	0,999	0,998	0,995	0,999	0,999	0,999	0,998
France	0,990	0,995	0,827	0,987	0,996	0,999	0,997	0,999	0,997	0,999	0,990
Georgia	0,915	0,910	0,356	0,985	0,808	0,998	0,853	0,998	0,897	0,998	0,914
Germany	0,998	0,996	0,972	0,998	0,997	0,997	0,998	0,999	0,998	0,999	0,997
Ghana	0,274	0,300	0,777	0,423	0,611	0,335	0,212	0,997	0,328	0,993	0,527
Greece	0,321	0,784	0,817	0,760	0,683	0,689	0,985	0,998	0,965	0,999	0,840
Grenada	0,750	0,264	0,994	0,229	0,798	0,001	0,853	0,001	0,862	0,973	0,189
Guatemala	0,008	0,046	0,253	0,312	0,009	0,010	0,056	0,997	0,186	0,992	0,159
Guyana	0,180	0,250	0,607	0,089	0,236	0,001	0,056	0,998	0,228	0,917	0,203
Haiti	0,001	0,001	0,189	0,004	0,010	0,001	0,002	0,995	0,006	0,956	0,029
Honduras	0,025	0,062	0,245	0,117	0,010	0,001	0,045	0,998	0,225	0,956	0,123
Hungary	0,445	0,863	0,985	0,910	0,909	0,995	0,975	0,998	0,969	0,998	0,926
Iceland	0,998	0,994	0,999	0,994	0,998	0,374	0,999	0,999	0,999	0,997	0,905
India	0,212	0,747	0,047	0,323	0,567	0,979	0,023	0,998	0,205	0,998	0,419
Indonesia	0,163	0,668	0,260	0,432	0,240	0,992	0,285	0,998	0,574	0,996	0,601
Iran (Islamic Republic of)	0,004	0,140	0,010	0,003	0,049	0,927	0,805	0,998	0,752	0,973	0,275
Ireland	0,995	0,994	0,995	0,997	0,996	0,992	0,996	0,999	0,997	0,998	0,997
Israel	0,936	0,988	0,053	0,990	0,981	0,992	0,995	0,999	0,997	0,998	0,895
Italy	0,631	0,828	0,915	0,929	0,756	0,997	0,979	0,998	0,972	0,999	0,931
Jamaica	0,230	0,867	0,956	0,749	0,309	0,227	0,503	0,998	0,660	0,992	0,640
Japan	0,993	0,997	0,995	0,992	0,997	0,998	0,998	0,999	0,999	0,998	0,998
Jordan	0,546	0,609	0,403	0,584	0,746	0,781	0,892	0,998	0,903	0,973	0,811
Kazakhstan	0,048	0,523	0,756	0,637	0,157	0,992	0,971	0,999	0,973	0,997	0,683
Kenya	0,007	0,151	0,018	0,284	0,170	0,987	0,018	0,998	0,184	0,995	0,264

Продовження таблиці Б.3

Назва країни	ОКК	ОЕУ	ОПС	ОЯР	ОВП	ГІК	ІР ІКТ	ІМГ	РЦР	НІК	$IIBNE_i$
Kiribati	0,719	0,244	0,995	0,029	0,888	0,001	0,004	0,001	0,003	0,890	0,049
Korea (Republic of)	0,879	0,987	0,965	0,984	0,992	0,998	0,999	0,999	0,999	0,998	0,988
Kyrgyzstan	0,004	0,064	0,221	0,187	0,017	0,010	0,326	0,998	0,478	0,984	0,205
Lao PDR	0,003	0,048	0,942	0,026	0,024	0,004	0,018	0,997	0,104	0,979	0,108
Latvia	0,713	0,979	0,944	0,988	0,978	0,987	0,988	0,999	0,987	0,999	0,971
Liberia	0,007	0,003	0,590	0,011	0,012	0,004	0,001	0,996	0,133	0,984	0,059
Libya	0,001	0,001	0,001	0,001	0,001	0,004	0,212	0,001	0,164	0,956	0,023
Lithuania	0,828	0,981	0,985	0,985	0,978	0,999	0,985	0,999	0,988	0,999	0,982
Luxembourg	0,999	0,998	0,998	0,998	0,998	0,998	0,998	0,999	0,999	0,998	0,999
Madagascar	0,003	0,005	0,272	0,034	0,027	0,004	0,002	0,995	0,007	0,969	0,054
Malawi	0,012	0,037	0,457	0,047	0,191	0,019	0,002	0,996	0,009	0,986	0,096
Malaysia	0,701	0,981	0,888	0,931	0,928	0,998	0,943	0,999	0,974	0,999	0,957
Mali	0,016	0,010	0,001	0,082	0,029	0,001	0,004	0,996	0,019	0,984	0,057
Malta	0,869	0,973	0,998	0,993	0,984	0,498	0,995	0,999	0,993	0,998	0,920
Mauritania	0,009	0,038	0,162	0,024	0,051	0,001	0,005	0,995	0,011	0,963	0,067
Mauritius	0,662	0,963	0,990	0,979	0,959	0,998	0,874	0,998	0,917	0,997	0,948
Mexico	0,006	0,352	0,229	0,646	0,054	0,915	0,673	0,998	0,754	0,995	0,497
Moldova (Republic of)	0,014	0,121	0,433	0,454	0,168	0,946	0,952	0,998	0,916	0,998	0,541
Mongolia	0,071	0,280	0,987	0,473	0,281	0,456	0,591	0,998	0,793	0,963	0,586
Montenegro	0,412	0,625	0,826	0,804	0,636	0,927	0,943	0,998	0,943	0,994	0,856
Morocco	0,188	0,301	0,450	0,270	0,403	0,297	0,503	0,998	0,645	0,988	0,550
Mozambique	0,010	0,019	0,102	0,036	0,009	0,002	0,005	0,996	0,028	0,947	0,068
Myanmar	0,030	0,008	0,010	0,031	0,009	0,002	0,023	0,996	0,037	0,956	0,075
Namibia	0,722	0,603	0,977	0,451	0,754	0,001	0,151	0,998	0,324	0,963	0,314
Nepal	0,018	0,016	0,190	0,032	0,130	0,012	0,018	0,997	0,074	0,992	0,127

Продовження таблиці Б.3

Назва країни	ОКК	ОЕУ	ОПС	ОЯР	ОВП	ГІК	ІР ІКТ	ІМГ	РЦР	НІК	$IIBNE_i$
Netherlands	0,999	0,998	0,990	0,999	0,998	0,998	0,998	0,999	0,999	0,999	0,999
New Zealand	0,999	0,997	0,999	0,999	0,999	0,993	0,998	0,999	0,998	0,998	0,998
Nicaragua	0,002	0,026	0,094	0,043	0,009	0,001	0,045	0,996	0,060	0,987	0,085
Nigeria	0,003	0,009	0,001	0,017	0,019	0,937	0,010	0,997	0,054	0,998	0,107
North Macedonia	0,097	0,588	0,586	0,883	0,266	0,994	0,892	0,998	0,926	0,996	0,742
Norway	0,999	0,998	0,997	0,998	0,999	0,998	0,998	0,999	0,999	0,998	0,999
Oman	0,641	0,673	0,977	0,770	0,877	0,998	0,943	0,998	0,943	0,994	0,909
Pakistan	0,009	0,058	0,001	0,053	0,054	0,227	0,006	0,997	0,061	0,997	0,129
Panama	0,033	0,482	0,903	0,826	0,483	0,119	0,548	0,998	0,785	0,997	0,546
Papua New Guinea	0,006	0,047	0,163	0,084	0,034	0,001	0,001	0,001	0,001	0,969	0,021
Paraguay	0,007	0,098	0,658	0,379	0,099	0,870	0,247	0,997	0,326	0,998	0,388
Peru	0,039	0,270	0,524	0,880	0,110	0,196	0,548	0,998	0,630	0,996	0,488
Philippines	0,038	0,550	0,022	0,548	0,130	0,927	0,458	0,998	0,654	0,994	0,518
Poland	0,893	0,923	0,965	0,966	0,861	0,995	0,975	0,998	0,972	0,999	0,969
Portugal	0,949	0,988	0,996	0,967	0,988	0,989	0,982	0,999	0,987	0,999	0,988
Qatar	0,920	0,914	0,979	0,879	0,951	0,998	0,985	0,999	0,992	0,998	0,973
Romania	0,268	0,263	0,796	0,848	0,807	0,807	0,952	0,998	0,929	0,999	0,785
Russian Federation	0,007	0,442	0,285	0,085	0,027	0,997	0,982	0,998	0,977	0,998	0,457
Rwanda	0,868	0,690	0,830	0,585	0,653	0,971	0,004	0,998	0,102	0,991	0,412
Saint Kitts and Nevis	0,802	0,889	0,982	0,877	0,902	0,001	0,985	0,001	0,991	0,956	0,222
Saint Lucia	0,848	0,681	0,994	0,755	0,910	0,001	0,413	0,001	0,379	0,947	0,184
Saint Vincent and the Grenadines	0,932	0,681	0,990	0,732	0,863	0,002	0,776	0,001	0,789	0,947	0,230
Samoa	0,894	0,902	0,997	0,389	0,965	0,119	0,045	0,001	0,027	0,890	0,179
Saudi Arabia	0,737	0,775	0,273	0,457	0,673	0,998	0,966	0,999	0,977	0,998	0,845
Senegal	0,363	0,251	0,685	0,396	0,335	0,037	0,012	0,997	0,079	0,976	0,262

Продовження таблиці Б.3

Назва країни	ОКК	ОЕУ	ОПС	ОЯР	ОВП	ГІК	ІР ІКТ	ІМГ	РЦР	НІК	$IIBNE_i$
Serbia	0,095	0,608	0,811	0,510	0,395	0,927	0,959	0,998	0,928	0,999	0,740
Seychelles	0,914	0,869	0,981	0,356	0,721	0,012	0,591	0,998	0,729	0,956	0,528
Sierra Leone	0,050	0,006	0,733	0,015	0,034	0,001	0,001	0,001	0,001	0,843	0,019
Singapore	0,999	0,999	0,999	0,999	0,999	0,999	0,997	0,999	0,999	0,999	0,999
Slovakia	0,740	0,934	0,984	0,956	0,901	0,982	0,982	0,998	0,973	0,999	0,962
Slovenia	0,952	0,984	0,992	0,934	0,985	0,971	0,989	0,999	0,987	0,998	0,984
Solomon Islands	0,383	0,008	0,911	0,020	0,316	0,001	0,004	0,001	0,002	0,740	0,032
South Africa	0,366	0,785	0,506	0,665	0,439	0,937	0,591	0,998	0,769	0,991	0,768
South Sudan	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,003
Spain	0,883	0,976	0,895	0,973	0,979	0,999	0,995	0,999	0,992	0,999	0,982
Sudan	0,001	0,001	0,002	0,001	0,006	0,024	0,010	0,001	0,005	0,963	0,018
Suriname	0,192	0,053	0,808	0,056	0,478	0,001	0,673	0,001	0,635	0,984	0,123
Sweden	0,999	0,998	0,992	0,998	0,999	0,995	0,998	0,999	0,999	0,998	0,998
Switzerland	0,999	0,999	0,998	0,998	0,999	0,993	0,999	0,999	0,999	0,999	0,998
Syrian Arab Republic	0,001	0,001	0,001	0,001	0,001	0,008	0,045	0,001	0,030	0,976	0,018
Tajikistan	0,001	0,007	0,130	0,008	0,003	0,012	0,001	0,997	0,420	0,973	0,060
Tanzania, United Republic of	0,064	0,033	0,239	0,061	0,093	0,927	0,002	0,996	0,013	0,969	0,154
Thailand	0,082	0,791	0,125	0,611	0,565	0,994	0,830	0,998	0,870	0,997	0,716
Tonga	0,316	0,633	0,991	0,186	0,841	0,004	0,285	0,001	0,247	0,988	0,169
Trinidad and Tobago	0,122	0,676	0,893	0,482	0,421	0,003	0,892	0,998	0,894	0,986	0,423
Tunisia	0,333	0,398	0,061	0,148	0,580	0,722	0,503	0,998	0,656	0,993	0,580
Turkey	0,112	0,507	0,009	0,456	0,237	0,997	0,908	0,998	0,931	0,998	0,606
Turkmenistan	0,001	0,008	0,750	0,001	0,002	0,001	0,001	0,001	0,001	0,843	0,010
Tuvalu	0,418	0,044	0,999	0,075	0,901	0,001	0,001	0,001	0,001	0,740	0,032

Продовження таблиці Б.3

Назва країни	ОКК	ОЕУ	ОПС	ОЯР	ОВП	ГІК	ІР ІКТ	ІМГ	РЦР	НІК	$IIBNE_i$
Uganda	0,003	0,066	0,148	0,263	0,257	0,902	0,004	0,997	0,028	0,998	0,183
Ukraine	0,006	0,148	0,002	0,290	0,043	0,946	0,805	0,998	0,865	0,998	0,377
United Arab Emirates	0,982	0,994	0,984	0,971	0,962	0,995	0,985	0,999	0,993	0,996	0,990
United Kingdom	0,998	0,992	0,789	0,998	0,998	0,999	0,999	0,999	0,999	0,999	0,990
United States	0,990	0,996	0,955	0,996	0,996	0,999	0,997	0,999	0,999	0,999	0,996
Uruguay	0,988	0,891	0,995	0,873	0,922	0,960	0,985	0,998	0,979	0,997	0,968
Uzbekistan	0,002	0,086	0,499	0,006	0,008	0,953	0,548	0,001	0,514	0,993	0,125
Vanuatu	0,231	0,109	0,989	0,114	0,813	0,001	0,015	0,001	0,009	0,956	0,063
Venezuela	0,001	0,001	0,008	0,001	0,001	0,082	0,673	0,997	0,571	0,994	0,091
Vietnam	0,052	0,498	0,874	0,163	0,539	0,966	0,326	0,998	0,564	0,994	0,568
Yemen	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,935	0,006
Zambia	0,020	0,081	0,845	0,130	0,217	0,335	0,008	0,997	0,050	0,996	0,212
Zimbabwe	0,001	0,004	0,139	0,001	0,003	0,003	0,018	0,996	0,056	0,976	0,052

Додаток В

Результати кластерного аналізу за методом карт Кохонена

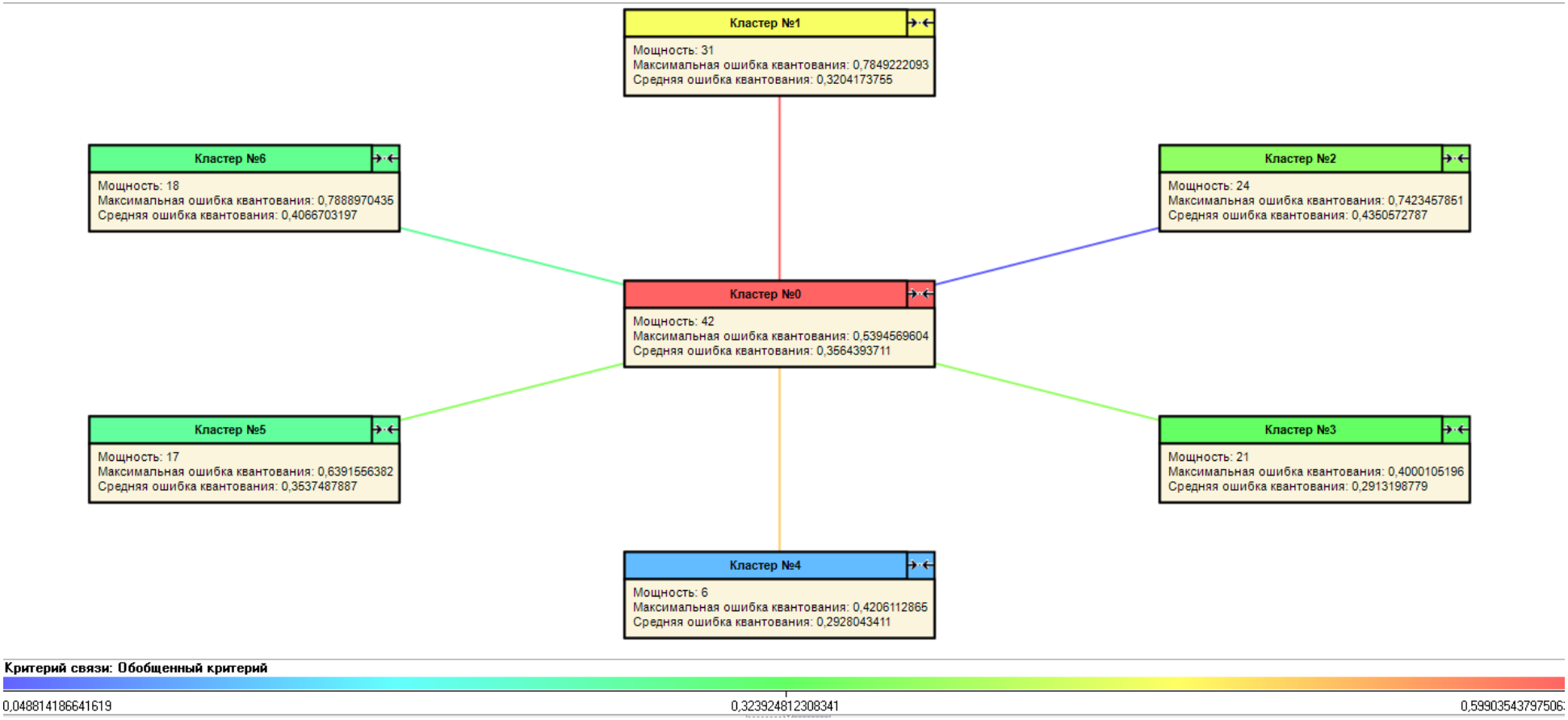


Рисунок В.1 – Зв’язки кластерів (складено авторкою)

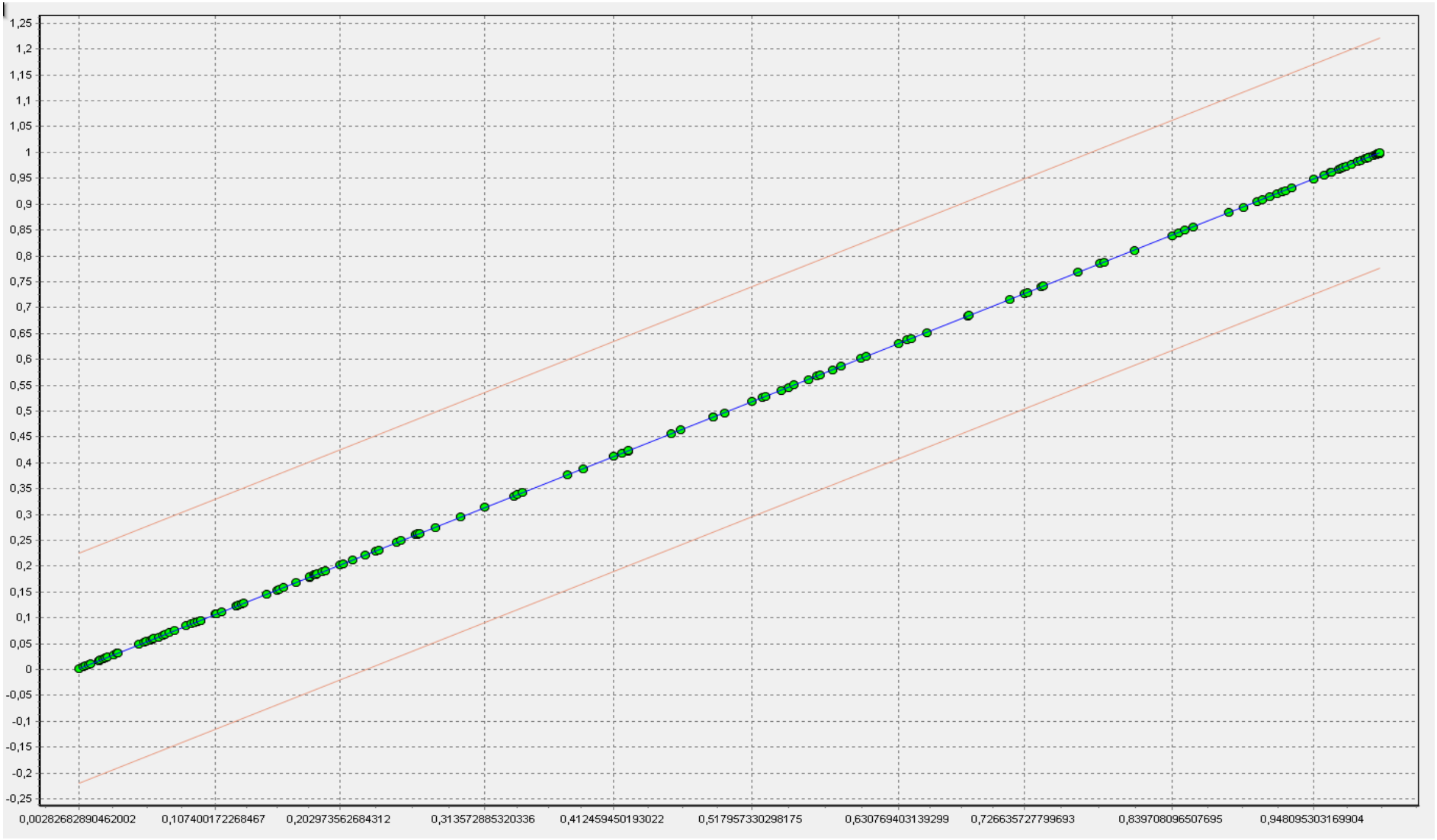


Рисунок В.2 – Діаграма розсіювання (складено авторкою)

Поля	Показатели	0 (42 (26,4%))	1 (31 (19,5%))	2 (24 (15,1%))	3 (21 (13,2%))	6 (18 (11,3%))	5 (17 (10,7%))	4 (6 (3,8%))	Итого
9.0 Оцінка верховенства права	Значимость	100,0%	94,6%	100,0%	98,9%	74,3%	97,8%	50,4%	100,0%
9.0 Оцінка якості регуляторів	Значимость	100,0%	18,6%	100,0%	92,7%	66,4%	98,9%	13,3%	100,0%
9.0 Оцінка політичної стабільності та відсутності	Значимость	100,0%	97,9%	100,0%	38,3%	100,0%	99,9%	95,1%	100,0%
9.0 Оцінка ефективності уряду	Значимость	100,0%	4,0%	100,0%	96,6%	27,4%	98,3%	57,9%	100,0%
9.0 Оцінка контролю корупції	Значимость	100,0%	99,3%	100,0%	99,2%	88,7%	99,3%	87,7%	100,0%
9.0 Національний індекс кібербезпеки	Значимость	100,0%	95,8%	100,0%	98,2%	100,0%	21,6%	83,1%	100,0%
9.0 Рівень цифрового розвитку	Значимость	100,0%	100,0%	100,0%	86,9%	85,8%	99,4%	13,4%	100,0%
9.0 Індекс мережевої готовності країни	Значимость	100,0%	99,9%	100,0%	47,2%	100,0%	32,3%	50,4%	100,0%
9.0 Індекс розвитку ІКТ	Значимость	100,0%	100,0%	100,0%	93,6%	61,4%	99,9%	24,8%	100,0%
9.0 Глобальний індекс кібербезпеки	Значимость	100,0%	100,0%	100,0%	99,9%	100,0%	76,5%	94,4%	100,0%

Рисунок В.3 – Профілі кластерів (складено авторкою)

Додаток Г

Результати DEA-аналізу

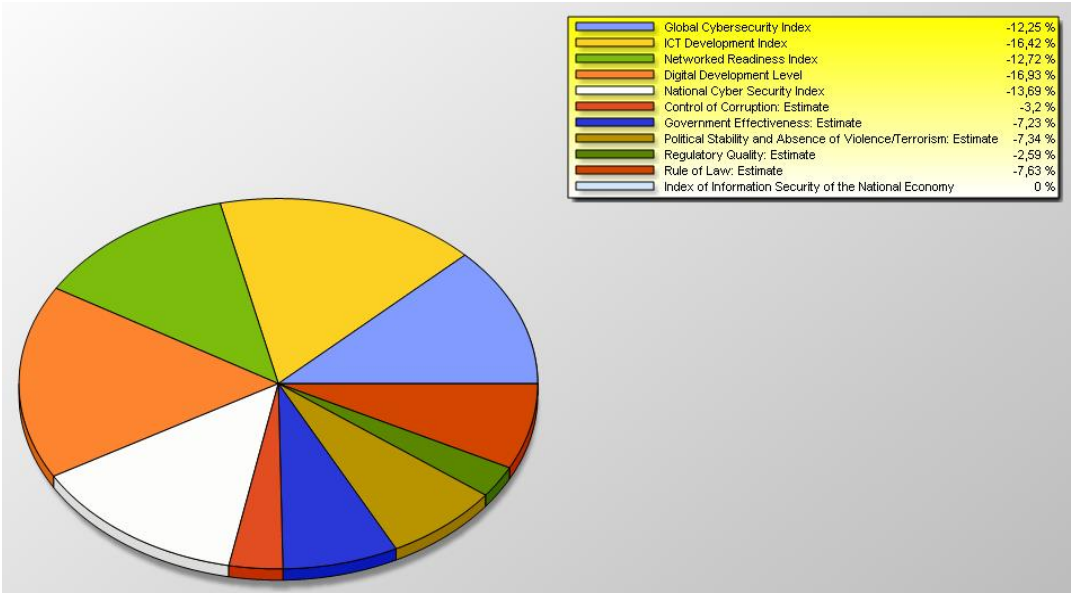


Рисунок Г.1 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 1-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

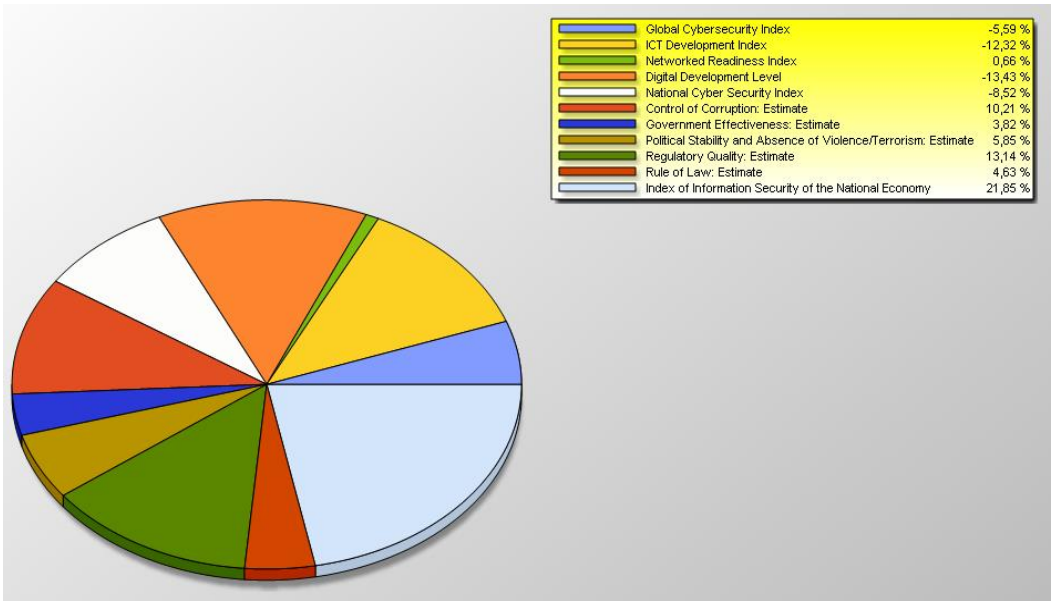


Рисунок Г.2 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 1-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Cyprus	100,0%	✓	
Poland	100,0%	✓	
Czech Republic	94,8%		
Spain	94,6%		
Portugal	94,6%		
Malta	91,8%		
United States	87,0%		
Germany	85,5%		
New Zealand	85,4%		
Finland	83,7%		
Netherlands	83,4%		
Singapore	82,1%		

Рисунок Г.3 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 0-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

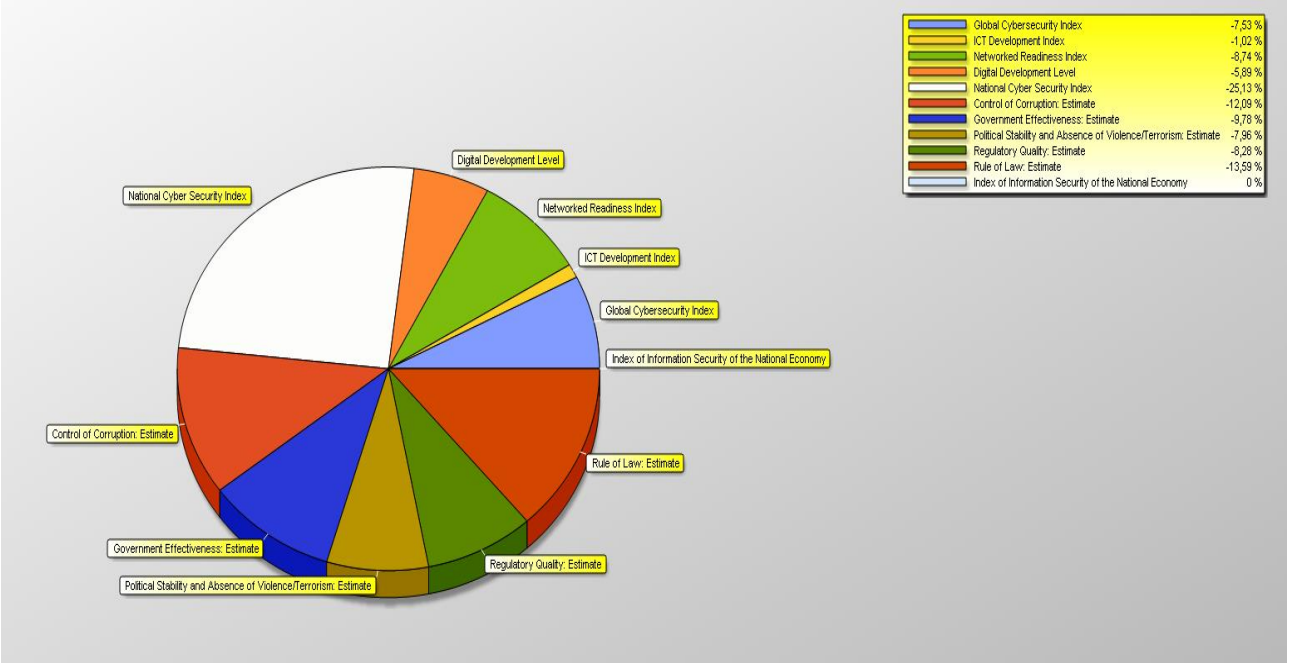


Рисунок Г.4 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 0-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Poland	100,0%	✓	
Cyprus	100,0%	✓	
Czech Republic	94,8%		
Spain	94,6%		
Portugal	94,6%		
Malta	91,8%		
United States	87,0%		
Germany	85,5%		
New Zealand	85,4%		
Finland	83,7%		
Netherlands	83,4%		
Singapore	82,1%		

Рисунок Г.5 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 0-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

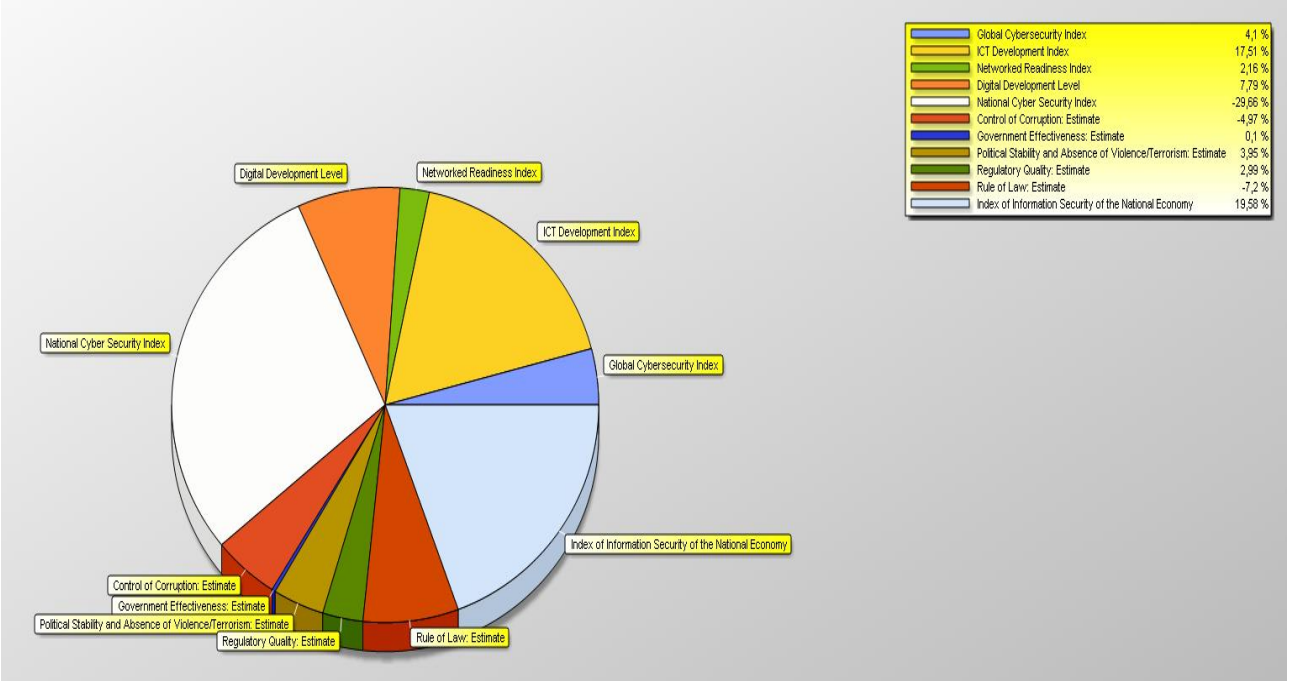


Рисунок Г.6 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 0-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Venezuela	100,0%	✓	
Nicaragua	87,6%		
Myanmar	84,2%		
Tajikistan	83,9%		
Mauritania	79,6%		
Mozambique	78,4%		
Mali	70,5%		
Madagascar	67,9%		
Zimbabwe	59,3%		
Haiti	42,7%		
Burundi	37,2%		
Chad	35,1%		

Рисунок Г.7 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 2-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

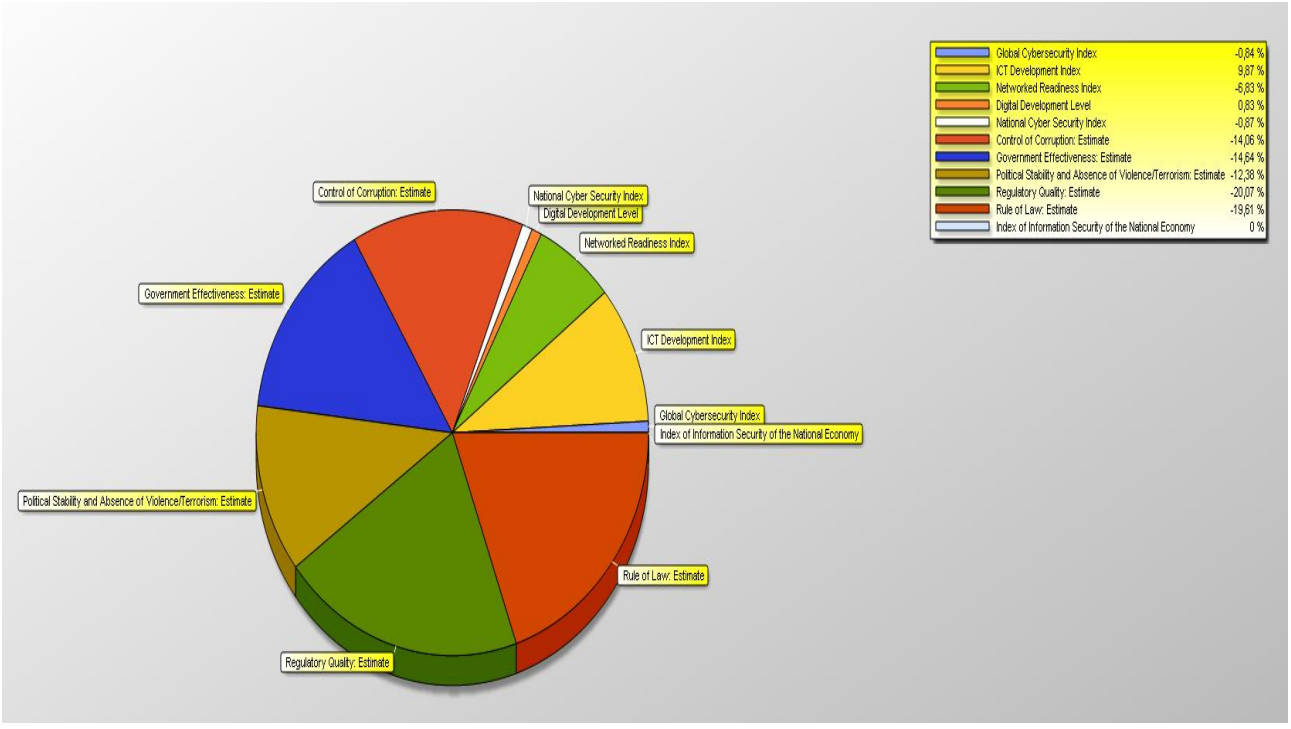


Рисунок Г.8 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 2-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Venezuela	100,0%	✓	
Nicaragua	87,6%		
Myanmar	84,2%		
Tajikistan	83,9%		
Mauritania	79,6%		
Mozambique	78,4%		
Mali	70,5%		
Madagascar	67,9%		
Zimbabwe	59,3%		
Haiti	42,7%		
Burundi	37,2%		
Chad	35,1%		

Рисунок Г.9 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 2-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

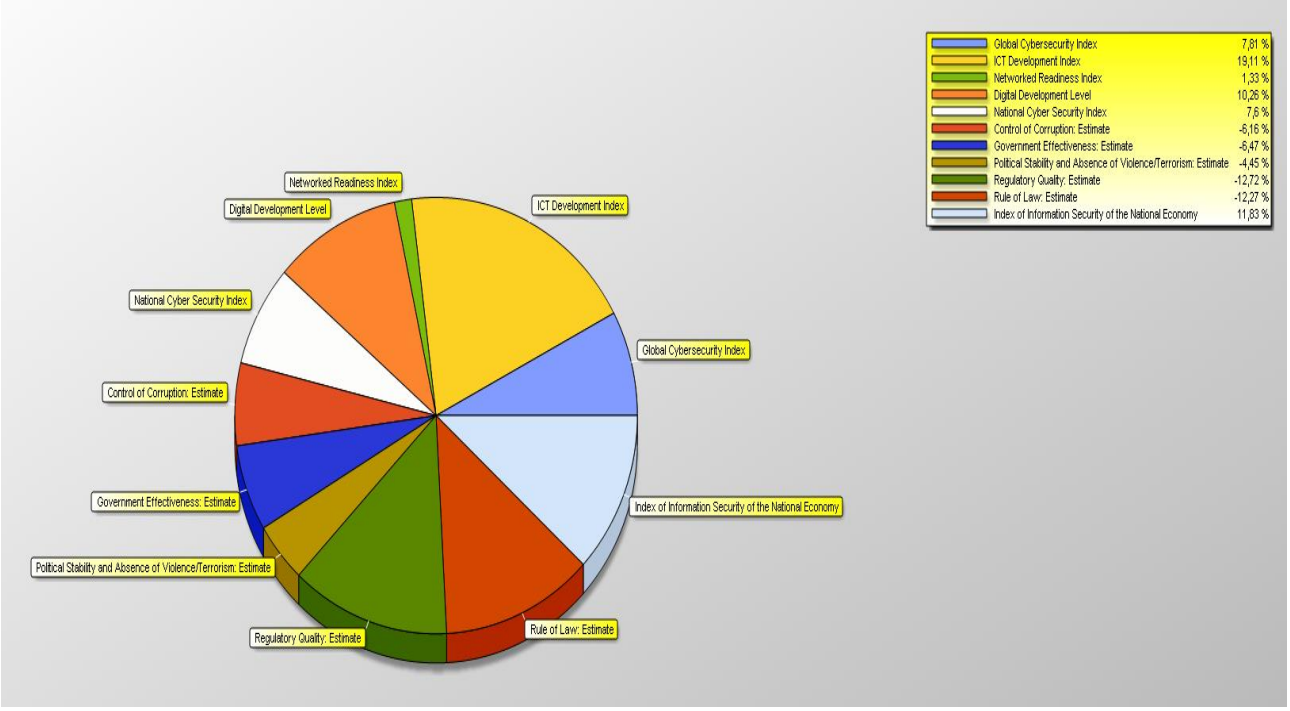


Рисунок Г.10 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 2-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Mongolia	100,0%	✓	
Morocco	97,4%		
Panama	87,9%		
Peru	85,6%		
Trinidad and Tobago	71,8%		
Bosnia and Herzegovina	56,7%		
Kyrgyzstan	45,6%		
El Salvador	41,9%		
Guatemala	36,8%		
Nepal	30,9%		
Cambodia	28,3%		
Malawi	25,3%		

Рисунок Г.11 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 3-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

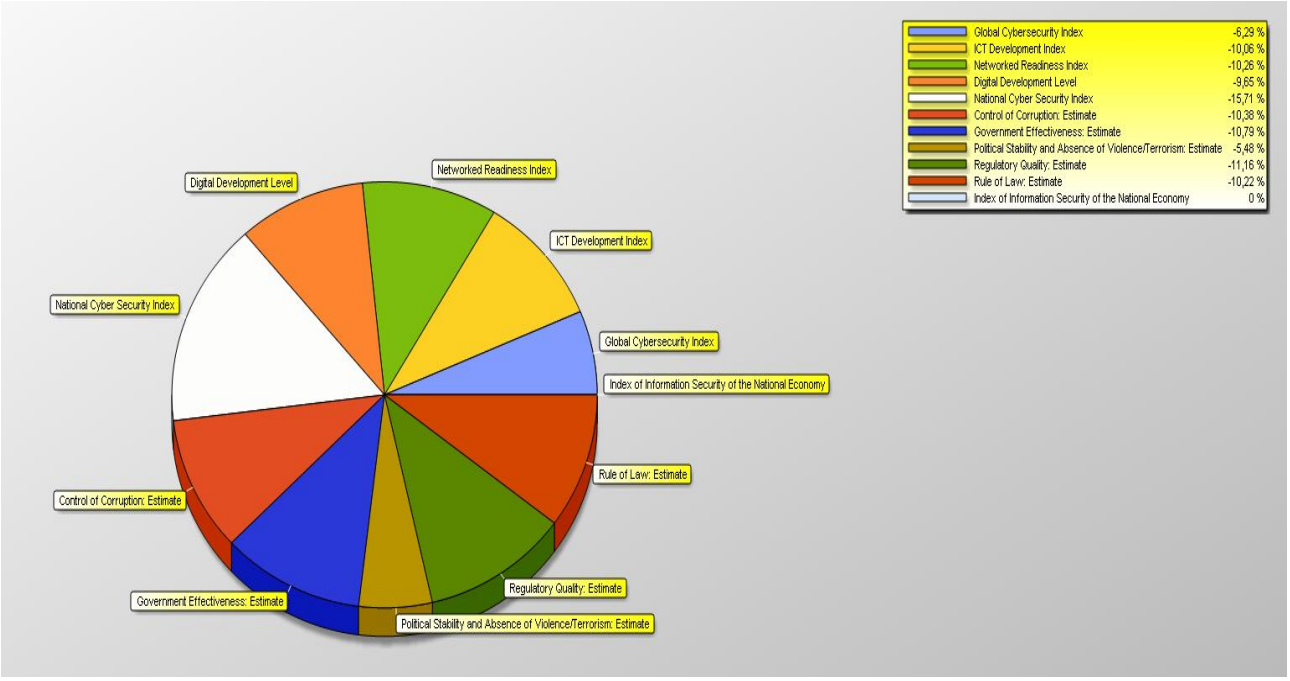


Рисунок Г.12 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 3-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Mongolia	100,0%	✓	
Morocco	97,4%		
Panama	87,9%		
Peru	85,6%		
Trinidad and Tobago	71,8%		
Bosnia and Herzegovina	56,7%		
Kyrgyzstan	45,6%		
El Salvador	41,9%		
Guatemala	36,8%		
Nepal	30,9%		
Cambodia	28,3%		
Malawi	25,3%		

Рисунок Г.13 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 3-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

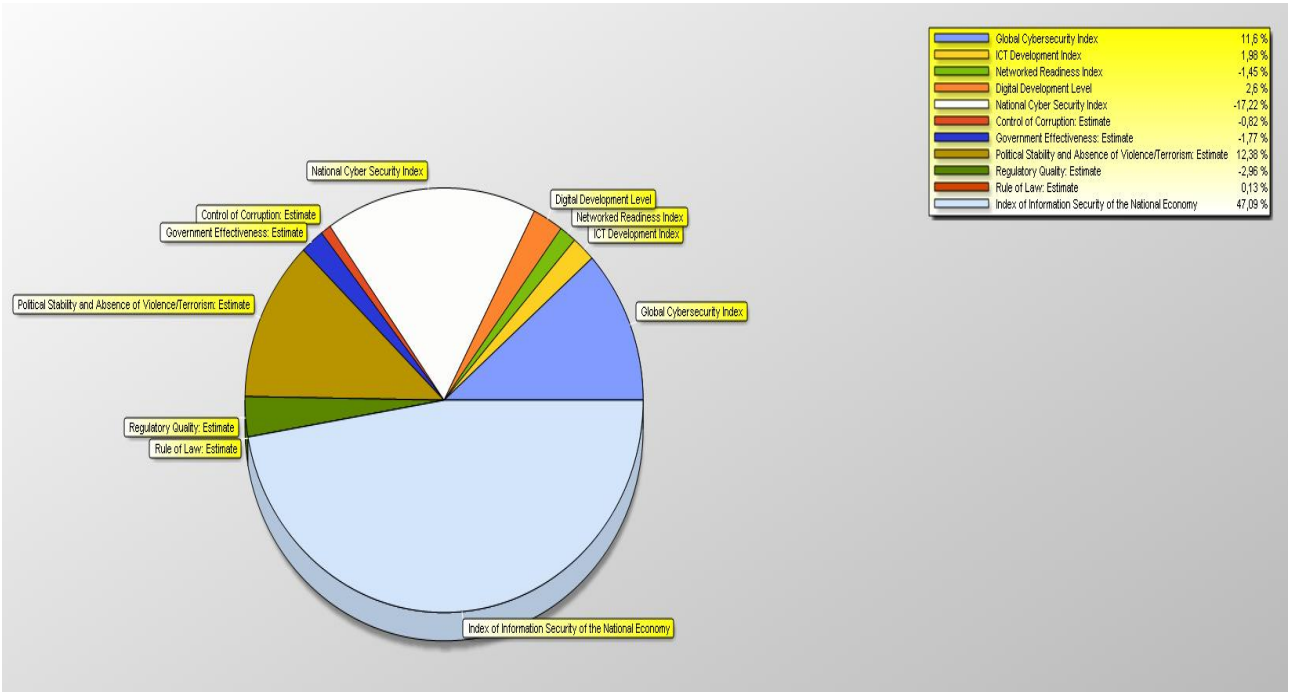


Рисунок Г.14 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 3-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Botswana	100,0%	✓	
Jamaica	95,0%		
Seychelles	79,5%		
Costa Rica	72,8%		
Namibia	54,2%		
Bhutan	53,6%		

Рисунок Г.15 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 4-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

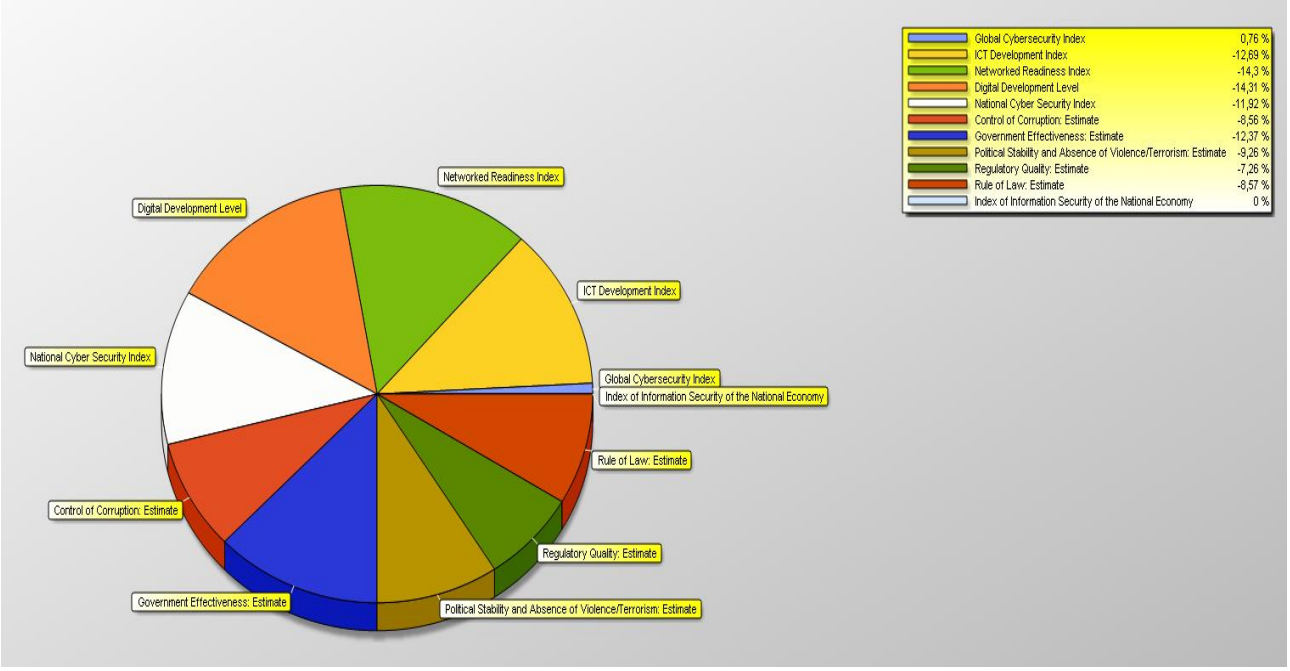


Рисунок Г.16 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 4-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Botswana	100,0%	✓	
Jamaica	95,0%		
Seychelles	79,5%		
Costa Rica	72,8%		
Namibia	54,2%		
Bhutan	53,6%		

Рисунок Г.17 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 4-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

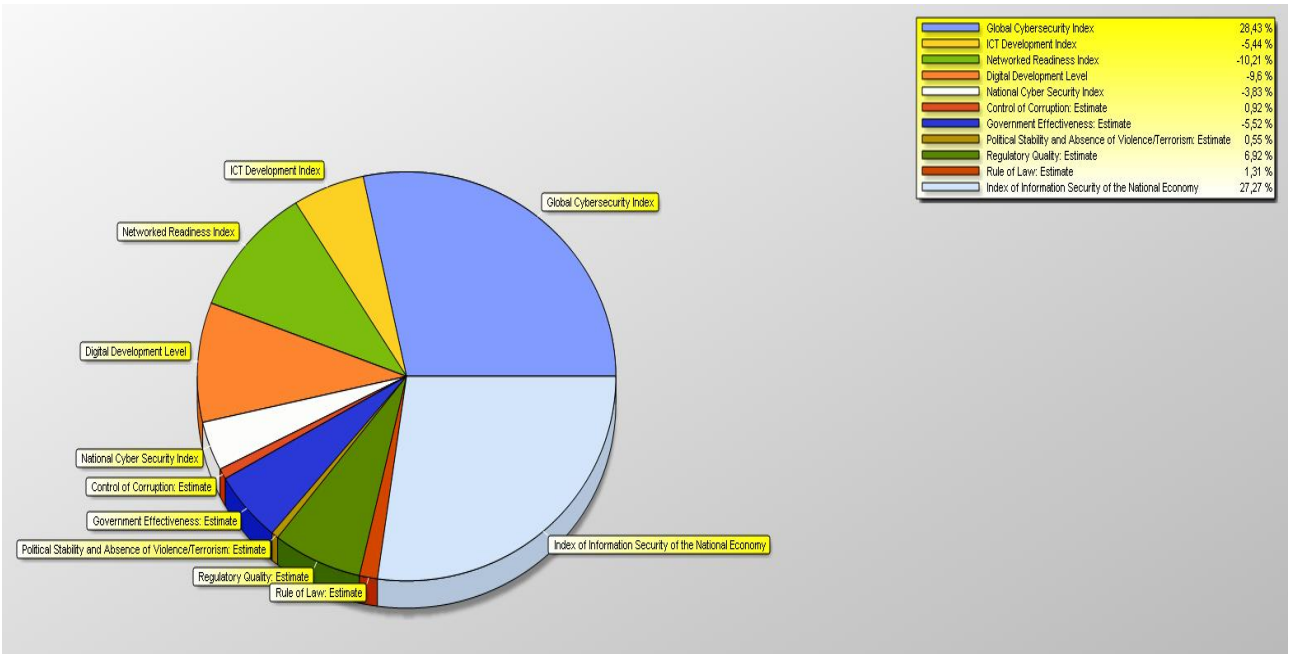


Рисунок Г.18 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 4-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
India	100,0%	✓	
Paraguay	100,0%	✓	
Rwanda	100,0%	✓	
Egypt	96,8%		
Iran (Islamic Republic of)	93,1%		
Cote d'Ivoire	78,0%		
Zambia	63,1%		
Uganda	56,2%		
Tanzania, United Republic of	53,8%		
Pakistan	45,9%		
Nigeria	40,5%		
Ethiopia	32,0%		

Рисунок Г.19 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 5-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

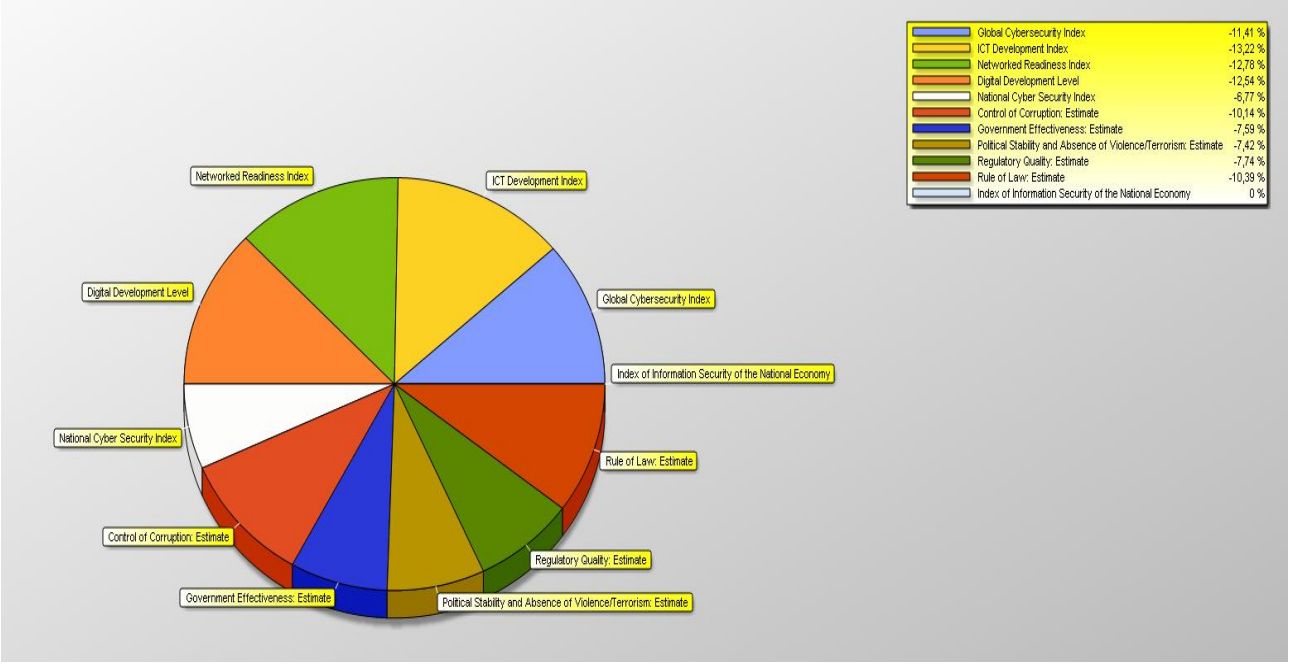


Рисунок Г.20 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 5-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Rwanda	100,0%	✓	
India	100,0%	✓	
Paraguay	100,0%	✓	
Egypt	96,8%		
Iran (Islamic Republic of)	93,1%		
Cote d'Ivoire	78,0%		
Zambia	63,1%		
Uganda	56,2%		
Tanzania, United Republic of	53,8%		
Pakistan	45,9%		
Nigeria	40,5%		
Ethiopia	32,0%		

Рисунок Г.21 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 5-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

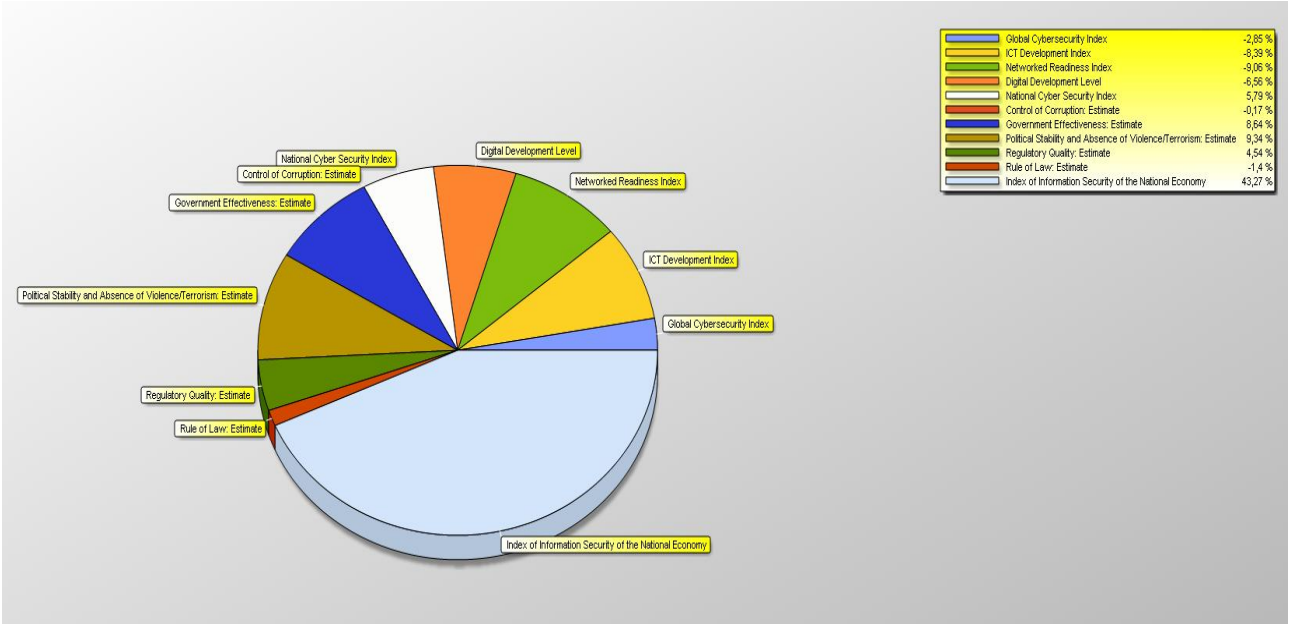


Рисунок Г.22 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 5-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Brunei Darussalam	100,0%	✓	
Antigua and Barbuda	75,3%		
Saint Vincent and the Grenadines	67,1%		
Barbados	64,7%		
Saint Kitts and Nevis	62,7%		
Bahamas	62,7%		
Dominica	61,1%		
Grenada	59,1%		
Samoa	58,6%		
Saint Lucia	57,8%		
Tonga	53,9%		
Suriname	45,2%		

Рисунок Г.23 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 6-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

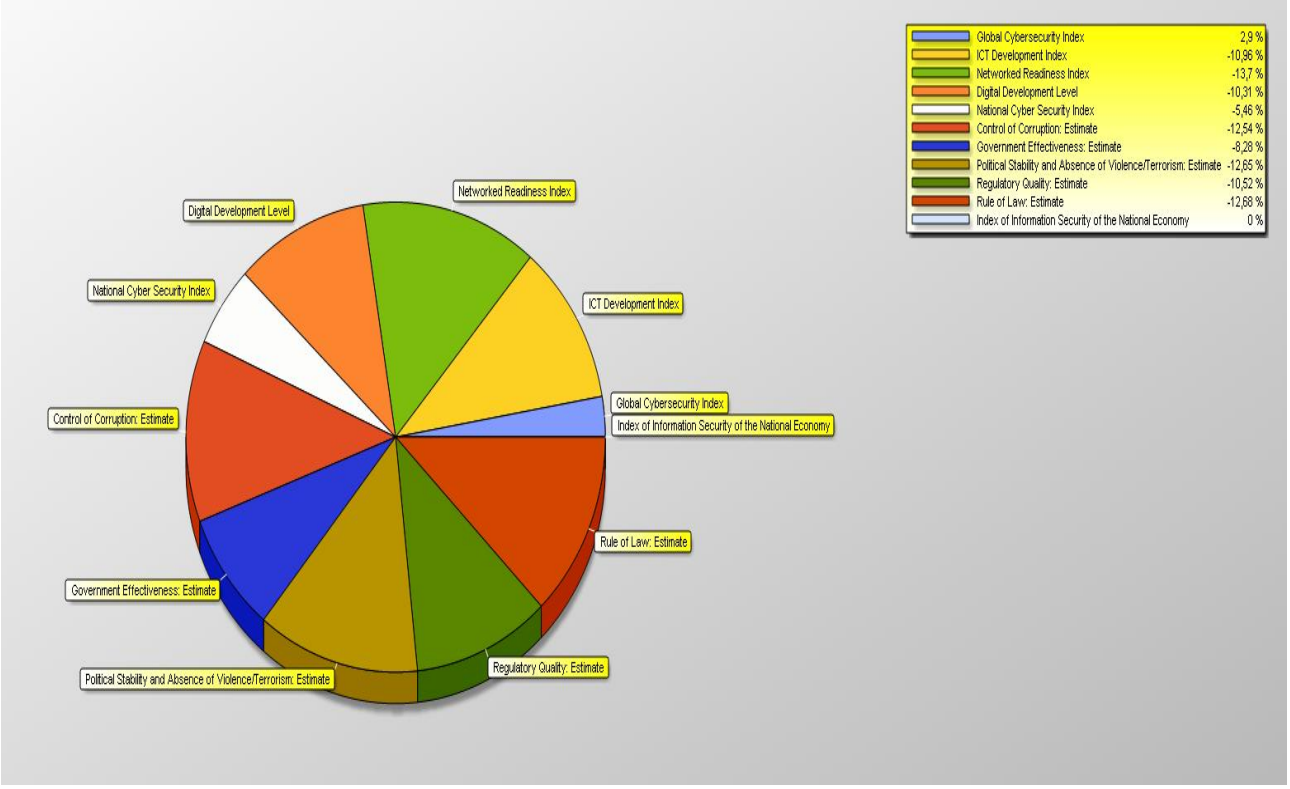


Рисунок Г.24 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 6-го кластеру (за Input-oriented CCR-моделлю) (складено авторкою)

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Brunei Darussalam	100,0%	✓	
Antigua and Barbuda	75,3%		
Saint Vincent and the Grenadines	67,1%		
Barbados	64,7%		
Saint Kitts and Nevis	62,7%		
Bahamas	62,7%		
Dominica	61,1%		
Grenada	59,1%		
Samoa	58,6%		
Saint Lucia	57,8%		
Tonga	53,9%		
Suriname	45,2%		

Рисунок Г.25 – Результати оцінок загальної ефективності системи інформаційної безпеки національної економіки країн 6-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

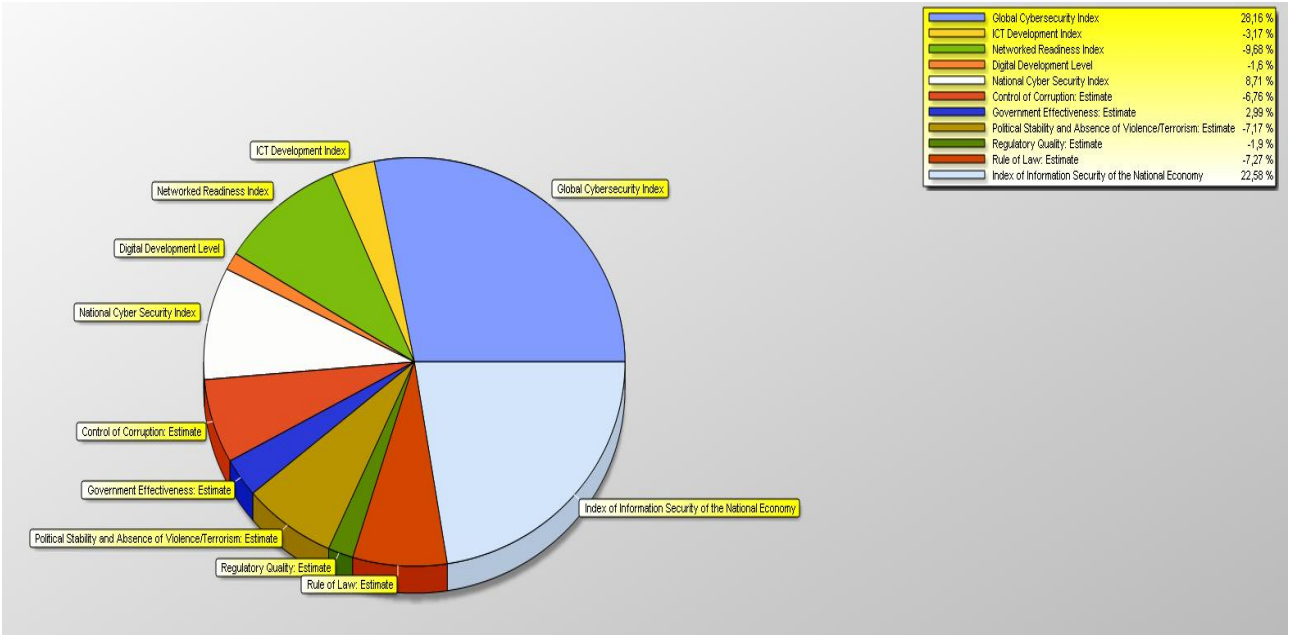


Рисунок Г.26 – Результати ефективності за складовими системи інформаційної безпеки національної економіки країн 6-го кластеру (за Output-oriented CCR-моделлю) (складено авторкою)

Додаток Д

Реалізація кластерного аналізу методом k-means

Таблиця Д.1 – Вхідні дані для здійснення кластерного аналізу

Країна*	Ймовірне придбання продуктів та послуг онлайн	Ймовірне використання онлайн-банкінгу	Ймовірне надання власної інформації на веб-сайтах	Персональна зміна налаштувань безпеки	Відвідування тільки надійних сайтів	Використання різних паролів для різних сайтів	Не відкривати електронні листи з незнайомих адрес	Використання тільки власного комп'ютера	Використання антивірусних програм	Скасування онлайн-покупки через підозри до сайту	Регулярна зміна паролів	Не змогли отримати доступ до онлайн-послуг через кібератаки	Жертви викрадення особистих даних	Жертви фішингу або соціальної інженерії	Жертви зламування поштового акаунту або акаунту соціальних мереж	Жертви шахрайств в онлайн-банкінгу або із банківськими картками	Жертви, яким було запропоновано здійснити платіж, щоб повернути контроль над пристроєм	Жертви вірусної атаки
BE	10%	9%	27%	14%	43%	28%	50%	43%	49%	7%	18%	10%	9%	43%	14%	9%	13%	32%
BG	9%	11%	25%	9%	32%	17%	36%	26%	32%	2%	18%	4%	2%	15%	7%	2%	2%	17%
CZ	10%	7%	26%	6%	31%	23%	43%	40%	34%	5%	16%	7%	5%	32%	12%	6%	9%	34%
DK	12%	2%	41%	19%	34%	41%	59%	36%	58%	9%	14%	7%	2%	72%	9%	11%	4%	31%
DE	10%	4%	48%	17%	26%	42%	50%	44%	57%	17%	27%	8%	6%	46%	10%	5%	15%	37%
EE	6%	3%	33%	16%	41%	32%	64%	43%	50%	12%	17%	12%	4%	35%	14%	4%	4%	32%
IE	12%	11%	28%	18%	35%	30%	38%	29%	35%	9%	25%	7%	6%	46%	15%	10%	7%	21%
EL	15%	22%	40%	9%	46%	15%	47%	42%	56%	4%	26%	1%	2%	9%	5%	1%	2%	18%
ES	11%	8%	19%	7%	26%	21%	33%	22%	29%	5%	14%	5%	5%	20%	5%	4%	4%	20%
FR	13%	7%	24%	14%	42%	29%	50%	32%	45%	8%	23%	11%	7%	47%	20%	14%	8%	37%
HR	12%	9%	24%	8%	22%	15%	27%	27%	30%	14%	13%	12%	10%	24%	12%	9%	10%	26%
IT	8%	8%	18%	8%	27%	18%	31%	19%	29%	4%	19%	8%	8%	26%	10%	8%	9%	23%
CY	21%	16%	39%	6%	44%	22%	47%	45%	33%	6%	21%	4%	5%	23%	14%	4%	5%	26%

Продовження таблиці Д.1

Країна*	Ймовірне придбання продуктів та послуг онлайн	Ймовірне використання онлайн-банкінгу	Ймовірне надання власної інформації на веб-сайтах	Персональна зміна налаштувань безпеки	Відвідування тільки надійних сайтів	Використання різних паролів для різних сайтів	Не відкривати електронні листи з незнайомих адрес	Використання тільки власного комп'ютера	Використання антивірусних програм	Скасування онлайн-покупки через підозри до сайту	Регулярна зміна паролів	Не змогли отримати доступ до онлайн-послуг через кібератаки	Жертви викрадення особистих даних	Жертви фішингу або соціальної інженерії	Жертви зламування поштового акаунту або акаунту соціальних мереж	Жертви шахрайств в онлайн-банкінгу або із банківськими картками	Жертви, яким було запропоновано здійснити платіж, щоб повернути контроль над пристроєм	Жертви вірусної атаки
LV	3%	2%	23%	8%	35%	27%	43%	39%	34%	8%	18%	8%	6%	26%	13%	3%	4%	25%
LT	16%	12%	42%	5%	37%	17%	45%	42%	57%	6%	18%	6%	1%	21%	6%	2%	3%	23%
LU	8%	9%	26%	17%	35%	31%	55%	37%	51%	9%	26%	13%	10%	41%	17%	15%	9%	40%
HU	8%	12%	20%	9%	20%	13%	25%	32%	33%	9%	14%	12%	12%	19%	12%	10%	9%	24%
MT	5%	4%	19%	11%	44%	34%	45%	42%	45%	3%	30%	4%	4%	31%	7%	2%	1%	16%
NL	10%	5%	59%	22%	45%	56%	64%	40%	60%	7%	23%	13%	3%	59%	11%	5%	10%	37%
AT	14%	12%	32%	20%	25%	28%	42%	36%	54%	14%	30%	15%	11%	36%	16%	9%	12%	40%
PL	7%	6%	25%	8%	27%	19%	35%	28%	33%	6%	18%	7%	6%	13%	7%	6%	6%	23%
PT	12%	11%	33%	10%	34%	20%	43%	26%	35%	2%	14%	2%	1%	5%	3%	2%	2%	11%
RO	12%	13%	13%	6%	13%	14%	23%	23%	28%	5%	12%	11%	11%	16%	13%	9%	11%	26%
SI	11%	9%	28%	11%	33%	23%	46%	43%	42%	5%	18%	7%	4%	20%	9%	4%	4%	32%
SK	4%	3%	16%	6%	29%	15%	35%	41%	45%	3%	16%	3%	3%	14%	5%	3%	3%	17%
FI	9%	2%	42%	28%	36%	46%	59%	38%	53%	10%	26%	25%	3%	45%	9%	6%	5%	34%
SE	22%	6%	55%	30%	37%	51%	60%	39%	52%	30%	17%	13%	5%	60%	12%	9%	8%	29%
UK	10%	10%	29%	19%	35%	34%	40%	30%	36%	6%	27%	5%	6%	45%	10%	13%	5%	20%

** BE – Бельгія, BG – Болгарія, CZ – Чехія, DK – Данія, DE – Німеччина, EE – Естонія, IE – Ірландія, EL – Греція, ES – Іспанія, FR – Франція, HR – Хорватія, IT – Італія, CY – Кіпр, LV – Латвія, LT – Литва, LU – Люксембург, HU – Угорщина, MT – Мальта, NL – Нідерланди, AT – Австрія, PL – Польща, PT – Португалія, RO – Румунія, SI – Словенія, SK – Словаччина, FI – Фінляндія, SE – Швеція, UK – Великобританія*

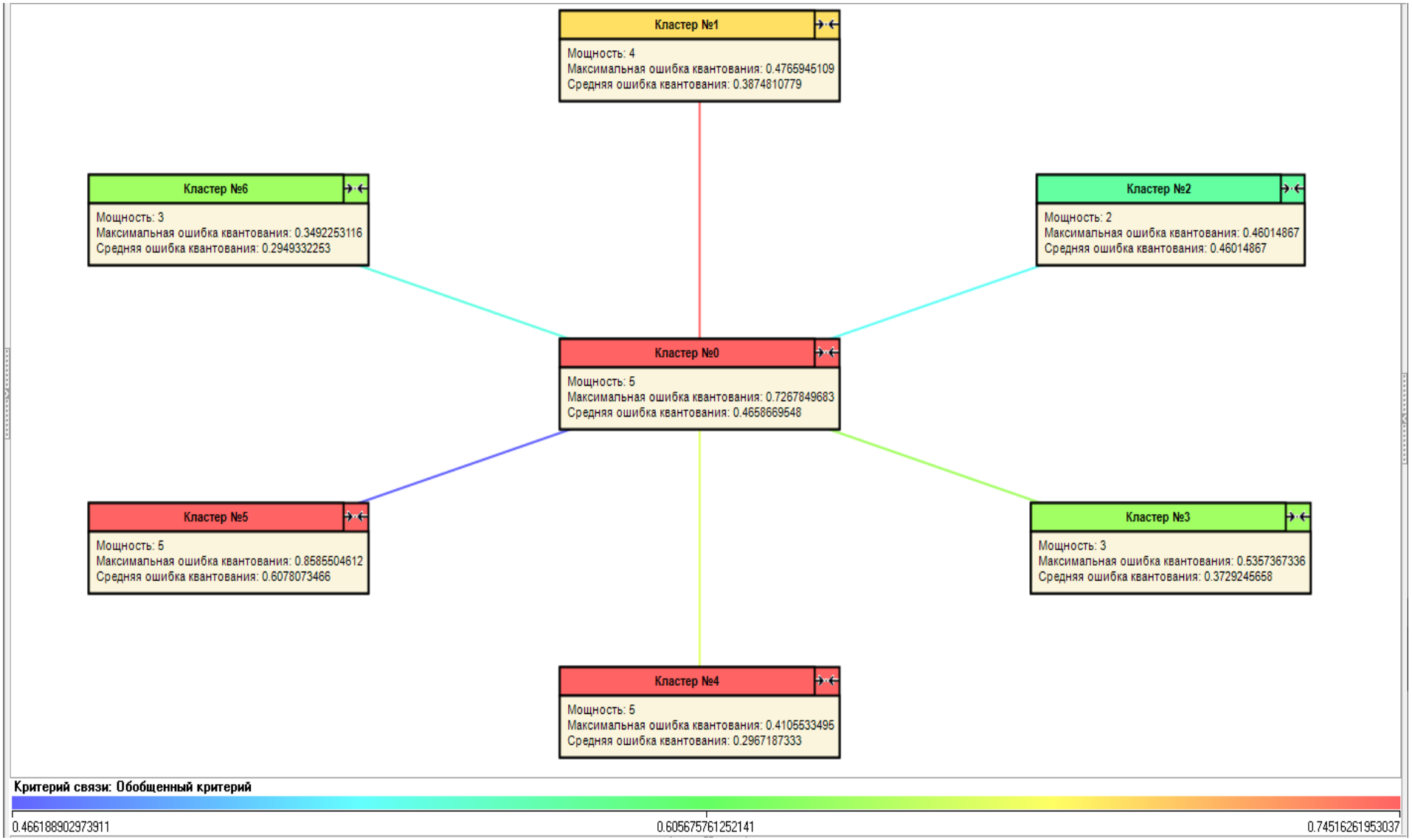


Рисунок Д.1 – Зв’язки отриманих кластерів (складено авторкою)

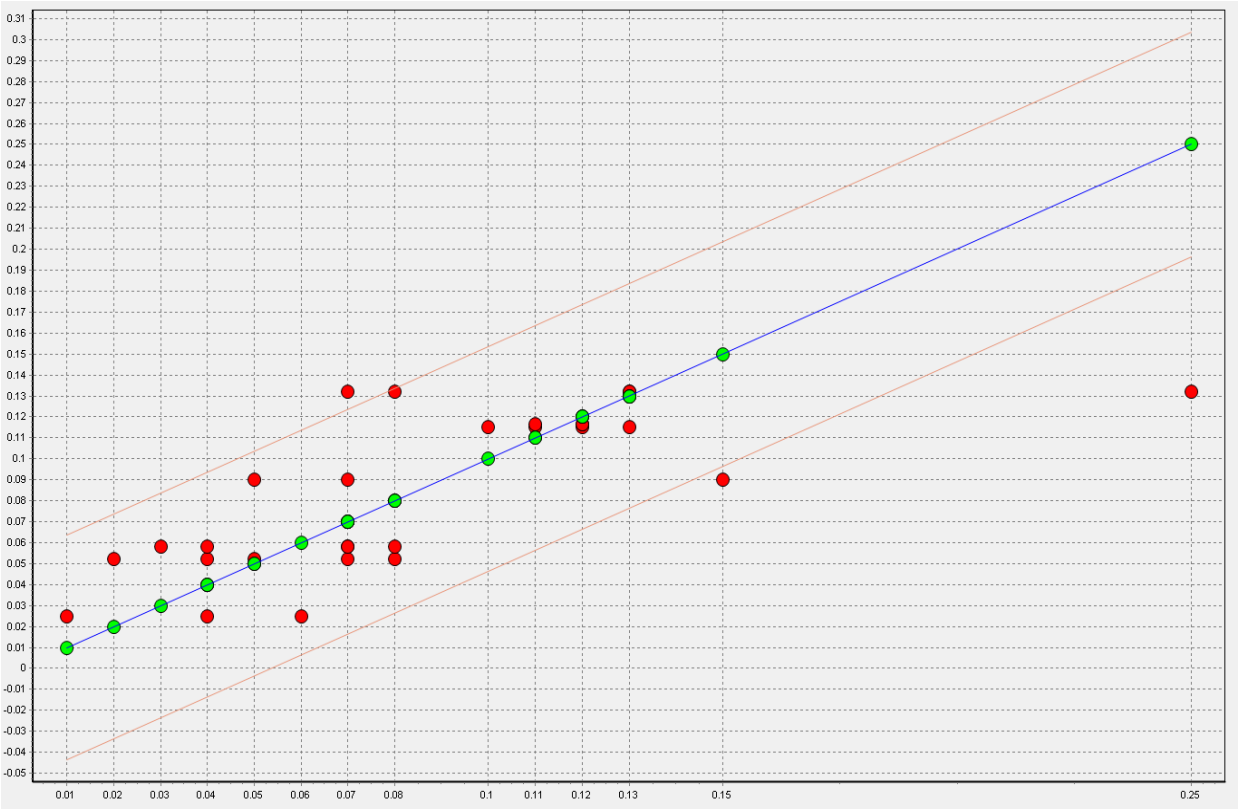


Рисунок Д.2 – Діаграма розсіювання по показнику «Респонденти, які не змогли отримати доступ до онлайн-послуг через кібератаки» (складено авторкою)

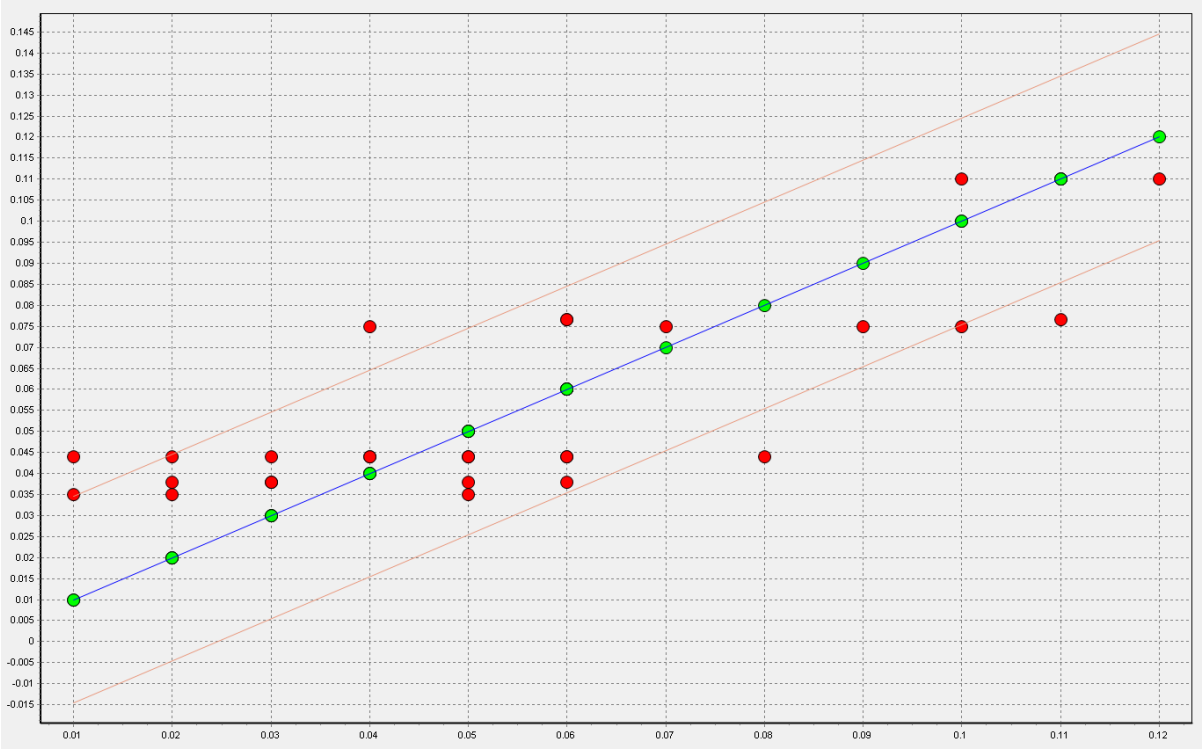


Рисунок Д.3 – Діаграма розсіювання по показнику «Жертви викрадення особистих даних» (складено авторкою)

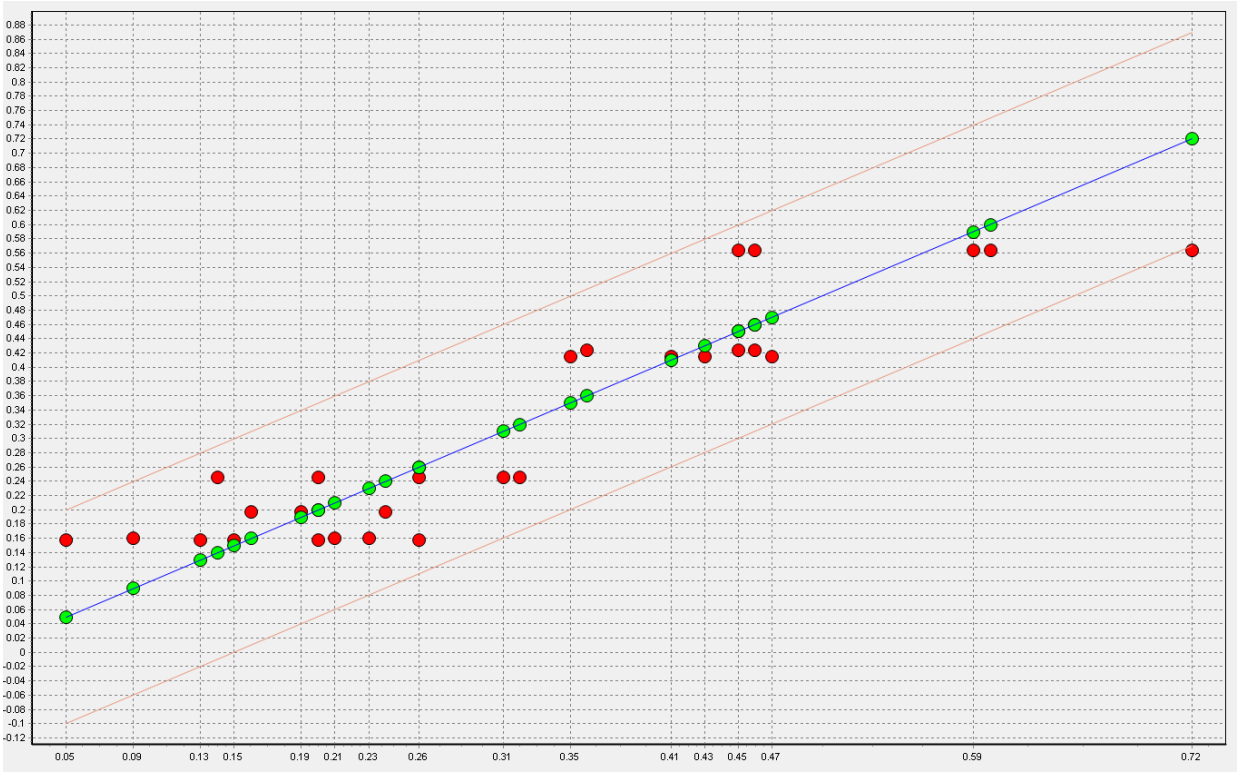


Рисунок Д.4 – Діаграма розсіювання по показнику «Жертви фішингу або соціальної інженерії» (складено авторкою)

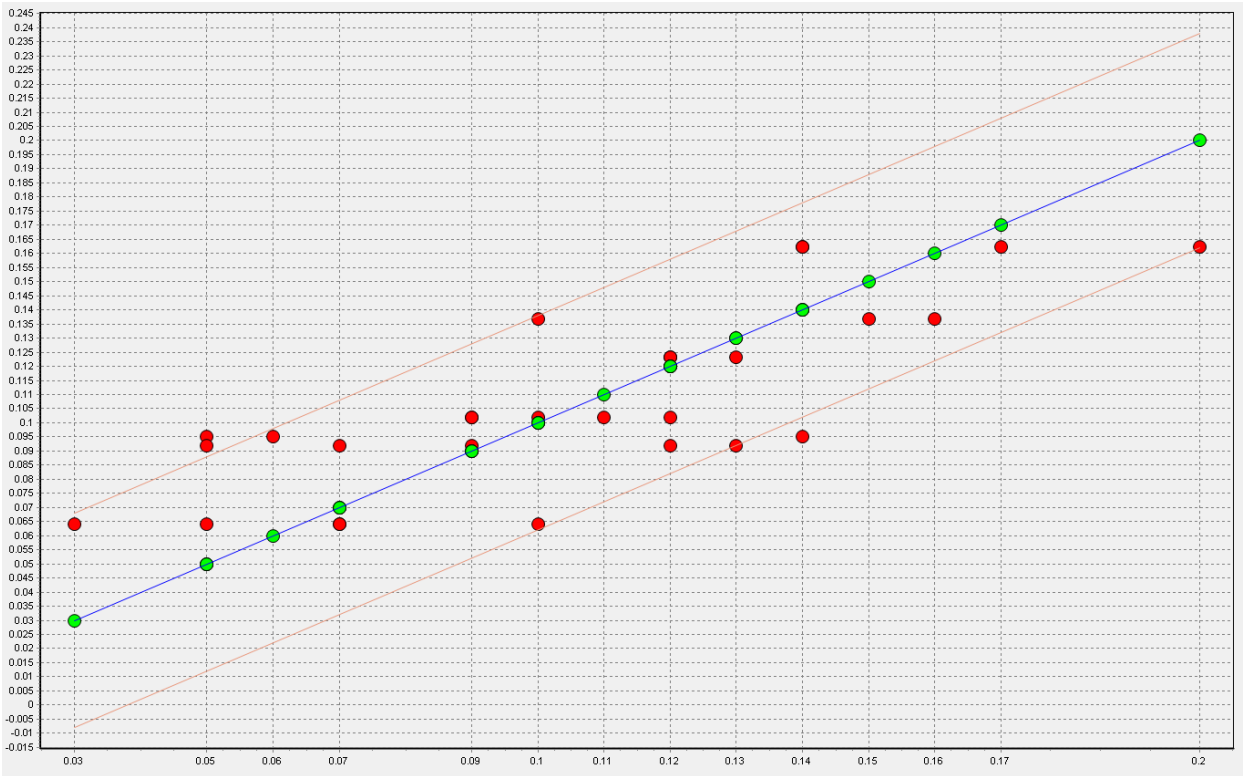


Рисунок Д.5 – Діаграма розсіювання по показнику «Жертви зламування поштового акаунту або акаунту соціальних мереж» (складено авторкою)

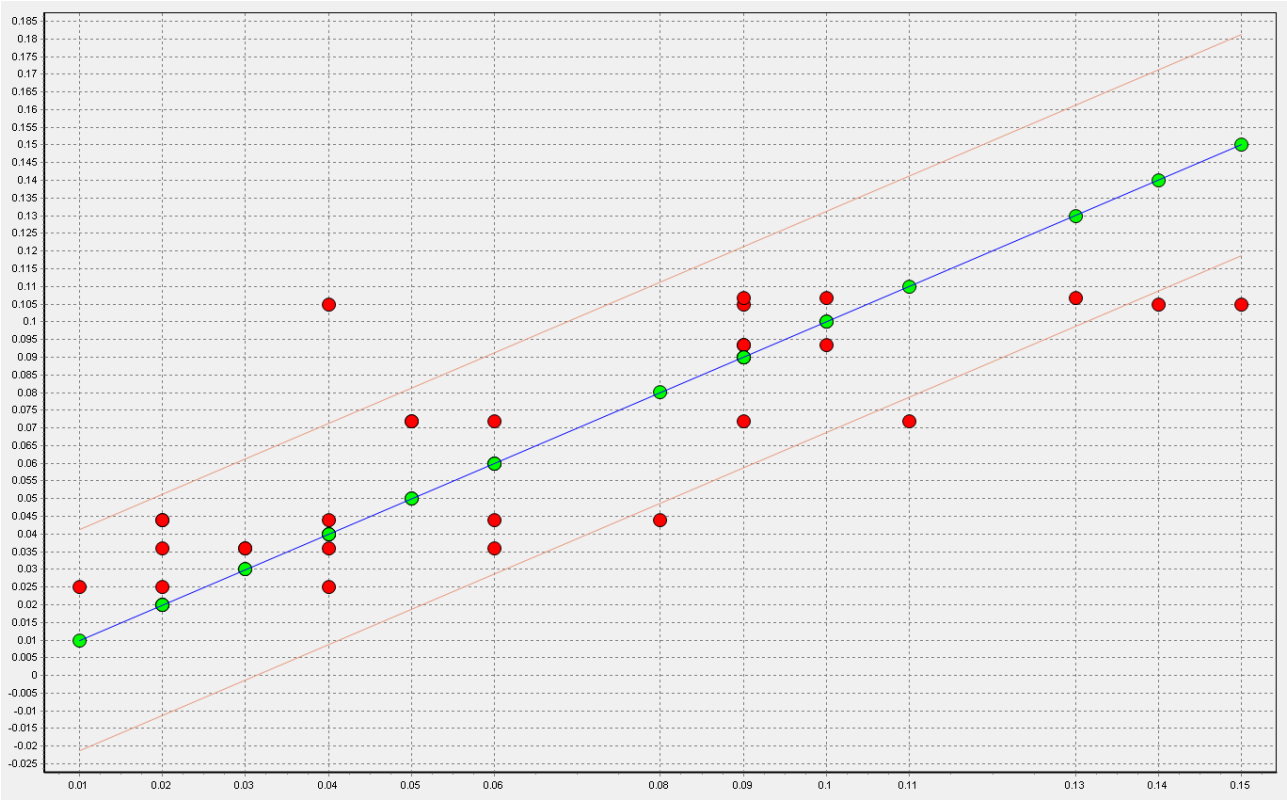


Рисунок Д.6 – Діаграма розсіювання по показнику «Жертви шахрайств онлайн-банкінгу або із банківськими картками» (складено авторкою)

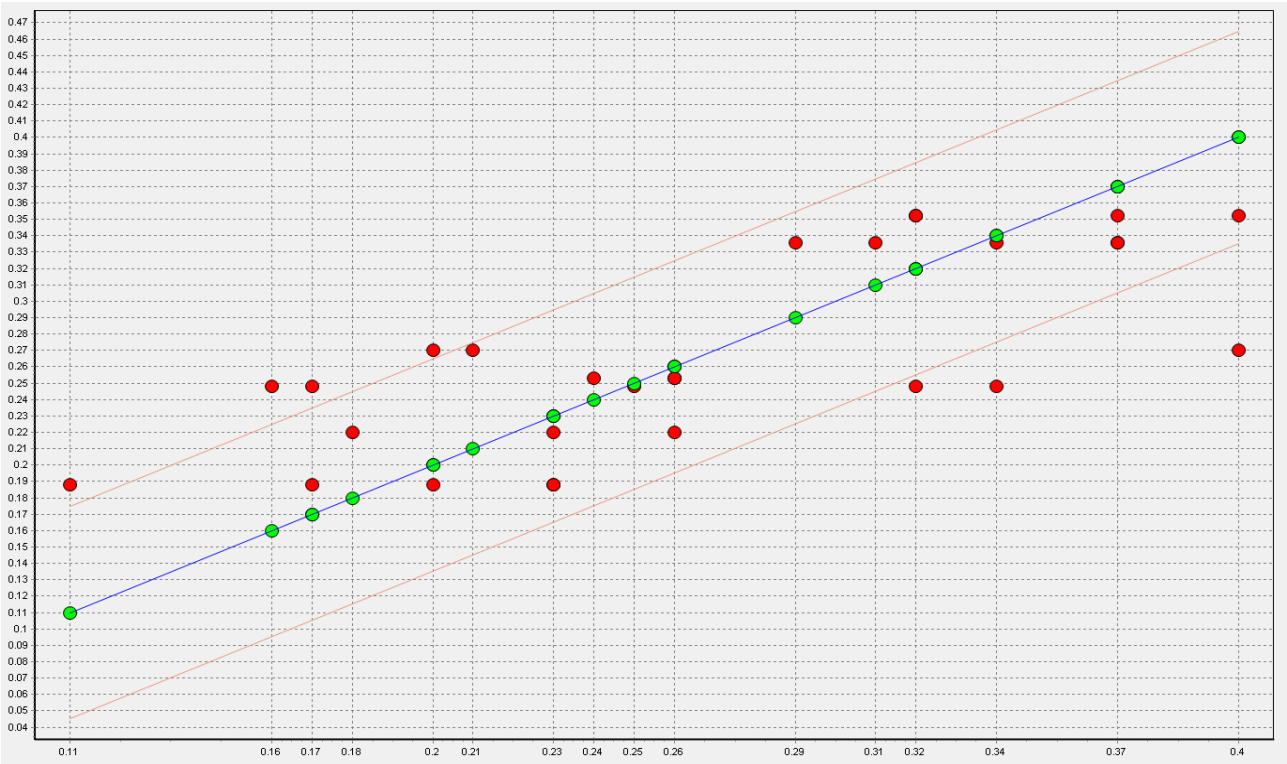


Рисунок Д.7 – Діаграма розсіювання по показнику «Жертви вірусної атаки» (складено авторкою)

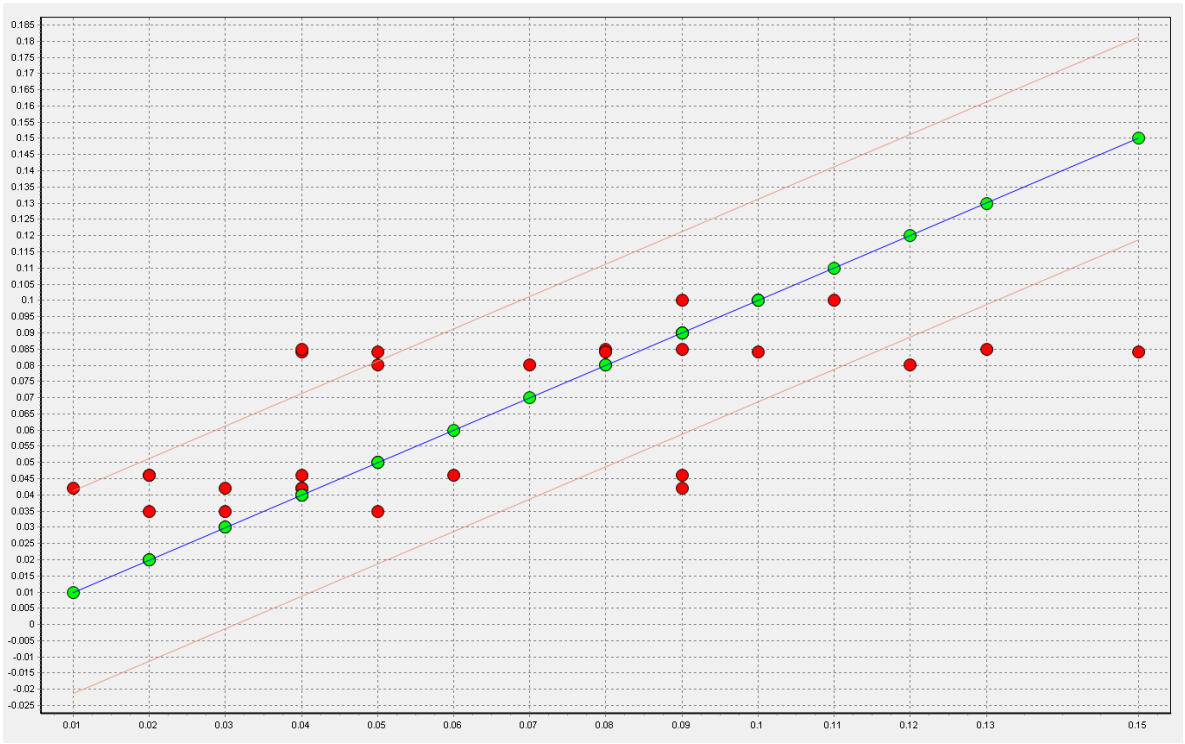
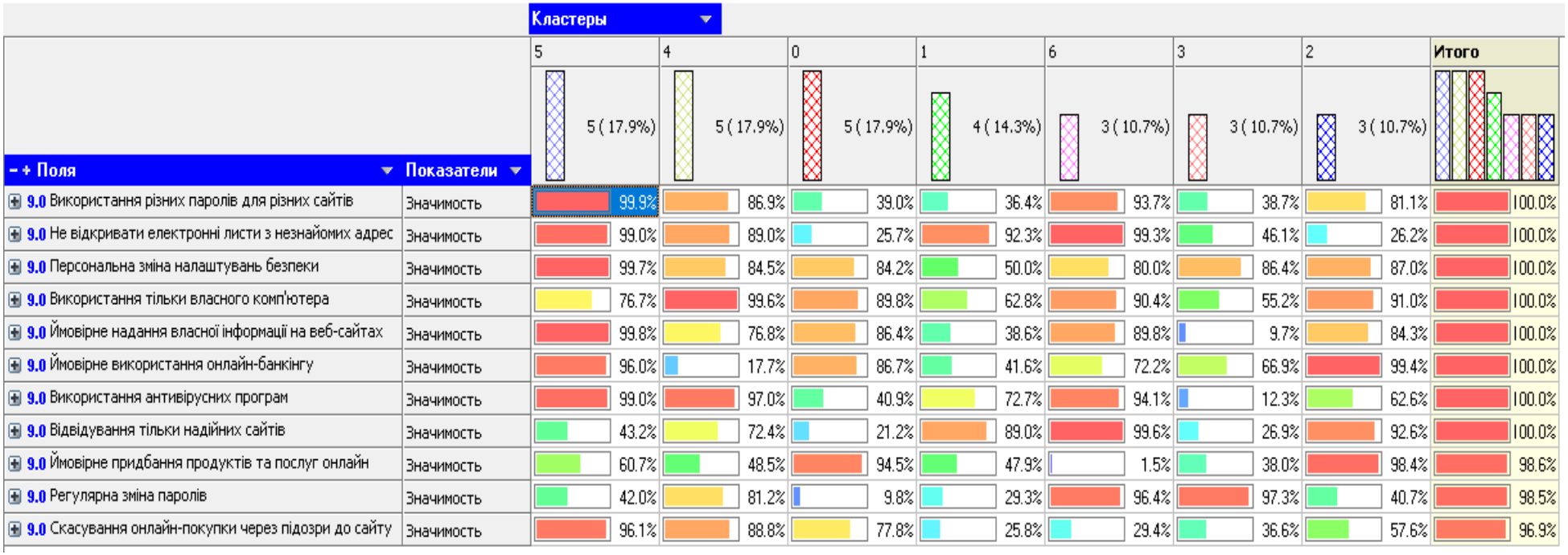


Рисунок Д.8 – Діаграма розсіювання по показнику «Жертви, яким було запропоновано здійснити платіж, щоб повернути контроль над пристроєм» (складено авторкою)

	0	1	2	3	4	5	6
0	100.00%	74.52%	53.90%	63.47%	66.27%	46.62%	54.75%
1	74.52%	100.00%	58.88%	69.35%	54.30%	65.90%	40.39%
2	53.90%	58.88%	100.00%	56.32%	44.35%	40.72%	34.90%
3	63.47%	69.35%	56.32%	100.00%	60.14%	55.31%	48.48%
4	66.27%	54.30%	44.35%	60.14%	100.00%	31.41%	76.30%
5	46.62%	65.90%	40.72%	55.31%	31.41%	100.00%	20.06%
6	54.75%	40.39%	34.90%	48.48%	76.30%	20.06%	100.00%

Рисунок Д.9 – Матриця порівняння (складено авторкою)



Поля	Показатели	Кластеры 5 (5 (17.9%))	4 (5 (17.9%))	0 (5 (17.9%))	1 (4 (14.3%))	6 (3 (10.7%))	3 (3 (10.7%))	2 (3 (10.7%))	Итого
9.0 Використання різних паролів для різних сайтів	Значимость	99.9%	86.9%	39.0%	36.4%	93.7%	38.7%	81.1%	100.0%
9.0 Не відкривати електронні листи з незнайомих адрес	Значимость	99.0%	89.0%	25.7%	92.3%	99.3%	46.1%	26.2%	100.0%
9.0 Персональна зміна налаштувань безпеки	Значимость	99.7%	84.5%	84.2%	50.0%	80.0%	86.4%	87.0%	100.0%
9.0 Використання тільки власного комп'ютера	Значимость	76.7%	99.6%	89.8%	62.8%	90.4%	55.2%	91.0%	100.0%
9.0 Ймовірне надання власної інформації на веб-сайтах	Значимость	99.8%	76.8%	86.4%	38.6%	89.8%	9.7%	84.3%	100.0%
9.0 Ймовірне використання онлайн-банкінгу	Значимость	96.0%	17.7%	86.7%	41.6%	72.2%	66.9%	99.4%	100.0%
9.0 Використання антивірусних програм	Значимость	99.0%	97.0%	40.9%	72.7%	94.1%	12.3%	62.6%	100.0%
9.0 Відвідування тільки надійних сайтів	Значимость	43.2%	72.4%	21.2%	89.0%	99.6%	26.9%	92.6%	100.0%
9.0 Ймовірне придбання продуктів та послуг онлайн	Значимость	60.7%	48.5%	94.5%	47.9%	1.5%	38.0%	98.4%	98.6%
9.0 Регулярна зміна паролів	Значимость	42.0%	81.2%	9.8%	29.3%	96.4%	97.3%	40.7%	98.5%
9.0 Скасування онлайн-покупки через підозри до сайту	Значимость	96.1%	88.8%	77.8%	25.8%	29.4%	36.6%	57.6%	96.9%

Рисунок Д.10 – Портрети кластерів (складено авторкою)

Додаток Е

Результати розрахунків за методикою гравітаційного моделювання

Таблиця Е.1 – Результати нормалізації показників

Назва країни	GDP*	FCI*	CCG*	CI*	CPI*	GTI*	HI*	NCSI*
Australia	0,0118	0,1537	0,8658	0,5090	0,2338	0,3735	0,4539	0,2174
Austria	0,0132	0,1953	0,7868	0,2441	0,2368	0,2447	0,4622	0,1887
Bahrain	0,0282	0,3087	0,7854	0,4421	0,5000	0,5131	0,5401	0,5002
Belgium	0,0142	0,1340	0,7604	0,5044	0,2400	0,5365	0,4762	0,1516
Bolivia	0,1909	0,0597	0,8699	0,6327	0,6207	0,0000	0,5739	0,4547
Botswana	0,0818	0,0248	0,9808	0,6321	0,2951	0,0000	0,9192	0,5883
Brazil	0,0752	0,0868	0,6123	0,8439	0,5143	0,1834	0,5140	0,2779
Bulgaria	0,0718	0,0575	0,8977	0,4749	0,4286	0,0416	0,6694	0,2500
Canada	0,0146	0,2679	0,7967	0,4699	0,2222	0,4660	0,4502	0,2273
Chile	0,0425	0,1061	0,8021	0,5560	0,2687	0,4564	0,5093	0,2273
China	0,0679	0,2344	0,7218	0,4718	0,4615	0,6749	0,6286	0,3705
Costa Rica	0,0559	0,1062	0,7752	0,6446	0,3214	0,0000	0,4668	0,2439
Croatia	0,0451	0,0751	0,7927	0,3230	0,3750	0,0018	0,6203	0,1563
Cyprus	0,0236	0,2544	0,7431	0,3610	0,3051	0,1594	0,5729	0,3126
Czech Republic	0,0289	0,0913	0,8746	0,3446	0,3051	0,2064	0,4918	0,1409
Denmark	0,0110	0,1045	0,9103	0,2634	0,2045	0,1080	0,4365	0,1588
Dominican Republic	0,0841	0,0925	0,7726	0,7360	0,6000	0,0505	0,6226	0,3126
Estonia	0,0292	0,0500	0,9125	0,2492	0,2466	0,0303	0,5749	0,1429
Finland	0,0135	0,0895	0,8220	0,2835	0,2118	0,3305	0,4325	0,1588
France	0,0163	0,2543	0,7661	0,5417	0,2500	0,7234	0,5085	0,1563
Germany	0,0142	0,4837	0,8388	0,4384	0,2250	0,6080	0,4735	0,1613
Ghana	0,3076	0,0433	0,8197	0,5383	0,4390	0,0214	0,7082	0,4167
Greece	0,0333	0,0746	0,9183	0,4673	0,4000	0,5670	0,6157	0,1352
Guatemala	0,1514	0,0778	0,8377	0,7099	0,6667	0,0271	0,5172	0,4547
Hungary	0,0413	0,0835	0,7899	0,4367	0,3913	0,0480	0,5872	0,2000
Iceland	0,0093	0,0879	0,9355	0,2929	0,2368	0,0075	0,4400	0,2779
India	0,3377	0,1992	0,7553	0,5282	0,4390	1,0000	0,7876	0,2174
Indonesia	0,1739	0,1188	0,8610	0,5349	0,4737	0,6003	0,6483	0,3334
Ireland	0,0086	0,2441	0,8157	0,5242	0,2466	0,4024	0,4728	0,2041
Israel	0,0162	0,1973	0,8715	0,4414	0,2951	0,6049	0,4590	0,2000
Italy	0,0196	0,1599	0,5610	0,5327	0,3462	0,3615	0,5500	0,1695
Japan	0,0173	0,3925	0,0000	0,1567	0,2466	0,3866	0,5574	0,2084
Kenya	0,3966	0,2380	0,8342	0,7150	0,6667	0,8079	0,7483	0,3705
Korea	0,0203	0,1976	0,9082	0,4286	0,3158	0,0378	0,5612	0,2084
Latvia	0,0379	0,1231	0,8777	0,4413	0,3103	0,0605	0,5565	0,1819
Liberia	1,0000	0,1744	0,8173	1,0000	0,5625	0,0277	0,9429	0,6668
Lithuania	0,0353	0,0370	0,8769	0,4496	0,3051	0,0000	0,5546	0,1471
Luxembourg	0,0058	0,6139	0,9029	0,3842	0,2222	0,0000	0,4776	0,2084

Назва країни	GDP*	FCI*	CCG*	CI*	CPI*	GTI*	HI*	NCSI*
Malaysia	0,0595	0,2108	0,8193	0,7542	0,3830	0,3568	0,5222	0,1786
Malta	0,0223	0,2682	0,7993	0,3819	0,3333	0,0000	0,4977	0,2565
Mauritius	0,0604	0,1406	0,7951	0,5779	0,3529	0,0000	0,5603	0,2703
Mexico	0,0699	0,0677	0,7926	0,6106	0,6429	0,4668	0,5085	0,3573
Montenegro	0,0766	0,0331	0,8719	0,4487	0,4000	0,0050	0,6168	0,3847
Netherlands	0,0128	0,3767	0,8028	0,3462	0,2195	0,2590	0,4435	0,1588
New Zealand	0,0158	0,1123	0,8533	0,4683	0,2069	0,0378	0,4508	0,2326
North Macedonia	0,1112	0,0250	0,8425	0,4810	0,4865	0,0858	0,6358	0,3227
Norway	0,0083	0,1528	0,9806	0,5183	0,2143	0,0202	0,4348	0,2084
Panama	0,0434	0,3937	0,9196	0,5783	0,4865	0,0100	0,5132	0,2703
Paraguay	0,1167	0,0997	0,9398	0,5858	0,6207	0,4549	0,5810	0,2273
Philippines	0,2083	0,1697	0,7853	0,4800	0,5000	0,9489	0,5978	0,4001
Poland	0,0438	0,1355	0,8118	0,4334	0,3000	0,0950	0,5392	0,1852
Portugal	0,0287	0,0954	0,7235	0,4132	0,2813	0,0000	0,6100	0,1819
Romania	0,0546	0,1461	0,8624	0,3474	0,3830	0,0000	0,5546	0,1819
Russian Federation	0,0596	0,2272	0,9290	0,5407	0,6429	0,6911	0,5680	0,2000
Saudi Arabia	0,0290	0,1753	1,0000	0,4389	0,3673	0,7240	0,5181	0,2223
Singapore	0,0102	0,6807	0,8034	0,1941	0,2118	0,0000	0,5205	0,1613
Slovakia	0,0349	0,0805	0,7959	0,3606	0,3600	0,0152	0,5348	0,1640
Slovenia	0,0259	0,0222	0,7909	0,2956	0,3000	0,0000	0,5546	0,2273
South Africa	0,1063	0,1362	0,7598	0,9056	0,4186	0,5633	0,6992	0,4763
Spain	0,0223	0,1346	0,6783	0,4395	0,3103	0,5317	0,5230	0,1471
Sweden	0,0124	0,1281	0,8730	0,5892	0,2118	0,5201	0,4514	0,2273
Switzerland	0,0082	1,0000	0,8664	0,2603	0,2118	0,0177	0,4406	0,1695
Tanzania	0,6384	0,0811	0,8719	0,7157	0,5000	0,4450	1,0000	1,0000
Thailand	0,0928	0,3464	0,7916	0,5652	0,5000	0,8261	0,5437	0,3031
Trinidad and Tobago	0,0395	0,0175	0,8887	0,8639	0,4390	0,0164	0,5331	0,6251
Turkey	0,0716	0,2226	0,8091	0,4911	0,4390	0,9297	0,6022	0,2381
Ukraine	0,2187	0,1549	0,7663	0,5908	0,5625	0,7992	0,8049	0,1570
United Kingdom	0,0157	0,2666	0,7232	0,4928	0,2250	0,7413	0,4846	0,1667
United States	0,0108	0,8169	0,6456	0,5931	0,2535	0,8015	0,4790	0,1640
Uruguay	0,0392	0,0932	0,8465	0,6200	0,2571	0,0455	0,5172	0,2703
Venezuela	0,0422	0,0661	0,8438	0,9879	1,0000	0,4843	0,6861	0,4001

** GDP - Валовий внутрішній продукт на душу населення, у поточних доларах США; CCG – Вимоги до центрального уряду; FCI – Індекс фінансової таємниці; CPI – Індекс сприйняття корупції; GTI – Глобальний індекс тероризму; HI – Індекс щастя; CI – Індекс злочинності; NCSI – Національний індекс кібербезпеки*

Таблиця Е.2 – Результати експертних оцінок щодо переваг одних факторів над іншими

Оцінки 1-го експерта									
Фактори	GDP	FCI	CCG	CI	CPI	GTI	HI	NCSI	Ваговий коефіцієнт з NCSI
GDP	1	1/8	1/3	1	1/9	1/5	7	1/5	0,0398
FCI	8	1	7	9	1	1	5	1/7	0,1906
CCG	3	1/7	1	7	1/3	1/3	1	1/7	0,0624
CI	1	1/9	1/7	1	1/7	1	1	1	0,0427
CPI	9	1	3	7	1	1	7	1	0,2242
GTI	5	1	3	1	1	1	7	1/3	0,1424
HI	1/7	1/5	1	1	1/7	1/7	1	1/8	0,0278
NCSI	5	7	7	1	1	3	8	1	0,2702
Оцінки 2-го експерта									
Фактори	GDP	FCI	CCG	CI	CPI	GTI	HI	NCSI	Ваговий коефіцієнт з NCSI
GDP	1	1/7	1/4	3	1/3	1/4	5	1/8	0,0527
FCI	7	1	4	3	3	1/5	7	1/7	0,1646
CCG	4	1/4	1	1/2	2	1/3	7	1/6	0,0896
CI	1/3	1/3	2	1	5	2	4	1	0,1325
CPI	3	1	1	1	1	1	3	1	0,1327
GTI	4	5	3	1	1	1	7	1/2	0,1967
HI	1/5	1/7	1/7	1/4	1/3	1/7	1	1/8	0,0225
NCSI	8	7	6	1	1	2	1/2	1	0,2086
Оцінки 3-го експерта									
Фактори	GDP	FCI	CCG	CI	CPI	GTI	HI	NCSI	Ваговий коефіцієнт з NCSI
GDP	1	1/6	6	4	1/5	1	9	1/5	0,1033
FCI	6	1	8	5	1/5	1	8	1/7	0,1628
CCG	1/6	1/8	1	2	1	1	7	1/7	0,0663
CI	1/4	1/5	1/2	1	1	1	2	1	0,0679
CPI	5	5	1	1	1	1	4	1	0,1755
GTI	1	1	1	1	1	1	8	1/3	0,1115
HI	1/9	1/8	1/7	1/2	1/4	1/8	1	1/8	0,0208
NCSI	5	7	7	1	1	3	8	1	0,2920

Продовження таблиці Е.2

Оцінки 4-го експерта									
Фактори	GDP	FCI	CCG	CI	CPI	GTI	HI	NCSI	Ваговий коефіцієнт з NCSI
GDP	1	1	1	1	1/6	1	9	1/4	0,0868
FCI	1	1	7	9	2	1/5	9	1/7	0,1515
CCG	1	1/7	1	5	1	1	9	1/6	0,0990
CI	1	1/9	1/5	1	1	1	9	1	0,0802
CPI	6	1/2	1	1	1	1	9	1	0,1481
GTI	1	5	1	1	1	1	9	1/4	0,1328
HI	1/9	1/9	1/9	1/9	1/9	1/9	1	1/8	0,0146
NCSI	4	7	6	1	1	4	8	1	0,2871
Оцінки 5-го експерта									
Фактори	GDP	FCI	CCG	CI	CPI	GTI	HI	NCSI	Ваговий коефіцієнт з NCSI
GDP	1	1/7	3	1/5	1/6	5	7	1/5	0,0715
FCI	7	1	6	4	3	2	7	1/7	0,2263
CCG	1/3	1/6	1	1/5	4	1/5	5	1/6	0,0516
CI	5	1/4	5	1	3	2	1	1/2	0,1375
CPI	6	1/3	1/4	1/3	1	1	8	1	0,0988
GTI	1/5	1/2	5	1/2	1	1	8	1/3	0,0906
HI	1/7	1/7	1/5	1	1/8	1/8	1	1/8	0,0220
NCSI	5	7	6	2	1	3	8	1	0,3017
Оцінки 6-го експерта									
Фактори	GDP	FCI	CCG	CI	CPI	GTI	HI	NCSI	Ваговий коефіцієнт з NCSI
GDP	1	1/9	1	1/5	1/9	1/9	1	1/5	0,0265
FCI	9	1	9	6	3	1/3	3	1/7	0,1757
CCG	1	1/9	1	1/5	1/5	1/5	1	1/7	0,0294
CI	5	1/6	5	1	1/3	1/3	3	1	0,0939
CPI	9	1/3	5	3	1	1	3	1	0,1665
GTI	9	3	5	3	1	1	5	1/3	0,2036
HI	1	1/3	1	1/3	1/3	1/5	1	1/8	0,0377
NCSI	5	7	7	1	1	3	8	1	0,2668

Продовження таблиці Е.2

Оцінки 7-го експерта									
Фактори	GDP	FCI	CCG	CI	CPI	GTI	HI	NCSI	Ваговий коефіцієнт з NCSI
GDP	1	1/7	2	1/5	1/5	5	3	1/5	0,06334
FCI	7	1	7	2	3	2	5	1/7	0,20543
CCG	1/2	1/7	1	1	1/5	1/5	3	1/7	0,04176
CI	5	1/2	1	1	1/5	1/5	3	1	0,08306
CPI	5	1/3	5	5	1	1	3	1	0,17655
GTI	1/5	1/2	5	5	1	1	5	1/3	0,11541
HI	1/3	1/5	1/3	1/3	1/3	1/5	1	1/8	0,02875
NCSI	5	7	7	1	1	3	8	1	0,28571

Таблиця Е.3 – Результати експертних оцінок щодо переваг одних факторів над іншими

Фактори	1 експерт	2 експерт	3 експерт	4 експерт	5 експерт	6 експерт	7 експерт	Середньо-зважене вагових коефіцієнтів
GDP	0,0398	0,0527	0,1033	0,0868	0,0715	0,0265	0,0633	0,0634
FCI	0,1906	0,1646	0,1628	0,1515	0,2263	0,1757	0,2054	0,1824
CCG	0,0624	0,0896	0,0663	0,0990	0,0516	0,0294	0,0418	0,0629
CI	0,0427	0,1325	0,0679	0,0802	0,1375	0,0939	0,0831	0,0911
CPI	0,2242	0,1327	0,1755	0,1481	0,0988	0,1665	0,1766	0,1603
GTI	0,1424	0,1967	0,1115	0,1328	0,0906	0,2036	0,1154	0,1419
HI	0,0278	0,0225	0,0208	0,0146	0,0220	0,0377	0,0287	0,0248
NCSI	0,2702	0,2086	0,2920	0,2871	0,3017	0,2668	0,2857	0,2732

Таблиця Е.4 – Результати розрахунків інтегральних показників

Країна	IRA(x_8)	Країна	IRA(x_8)
Australia	0,2341	Lithuania	0,1551
Austria	0,2013	Luxembourg	0,2339
Bahrain	0,3725	Malaysia	0,2740
Belgium	0,2344	Malta	0,2138
Bolivia	0,2689	Mauritius	0,2109
Botswana	0,2427	Mexico	0,3128
Brazil	0,2560	Montenegro	0,2106
Bulgaria	0,2046	Netherlands	0,2338
Canada	0,2627	New Zealand	0,1744
Chile	0,2457	Macedonia	0,2262
China	0,3449	Norway	0,1791
Costa Rica	0,1961	Panama	0,2732
Croatia	0,1655	Paraguay	0,2973
Cyprus	0,2429	Philippines	0,3665
Czech Republic	0,1886	Poland	0,1948
Denmark	0,1572	Portugal	0,1650
Dominican Republic	0,2531	Romania	0,1870
Estonia	0,1402	Russian Federation	0,3354
Finland	0,1859	Saudi Arabia	0,2888
France	0,2769	Singapore	0,2135
Germany	0,2967	Slovakia	0,1692
Ghana	0,2473	Slovenia	0,1521
Greece	0,2477	South Africa	0,3537
Guatemala	0,2810	Spain	0,2395
Hungary	0,1913	Sweden	0,2465
Iceland	0,1646	Switzerland	0,2355
India	0,3411	Tanzania	0,4955
Indonesia	0,3232	Thailand	0,3755
Ireland	0,2548	Trinidad and Tobago	0,2702
Israel	0,2679	Turkey	0,3262
Italy	0,2384	Ukraine	0,3252
Japan	0,2115	United Kingdom	0,2735
Kenya	0,4215	United States	0,3510
Korea	0,2025	Uruguay	0,1963
Latvia	0,1887	Venezuela	0,3497
Liberia	0,3817	X	X

Таблиця Е.5 – Розрахунок рівня привабливості країни для легалізації кримінальних доходів іншою країною

Назва країни	Australia	Austria	Bahrain	Belgium	Bolivia	Botswana	Brazil	Bulgaria	Canada	Chile	China	Costa Rica	Croatia	Cyprus	Czech Republic	Denmark	Dominican Republic	Estonia
Australia	–	1,0000	0,4243	1,0000	0,4026	0,4015	0,4047	0,4033	1,0000	0,5211	0,4184	0,4544	0,4186	0,5332	0,8117	0,9100	0,4030	0,9998
Austria	1,0000	–	0,4114	0,9999	0,3956	0,3943	0,3966	0,3944	1,0000	0,4763	0,4071	0,4301	0,4051	0,4850	0,6750	0,9592	0,3955	0,9609
Bahrain	0,4972	0,4701	–	0,5074	0,8114	0,9877	1,0000	0,9994	0,4945	0,6878	1,0000	0,6935	0,7258	0,6452	0,5140	0,4346	0,9930	0,4552
Belgium	1,0000	0,9999	0,4367	–	0,4077	0,4074	0,4120	0,4137	0,9992	0,5912	0,4288	0,4900	0,4365	0,6086	0,9724	0,7664	0,4093	1,0000
Bolivia	0,4098	0,4029	0,6278	0,4110	–	0,9485	0,7459	0,4382	0,4128	0,4258	0,7202	0,4169	0,4118	0,4229	0,4056	0,3934	0,9041	0,3940
Botswana	0,4229	0,4126	0,9456	0,4256	0,9894	–	1,0000	0,5461	0,4246	0,4650	0,9986	0,4552	0,4518	0,4565	0,4221	0,3990	1,0000	0,4031
Brazil	0,4380	0,4242	1,0000	0,4423	0,8840	1,0000	–	0,7219	0,4387	0,5124	1,0000	0,5040	0,5059	0,4963	0,4410	0,4060	1,0000	0,4137
Bulgaria	0,4723	0,4473	0,9936	0,4842	0,5322	0,6373	0,7814	–	0,4649	0,7842	0,9221	0,8553	0,9571	0,7016	0,5058	0,4162	0,6562	0,4415
Canada	1,0000	1,0000	0,4199	0,9988	0,4019	0,3999	0,4025	0,3989	–	0,4885	0,4151	0,4384	0,4107	0,4980	0,6767	0,9986	0,4013	0,9284
Chile	0,6578	0,5726	0,6315	0,7147	0,4604	0,4805	0,5119	0,7102	0,6020	–	0,5768	1,0000	0,9769	1,0000	0,9015	0,4732	0,4871	0,6148
China	0,4717	0,4508	1,0000	0,4788	0,8823	0,9999	1,0000	0,9206	0,4714	0,5972	–	0,5906	0,6011	0,5697	0,4796	0,4232	1,0000	0,4366
Costa Rica	0,5559	0,5018	0,6579	0,5907	0,4549	0,4800	0,5175	0,8360	0,5249	1,0000	0,5892	–	1,0000	1,0000	0,7116	0,4397	0,4870	0,5170
Croatia	0,4944	0,4600	0,7253	0,5146	0,4566	0,4908	0,5412	0,9907	0,4778	0,9964	0,6296	1,0000	–	0,9426	0,5744	0,4196	0,4989	0,4630
Cyprus	0,6852	0,5903	0,6019	0,7496	0,4538	0,4705	0,4973	0,6499	0,6197	1,0000	0,5550	1,0000	0,9203	–	0,9472	0,4797	0,4763	0,6465
Czech Rep.	0,9364	0,7733	0,4582	0,9923	0,4118	0,4146	0,4224	0,4401	0,7825	0,8513	0,4447	0,6239	0,4929	0,8761	–	0,5316	0,4170	0,9802
Denmark	0,8986	0,9224	0,3905	0,6763	0,3840	0,3825	0,3834	0,3805	0,9946	0,4107	0,3888	0,3940	0,3845	0,4141	0,4595	–	0,3832	0,5265
Dominican Republic	0,4274	0,4162	0,9746	0,4304	0,9797	1,0000	1,0000	0,5767	0,4290	0,4759	0,9999	0,4658	0,4629	0,4660	0,4271	0,4013	–	0,4061
Estonia	1,0000	0,9779	0,4124	1,0000	0,3930	0,3930	0,3961	0,3982	0,9566	0,5297	0,4070	0,4526	0,4142	0,5433	0,9590	0,5990	0,3942	–
Finland	0,9710	0,9833	0,3961	0,7697	0,3877	0,3860	0,3871	0,3837	0,9999	0,4229	0,3939	0,4012	0,3889	0,4272	0,4890	1,0000	0,3868	0,5845
France	1,0000	0,9998	0,4528	1,0000	0,4164	0,4162	0,4220	0,4253	0,9990	0,6490	0,4427	0,5231	0,4546	0,6696	0,9952	0,7829	0,4185	1,0000
Germany	1,0000	1,0000	0,4236	0,9964	0,4049	0,4025	0,4052	0,4007	1,0000	0,4921	0,4186	0,4413	0,4129	0,5018	0,6710	1,0000	0,4041	0,9039
Ghana	0,4104	0,4032	0,6814	0,4118	1,0000	0,9958	0,8433	0,4504	0,4130	0,4301	0,7981	0,4213	0,4165	0,4265	0,4070	0,3933	0,9789	0,3945
Greece	0,5237	0,4843	0,9332	0,5445	0,5226	0,5942	0,6931	1,0000	0,5079	0,9741	0,8256	0,9988	1,0000	0,9043	0,5944	0,4361	0,6090	0,4820

Продовження таблиці Е.5

Назва країни	Australia	Austria	Bahrain	Belgium	Bolivia	Botswana	Brazil	Bulgaria	Canada	Chile	China	Costa Rica	Croatia	Cyprus	Czech Republic	Denmark	Dominican Republic	Estonia
Guatemala	0,4175	0,4090	0,7383	0,4192	1,0000	0,9996	0,9055	0,4682	0,4204	0,4417	0,8603	0,4314	0,4260	0,4372	0,4138	0,3974	0,9951	0,3991
Hungary	0,4886	0,4577	0,8860	0,5051	0,4896	0,5487	0,6344	1,0000	0,4763	0,9368	0,7612	0,9931	1,0000	0,8380	0,5448	0,4204	0,5611	0,4558
Iceland	1,0000	1,0000	0,4016	0,9947	0,3897	0,3885	0,3903	0,3881	1,0000	0,4489	0,3984	0,4147	0,3961	0,4554	0,5933	0,9669	0,3895	0,8666
India	0,4235	0,4141	0,7201	0,4251	1,0000	0,9935	0,8605	0,4670	0,4271	0,4465	0,8281	0,4349	0,4284	0,4423	0,4184	0,4015	0,9771	0,4026
Indonesia	0,4661	0,4462	1,0000	0,4729	0,8615	0,9997	1,0000	0,9170	0,4658	0,5876	1,0000	0,5817	0,5926	0,5607	0,4739	0,4201	0,9999	0,4329
Ireland	1,0000	1,0000	0,4178	0,9978	0,4006	0,3987	0,4012	0,3976	1,0000	0,4828	0,4132	0,4352	0,4088	0,4919	0,6617	0,9989	0,4001	0,9125
Israel	0,8519	0,7149	0,5443	0,9290	0,4440	0,4530	0,4706	0,5351	0,7415	1,0000	0,5141	0,9370	0,6865	1,0000	1,0000	0,5310	0,4576	0,8529
Italy	0,7808	0,6546	0,5415	0,8638	0,4395	0,4494	0,4673	0,5416	0,6822	1,0000	0,5102	0,9672	0,7140	1,0000	0,9995	0,5030	0,4538	0,7675
Japan	1,0000	1,0000	0,4275	1,0000	0,4028	0,4023	0,4062	0,4070	0,9997	0,5550	0,4207	0,4703	0,4259	0,5699	0,9311	0,7676	0,4040	1,0000
Kenya	0,4255	0,4163	0,6467	0,4267	1,0000	0,9037	0,7329	0,4493	0,4302	0,4419	0,7254	0,4296	0,4223	0,4390	0,4183	0,4039	0,8652	0,4034
Korea	0,8378	0,6881	0,4880	0,9293	0,4216	0,4269	0,4383	0,4744	0,7091	0,9871	0,4681	0,7862	0,5678	0,9926	1,0000	0,5072	0,4301	0,8608
Latvia	0,6378	0,5522	0,5451	0,7004	0,4331	0,4452	0,4650	0,5762	0,5769	1,0000	0,5091	0,9998	0,8267	1,0000	0,9263	0,4581	0,4496	0,6061
Liberia	0,4024	0,3975	0,4728	0,4025	0,8547	0,5384	0,4852	0,4004	0,4065	0,4048	0,4953	0,3975	0,3930	0,4043	0,3959	0,3909	0,5277	0,3886
Lithuania	0,6251	0,5388	0,4992	0,6925	0,4182	0,4265	0,4406	0,5109	0,5602	1,0000	0,4734	0,9779	0,6888	1,0000	0,9496	0,4483	0,4298	0,6024
Luxembourg	1,0000	1,0000	0,4129	0,9936	0,3976	0,3958	0,3980	0,3945	1,0000	0,4706	0,4088	0,4281	0,4046	0,4787	0,6304	0,9991	0,3970	0,8755
Malaysia	0,5494	0,5031	0,9213	0,5744	0,5286	0,5966	0,6895	1,0000	0,5297	0,9944	0,8178	1,0000	1,0000	0,9547	0,6373	0,4464	0,6111	0,5027
Malta	1,0000	0,9886	0,4395	1,0000	0,4075	0,4079	0,4130	0,4176	0,9795	0,6341	0,4306	0,5096	0,4448	0,6545	0,9989	0,6684	0,4098	1,0000
Mauritius	0,5214	0,4806	0,8136	0,5446	0,4841	0,5303	0,5969	0,9997	0,5025	0,9971	0,7056	1,0000	1,0000	0,9567	0,6094	0,4319	0,5409	0,4829
Mexico	0,4554	0,4381	1,0000	0,4609	0,9105	1,0000	1,0000	0,8049	0,4559	0,5502	1,0000	0,5409	0,5446	0,5298	0,4597	0,4152	1,0000	0,4253
Montenegro	0,4601	0,4390	1,0000	0,4692	0,5749	0,7354	0,9157	1,0000	0,4554	0,6779	0,9926	0,7139	0,7935	0,6209	0,4817	0,4124	0,7598	0,4314
Netherlands	0,9995	0,9999	0,4063	0,9067	0,3943	0,3923	0,3939	0,3898	1,0000	0,4465	0,4031	0,4150	0,3974	0,4527	0,5487	1,0000	0,3933	0,7019
New Zealand	0,9993	0,9999	0,3975	0,8732	0,3881	0,3866	0,3879	0,3849	1,0000	0,4300	0,3950	0,4049	0,3909	0,4350	0,5161	1,0000	0,3874	0,6598
North Macedonia	0,4471	0,4303	1,0000	0,4535	0,6812	0,9355	0,9999	0,9872	0,4455	0,5753	1,0000	0,5792	0,6036	0,5445	0,4576	0,4084	0,9539	0,4210
Norway	0,8708	0,8930	0,3924	0,6657	0,3856	0,3839	0,3847	0,3814	0,9859	0,4129	0,3906	0,3955	0,3855	0,4164	0,4610	1,0000	0,3846	0,5225

Продовження таблиці Е.5

Назва країни	Australia	Austria	Bahrain	Belgium	Bolivia	Botswana	Brazil	Bulgaria	Canada	Chile	China	Costa Rica	Croatia	Cyprus	Czech Republic	Denmark	Dominican Republic	Estonia
Panama	0,5250	0,4865	0,9799	0,5445	0,5532	0,6465	0,7682	1,0000	0,5111	0,9466	0,9005	0,9893	1,0000	0,8691	0,5863	0,4386	0,6643	0,4815
Paraguay	0,4379	0,4247	0,9875	0,4415	0,9889	1,0000	1,0000	0,6115	0,4397	0,4948	1,0000	0,4832	0,4799	0,4833	0,4377	0,4072	1,0000	0,4130
Philippines	0,4466	0,4323	0,9681	0,4502	0,9999	1,0000	1,0000	0,5916	0,4495	0,5009	0,9991	0,4867	0,4809	0,4903	0,4445	0,4130	1,0000	0,4182
Poland	0,6291	0,5477	0,5620	0,6874	0,4375	0,4513	0,4735	0,6061	0,5727	1,0000	0,5217	1,0000	0,8825	1,0000	0,9013	0,4572	0,4561	0,5944
Portugal	0,9541	0,7854	0,4411	0,9977	0,4045	0,4063	0,4124	0,4244	0,7880	0,7519	0,4305	0,5604	0,4632	0,7783	1,0000	0,5270	0,4083	0,9947
Romania	0,4845	0,4548	0,8893	0,5003	0,4885	0,5481	0,6350	1,0000	0,4728	0,9242	0,7629	0,9890	1,0000	0,8222	0,5378	0,4188	0,5606	0,4526
Russian Federation	0,4454	0,4310	0,9890	0,4493	0,9960	1,0000	1,0000	0,6247	0,4476	0,5063	1,0000	0,4933	0,4892	0,4941	0,4448	0,4116	1,0000	0,4178
Saudi Arabia	0,4369	0,4239	0,9903	0,4405	0,9829	1,0000	1,0000	0,6169	0,4386	0,4946	1,0000	0,4834	0,4805	0,4829	0,4370	0,4065	1,0000	0,4124
Singapore	1,0000	1,0000	0,4149	1,0000	0,3977	0,3963	0,3989	0,3967	1,0000	0,4869	0,4103	0,4360	0,4085	0,4964	0,7058	0,9550	0,3976	0,9794
Slovakia	0,6011	0,5268	0,5366	0,6559	0,4281	0,4400	0,4591	0,5744	0,5492	1,0000	0,5012	1,0000	0,8406	1,0000	0,8752	0,4462	0,4441	0,5699
Slovenia	0,9140	0,7335	0,4388	0,9886	0,4027	0,4047	0,4107	0,4237	0,7402	0,7692	0,4283	0,5659	0,4638	0,7962	1,0000	0,5064	0,4066	0,9749
South Africa	0,4511	0,4355	0,9947	0,4553	0,9951	1,0000	1,0000	0,6516	0,4532	0,5181	1,0000	0,5046	0,5007	0,5046	0,4508	0,4147	1,0000	0,4215
Spain	0,9995	0,9492	0,4604	1,0000	0,4167	0,4181	0,4253	0,4358	0,9422	0,7536	0,4481	0,5755	0,4771	0,7785	1,0000	0,6341	0,4206	1,0000
Sweden	0,9793	0,9877	0,4040	0,8123	0,3935	0,3912	0,3926	0,3880	0,9999	0,4368	0,4012	0,4099	0,3945	0,4422	0,5153	1,0000	0,3922	0,6200
Switzerland	0,9870	0,9933	0,4034	0,8278	0,3929	0,3907	0,3921	0,3878	1,0000	0,4368	0,4006	0,4097	0,3943	0,4422	0,5181	1,0000	0,3917	0,6307
Tanzania	0,4227	0,4145	0,5715	0,4234	0,9995	0,7315	0,6119	0,4296	0,4283	0,4316	0,6211	0,4199	0,4127	0,4300	0,4140	0,4034	0,7042	0,4013
Thailand	0,4755	0,4541	1,0000	0,4824	0,9285	1,0000	1,0000	0,8852	0,4758	0,5945	1,0000	0,5851	0,5916	0,5691	0,4818	0,4259	1,0000	0,4388
Trinidad and Tobago	0,4584	0,4395	1,0000	0,4653	0,7523	0,9806	1,0000	0,9765	0,4570	0,5918	1,0000	0,5925	0,6131	0,5608	0,4688	0,4148	0,9887	0,4284
Turkey	0,4351	0,4230	0,9223	0,4380	1,0000	1,0000	0,9994	0,5453	0,4379	0,4784	0,9915	0,4656	0,4599	0,4700	0,4325	0,4067	1,0000	0,4107
Ukraine	0,4596	0,4414	1,0000	0,4654	0,9129	1,0000	1,0000	0,8259	0,4600	0,5598	1,0000	0,5506	0,5549	0,5382	0,4644	0,4174	1,0000	0,4281
United Kingdom	1,0000	1,0000	0,4203	0,9969	0,4025	0,4003	0,4029	0,3989	1,0000	0,4865	0,4155	0,4377	0,4105	0,4958	0,6642	0,9998	0,4018	0,9057
United States	1,0000	1,0000	0,4635	1,0000	0,4247	0,4237	0,4298	0,4303	1,0000	0,6468	0,4529	0,5270	0,4596	0,6667	0,9797	0,9109	0,4263	1,0000
Uruguay	0,5715	0,5117	0,6300	0,6110	0,4503	0,4720	0,5048	0,7660	0,5354	1,0000	0,5697	1,0000	0,9992	1,0000	0,7543	0,4437	0,4783	0,5324
Venezuela	0,3980	0,3938	0,4551	0,3980	0,7743	0,5057	0,4638	0,3951	0,4016	0,3994	0,4730	0,3931	0,3892	0,3991	0,3921	0,3881	0,4976	0,3859

Продовження таблиці Е.5

Назва країни	Finland	France	Germany	Ghana	Greece	Guatemala	Hungary	Iceland	India	Indonesia	Ireland	Israel	Italy	Japan	Kenya	Korea	Latvia	Liberia
Australia	0,9629	1,0000	1,0000	0,4003	0,4248	0,4049	0,4114	1,0000	0,4123	0,4153	1,0000	0,7085	0,6346	1,0000	0,4218	0,7151	0,5112	0,4131
Austria	0,9903	0,9995	1,0000	0,3937	0,4102	0,3973	0,4002	1,0000	0,4032	0,4047	1,0000	0,6060	0,5522	1,0000	0,4110	0,6036	0,4680	0,4045
Bahrain	0,4479	0,5338	0,5075	0,8413	0,9050	0,8898	0,8494	0,4503	0,8971	1,0000	0,4902	0,6215	0,6107	0,4905	0,8967	0,5544	0,5901	0,6633
Belgium	0,8408	1,0000	0,9986	0,4053	0,4424	0,4107	0,4248	0,9980	0,4190	0,4251	0,9986	0,8627	0,7714	1,0000	0,4295	0,8918	0,5827	0,4181
Bolivia	0,3983	0,4190	0,4182	1,0000	0,4371	1,0000	0,4217	0,3963	1,0000	0,6962	0,4113	0,4253	0,4200	0,4064	1,0000	0,4107	0,4107	0,9561
Botswana	0,4051	0,4366	0,4310	0,9992	0,5078	1,0000	0,4777	0,4041	0,9995	0,9969	0,4227	0,4558	0,4491	0,4190	0,9962	0,4324	0,4369	0,7125
Brazil	0,4135	0,4567	0,4465	0,9304	0,6045	0,9662	0,5570	0,4133	0,9583	1,0000	0,4363	0,4910	0,4830	0,4336	0,9418	0,4576	0,4683	0,6480
Bulgaria	0,4263	0,5076	0,4742	0,5387	1,0000	0,5684	0,9999	0,4314	0,5863	0,9155	0,4614	0,6409	0,6395	0,4687	0,6014	0,5627	0,6388	0,4934
Canada	1,0000	0,9972	1,0000	0,3994	0,4172	0,4038	0,4056	1,0000	0,4112	0,4122	1,0000	0,6190	0,5650	0,9993	0,4208	0,6113	0,4784	0,4135
Chile	0,4965	0,7725	0,6171	0,4585	0,8910	0,4728	0,8198	0,5304	0,4887	0,5666	0,5932	1,0000	1,0000	0,6652	0,5064	0,9983	1,0000	0,4608
China	0,4341	0,4999	0,4825	0,9184	0,7527	0,9552	0,6884	0,4348	0,9532	1,0000	0,4679	0,5578	0,5472	0,4656	0,9447	0,5070	0,5272	0,6877
Costa Rica	0,4554	0,6349	0,5369	0,4541	0,9820	0,4681	0,9495	0,4739	0,4823	0,5790	0,5188	0,9785	0,9903	0,5572	0,4977	0,8987	0,9996	0,4508
Croatia	0,4308	0,5450	0,4873	0,4569	1,0000	0,4719	1,0000	0,4409	0,4853	0,6189	0,4737	0,8195	0,8412	0,4931	0,4991	0,6982	0,8931	0,4470
Cyprus	0,5046	0,8091	0,6348	0,4517	0,8226	0,4649	0,7458	0,5444	0,4799	0,5456	0,6102	1,0000	1,0000	0,6958	0,4970	1,0000	1,0000	0,4560
Czech Republic	0,5711	0,9987	0,7895	0,4097	0,4896	0,4159	0,4610	0,6946	0,4246	0,4403	0,7677	1,0000	0,9998	0,9676	0,4352	1,0000	0,8737	0,4189
Denmark	1,0000	0,6787	0,9999	0,3828	0,3876	0,3848	0,3830	0,9502	0,3884	0,3875	0,9956	0,4499	0,4327	0,6751	0,3932	0,4424	0,4062	0,3906
Dominican Republic	0,4078	0,4424	0,4359	0,9967	0,5271	0,9996	0,4932	0,4069	0,9983	0,9997	0,4269	0,4646	0,4574	0,4233	0,9925	0,4388	0,4444	0,7059
Estonia	0,6590	1,0000	0,9487	0,3915	0,4175	0,3949	0,4058	0,9248	0,4001	0,4047	0,9457	0,7952	0,6956	1,0000	0,4067	0,8426	0,5251	0,3991
Finland	–	0,7687	1,0000	0,3862	0,3928	0,3887	0,3869	0,9943	0,3931	0,3922	0,9999	0,4747	0,4521	0,7703	0,3989	0,4658	0,4172	0,3956
France	0,8544	–	0,9985	0,4134	0,4613	0,4200	0,4394	0,9969	0,4300	0,4383	0,9983	0,9303	0,8513	1,0000	0,4427	0,9548	0,6408	0,4284
Germany	1,0000	0,9940	–	0,4022	0,4200	0,4069	0,4077	1,0000	0,4150	0,4155	1,0000	0,6200	0,5670	0,9973	0,4255	0,6096	0,4813	0,4179
Ghana	0,3982	0,4201	0,4184	–	0,4455	1,0000	0,4282	0,3965	1,0000	0,7721	0,4116	0,4284	0,4230	0,4071	1,0000	0,4128	0,4135	0,8828
Greece	0,4504	0,5792	0,5203	0,5252	–	0,5514	1,0000	0,4607	0,5716	0,8140	0,5028	0,8107	0,8200	0,5203	0,5908	0,6999	0,8440	0,4981
Guatemala	0,4031	0,4288	0,4266	1,0000	0,4609	–	0,4403	0,4012	1,0000	0,8356	0,4187	0,4392	0,4329	0,4136	1,0000	0,4207	0,4218	0,8943

Продовження таблиці Е.5

Назва країни	Finland	France	Germany	Ghana	Greece	Guatemala	Hungary	Iceland	India	Indonesia	Ireland	Israel	Italy	Japan	Kenya	Korea	Latvia	Liberia
Hungary	0,4315	0,5330	0,4861	0,4918	1,0000	0,5130	–	0,4394	0,5294	0,7494	0,4723	0,7367	0,7455	0,4859	0,5452	0,6333	0,7694	0,4697
Iceland	0,9940	0,9884	1,0000	0,3882	0,4002	0,3910	0,3926	–	0,3957	0,3966	1,0000	0,5446	0,5041	0,9967	0,4019	0,5402	0,4422	0,3970
India	0,4079	0,4358	0,4342	1,0000	0,4636	1,0000	0,4424	0,4055	–	0,8032	0,4252	0,4452	0,4382	0,4190	1,0000	0,4254	0,4258	0,9665
Indonesia	0,4304	0,4930	0,4762	0,8998	0,7425	0,9415	0,6789	0,4311	0,9397	–	0,4624	0,5489	0,5388	0,4604	0,9304	0,5002	0,5199	0,6688
Ireland	1,0000	0,9954	1,0000	0,3983	0,4151	0,4025	0,4040	1,0000	0,4096	0,4104	–	0,6072	0,5555	0,9985	0,4188	0,5992	0,4731	0,4118
Israel	0,5678	0,9653	0,7553	0,4411	0,6488	0,4523	0,5883	0,6477	0,4665	0,5062	0,7286	–	1,0000	0,8768	0,4832	1,0000	1,0000	0,4512
Italy	0,5337	0,9166	0,6965	0,4371	0,6625	0,4477	0,5996	0,5962	0,4609	0,5026	0,6705	1,0000	–	0,8031	0,4764	1,0000	1,0000	0,4451
Japan	0,8439	1,0000	0,9992	0,4006	0,4313	0,4053	0,4164	0,9993	0,4127	0,4175	0,9993	0,8011	0,7109	–	0,4220	0,8272	0,5465	0,4122
Kenya	0,4106	0,4375	0,4378	1,0000	0,4522	1,0000	0,4334	0,4073	1,0000	0,7023	0,4283	0,4432	0,4359	0,4206	–	0,4243	0,4232	0,9998
Korea	0,5399	0,9671	0,7206	0,4194	0,5498	0,4272	0,5079	0,6223	0,4375	0,4625	0,6961	1,0000	1,0000	0,8711	0,4499	–	0,9961	0,4280
Latvia	0,4786	0,7596	0,5897	0,4314	0,7263	0,4414	0,6542	0,5130	0,4530	0,5017	0,5685	1,0000	1,0000	0,6489	0,4664	1,0000	–	0,4353
Liberia	0,3951	0,4088	0,4114	0,7206	0,4055	0,7298	0,3970	0,3921	0,8679	0,4856	0,4053	0,4079	0,4035	0,3991	0,9997	0,3981	0,3962	–
Lithuania	0,4669	0,7531	0,5714	0,4167	0,6211	0,4244	0,5645	0,5016	0,4336	0,4677	0,5522	1,0000	1,0000	0,6391	0,4443	1,0000	1,0000	0,4210
Luxembourg	1,0000	0,9893	1,0000	0,3954	0,4103	0,3993	0,4003	1,0000	0,4057	0,4063	1,0000	0,5820	0,5352	0,9954	0,4141	0,5739	0,4617	0,4079
Malaysia	0,4630	0,6140	0,5435	0,5305	1,0000	0,5571	1,0000	0,4759	0,5786	0,8056	0,5238	0,8717	0,8832	0,5462	0,5995	0,7604	0,9109	0,5063
Malta	0,7357	1,0000	0,9764	0,4052	0,4495	0,4106	0,4302	0,9549	0,4188	0,4268	0,9733	0,9387	0,8554	1,0000	0,4290	0,9697	0,6297	0,4167
Mauritius	0,4457	0,5800	0,5140	0,4849	1,0000	0,5044	1,0000	0,4575	0,5213	0,6934	0,4975	0,8560	0,8733	0,5194	0,5384	0,7381	0,9137	0,4704
Mexico	0,4246	0,4786	0,4655	0,9479	0,6657	0,9762	0,6093	0,4245	0,9714	1,0000	0,4530	0,5224	0,5128	0,4499	0,9602	0,4809	0,4949	0,6889
Montenegro	0,4215	0,4894	0,4642	0,5874	0,9763	0,6255	0,9506	0,4249	0,6426	0,9919	0,4523	0,5839	0,5788	0,4561	0,6544	0,5223	0,5694	0,5136
Netherlands	1,0000	0,9004	1,0000	0,3923	0,4025	0,3957	0,3944	1,0000	0,4015	0,4009	1,0000	0,5237	0,4906	0,9099	0,4092	0,5129	0,4388	0,4044
New Zealand	1,0000	0,8631	1,0000	0,3866	0,3948	0,3892	0,3885	1,0000	0,3936	0,3933	1,0000	0,4936	0,4662	0,8786	0,3995	0,4854	0,4241	0,3957
North Macedonia	0,4166	0,4703	0,4536	0,7108	0,7778	0,7646	0,7137	0,4180	0,7734	1,0000	0,4428	0,5281	0,5207	0,4429	0,7726	0,4834	0,5067	0,5592
Norway	1,0000	0,6709	0,9990	0,3842	0,3890	0,3864	0,3840	0,9175	0,3903	0,3892	0,9876	0,4526	0,4351	0,6632	0,3956	0,4444	0,4080	0,3930
Panama	0,4534	0,5788	0,5241	0,5577	1,0000	0,5889	1,0000	0,4627	0,6109	0,8916	0,5060	0,7855	0,7901	0,5208	0,6309	0,6799	0,8033	0,5190

Продовження таблиці Е.5

Назва країни	Finland	France	Germany	Ghana	Greece	Guatemala	Hungary	Iceland	India	Indonesia	Ireland	Israel	Italy	Japan	Kenya	Korea	Latvia	Liberia
Paraguay	0,4149	0,4555	0,4478	0,9986	0,5544	0,9999	0,5153	0,4139	0,9994	0,9999	0,4374	0,4816	0,4732	0,4331	0,9965	0,4514	0,4580	0,7469
Philippines	0,4218	0,4657	0,4587	1,0000	0,5522	1,0000	0,5133	0,4200	1,0000	0,9980	0,4468	0,4903	0,4807	0,4410	1,0000	0,4583	0,4635	0,8468
Poland	0,4774	0,7451	0,5858	0,4358	0,7711	0,4465	0,6951	0,5096	0,4588	0,5138	0,5647	1,0000	1,0000	0,6383	0,4728	0,9995	1,0000	0,4391
Portugal	0,5664	0,9998	0,7925	0,4026	0,4627	0,4078	0,4403	0,7034	0,4151	0,4269	0,7725	0,9998	0,9899	0,9827	0,4241	1,0000	0,7676	0,4110
Romania	0,4295	0,5272	0,4823	0,4908	1,0000	0,5119	1,0000	0,4371	0,5280	0,7512	0,4689	0,7231	0,7311	0,4818	0,5435	0,6224	0,7531	0,4683
Russian Federation	0,4202	0,4647	0,4566	0,9998	0,5683	1,0000	0,5266	0,4189	0,9999	0,9999	0,4450	0,4926	0,4833	0,4401	0,9990	0,4597	0,4665	0,7875
Saudi Arabia	0,4141	0,4544	0,4466	0,9971	0,5561	0,9996	0,5167	0,4132	0,9986	1,0000	0,4363	0,4809	0,4726	0,4322	0,9943	0,4508	0,4576	0,7324
Singapore	0,9882	0,9999	1,0000	0,3956	0,4140	0,3995	0,4031	1,0000	0,4059	0,4077	1,0000	0,6294	0,5708	1,0000	0,4142	0,6281	0,4780	0,4072
Slovakia	0,4640	0,7113	0,5610	0,4266	0,7276	0,4360	0,6551	0,4927	0,4467	0,4943	0,5419	1,0000	1,0000	0,6098	0,4589	0,9991	1,0000	0,4296
Slovenia	0,5409	0,9979	0,7462	0,4010	0,4621	0,4059	0,4398	0,6569	0,4128	0,4248	0,7253	1,0000	0,9961	0,9550	0,4213	1,0000	0,7902	0,4085
South Africa	0,4238	0,4718	0,4628	0,9996	0,5871	1,0000	0,5421	0,4226	0,9998	1,0000	0,4504	0,5026	0,4928	0,4454	0,9988	0,4671	0,4749	0,7932
Spain	0,6940	1,0000	0,9417	0,4140	0,4801	0,4208	0,4538	0,8869	0,4306	0,4434	0,9318	0,9970	0,9728	1,0000	0,4429	0,9999	0,7577	0,4265
Sweden	1,0000	0,8137	1,0000	0,3915	0,3995	0,3948	0,3921	0,9950	0,4004	0,3992	0,9999	0,4996	0,4723	0,8117	0,4080	0,4881	0,4296	0,4039
Switzerland	1,0000	0,8272	1,0000	0,3910	0,3992	0,3941	0,3919	0,9981	0,3997	0,3986	1,0000	0,5009	0,4731	0,8283	0,4070	0,4899	0,4297	0,4029
Tanzania	0,4099	0,4334	0,4358	0,9729	0,4361	0,9723	0,4207	0,4059	0,9992	0,6032	0,4264	0,4350	0,4281	0,4178	1,0000	0,4184	0,4162	1,0000
Thailand	0,4373	0,5040	0,4873	0,9586	0,7345	0,9819	0,6711	0,4375	0,9791	1,0000	0,4722	0,5591	0,5478	0,4689	0,9716	0,5084	0,5267	0,7262
Trinidad and Tobago	0,4242	0,4842	0,4664	0,7871	0,7826	0,8418	0,7179	0,4255	0,8471	1,0000	0,4539	0,5450	0,5363	0,4534	0,8429	0,4964	0,5199	0,6024
Turkey	0,4142	0,4512	0,4459	1,0000	0,5179	1,0000	0,4857	0,4125	1,0000	0,9860	0,4356	0,4706	0,4624	0,4302	1,0000	0,4438	0,4475	0,8399
Ukraine	0,4272	0,4840	0,4700	0,9489	0,6816	0,9766	0,6233	0,4272	0,9723	1,0000	0,4570	0,5303	0,5203	0,4539	0,9620	0,4867	0,5017	0,6958
United Kingdom	1,0000	0,9944	1,0000	0,4000	0,4171	0,4044	0,4056	1,0000	0,4119	0,4126	1,0000	0,6118	0,5598	0,9978	0,4217	0,6026	0,4763	0,4145
United States	0,9593	1,0000	1,0000	0,4211	0,4686	0,4287	0,4451	1,0000	0,4405	0,4478	1,0000	0,9047	0,8260	1,0000	0,4556	0,9214	0,6344	0,4401
Uruguay	0,4604	0,6587	0,5478	0,4491	0,9462	0,4623	0,8900	0,4816	0,4760	0,5601	0,5289	0,9938	0,9985	0,5742	0,4911	0,9438	1,0000	0,4478
Venezuela	0,3918	0,4034	0,4060	0,6523	0,3997	0,6621	0,3925	0,3890	0,7928	0,4651	0,4006	0,4023	0,3985	0,3951	0,9943	0,3939	0,3921	1,0000

Продовження таблиці Е.5

Назва країни	Lithuania	Luxembourg	Malaysia	Malta	Mauritius	Mexico	Montenegro	Netherlands	New Zealand	North Macedonia	Norway	Panama	Paraguay	Philippines	Poland	Portugal	Romania	Russian Federation
Australia	0,5154	1,0000	0,4383	0,9999	0,4287	0,4130	0,4030	0,9991	0,9983	0,4022	0,9214	0,4237	0,4091	0,4182	0,5003	0,8538	0,4096	0,4143
Austria	0,4688	1,0000	0,4200	0,9834	0,4127	0,4030	0,3944	1,0000	1,0000	0,3943	0,9639	0,4095	0,4003	0,4075	0,4612	0,7041	0,3990	0,4044
Bahrain	0,5477	0,4793	0,9214	0,5054	0,8094	1,0000	1,0000	0,4729	0,4479	1,0000	0,4432	0,9784	0,9971	0,9971	0,5998	0,4920	0,8543	0,9984
Belgium	0,5996	0,9954	0,4615	1,0000	0,4496	0,4218	0,4126	0,9580	0,9324	0,4098	0,7877	0,4407	0,4165	0,4269	0,5626	0,9926	0,4225	0,4226
Bolivia	0,4027	0,4076	0,4442	0,4082	0,4245	0,7661	0,4717	0,4068	0,3971	0,5348	0,3969	0,4492	0,9305	0,9989	0,4122	0,4005	0,4208	0,9671
Botswana	0,4237	0,4179	0,5209	0,4230	0,4774	1,0000	0,6742	0,4160	0,4042	0,8447	0,4031	0,5445	1,0000	1,0000	0,4397	0,4144	0,4770	1,0000
Brazil	0,4487	0,4302	0,6240	0,4399	0,5484	1,0000	0,9370	0,4273	0,4129	0,9987	0,4110	0,6785	1,0000	1,0000	0,4726	0,4303	0,5572	1,0000
Bulgaria	0,5840	0,4526	1,0000	0,4865	0,9918	0,8414	1,0000	0,4460	0,4275	0,9522	0,4223	1,0000	0,6969	0,7239	0,6529	0,4828	1,0000	0,7256
Canada	0,4776	1,0000	0,4282	0,9671	0,4196	0,4102	0,3991	1,0000	1,0000	0,3995	0,9987	0,4164	0,4072	0,4160	0,4717	0,6986	0,4041	0,4122
Chile	1,0000	0,5713	0,9757	0,7554	0,9797	0,5435	0,6439	0,5457	0,5074	0,5352	0,4853	0,8706	0,5073	0,5308	1,0000	0,8338	0,8039	0,5236
China	0,4965	0,4590	0,7765	0,4760	0,6675	1,0000	0,9997	0,4545	0,4336	1,0000	0,4304	0,8531	1,0000	1,0000	0,5341	0,4630	0,6901	1,0000
Costa Rica	0,9944	0,5039	0,9999	0,6124	1,0000	0,5505	0,7266	0,4884	0,4613	0,5537	0,4483	0,9701	0,5071	0,5292	0,9999	0,6503	0,9380	0,5233
Croatia	0,8141	0,4633	1,0000	0,5245	1,0000	0,5793	0,8961	0,4537	0,4339	0,6039	0,4260	1,0000	0,5209	0,5428	0,9123	0,5365	1,0000	0,5383
Cyprus	1,0000	0,5866	0,9310	0,7976	0,9324	0,5259	0,5992	0,5578	0,5175	0,5150	0,4924	0,8022	0,4948	0,5168	1,0000	0,8891	0,7307	0,5098
Czech Republic	0,9497	0,7306	0,5284	0,9999	0,5129	0,4347	0,4346	0,6625	0,6105	0,4230	0,5477	0,4854	0,4255	0,4371	0,8152	1,0000	0,4569	0,4327
Denmark	0,4043	0,9955	0,3916	0,5813	0,3880	0,3868	0,3808	1,0000	1,0000	0,3816	1,0000	0,3874	0,3858	0,3900	0,4045	0,4613	0,3824	0,3881
Dominican Republic	0,4297	0,4218	0,5417	0,4278	0,4919	1,0000	0,7284	0,4197	0,4070	0,9012	0,4057	0,5704	1,0000	1,0000	0,4475	0,4187	0,4925	1,0000
Estonia	0,5424	0,9135	0,4308	1,0000	0,4230	0,4024	0,3972	0,8018	0,7523	0,3949	0,6167	0,4163	0,3988	0,4054	0,5082	0,9921	0,4042	0,4027
Finland	0,4150	0,9999	0,3979	0,6528	0,3934	0,3914	0,3841	1,0000	1,0000	0,3850	1,0000	0,3925	0,3901	0,3952	0,4150	0,4923	0,3862	0,3929
France	0,6645	0,9950	0,4855	1,0000	0,4709	0,4341	0,4237	0,9616	0,9356	0,4196	0,8050	0,4591	0,4274	0,4400	0,6152	0,9996	0,4365	0,4348
Germany	0,4795	1,0000	0,4313	0,9531	0,4222	0,4135	0,4010	1,0000	1,0000	0,4018	1,0000	0,4192	0,4104	0,4199	0,4748	0,6891	0,4062	0,4158
Ghana	0,4049	0,4078	0,4533	0,4092	0,4307	0,8549	0,4941	0,4068	0,3971	0,5738	0,3968	0,4605	0,9875	1,0000	0,4152	0,4017	0,4274	0,9973
Greece	0,7685	0,4900	1,0000	0,5521	1,0000	0,7507	1,0000	0,4791	0,4534	0,8181	0,4445	1,0000	0,6453	0,6763	0,8623	0,5560	1,0000	0,6724

Продовження таблиці Е.5

Назва країни	Lithuania	Luxembourg	Malaysia	Malta	Mauritius	Mexico	Montenegro	Netherlands	New Zealand	North Macedonia	Norway	Panama	Paraguay	Philippines	Poland	Portugal	Romania	Russian Federation
Guatemala	0,4117	0,4143	0,4701	0,4162	0,4430	0,9128	0,5224	0,4131	0,4019	0,6182	0,4014	0,4793	0,9976	1,0000	0,4238	0,4075	0,4394	0,9998
Hungary	0,6943	0,4623	1,0000	0,5110	1,0000	0,6872	0,9998	0,4538	0,4338	0,7549	0,4269	1,0000	0,5919	0,6187	0,7890	0,5139	1,0000	0,6153
Iceland	0,4421	1,0000	0,4075	0,9224	0,4019	0,3953	0,3882	1,0000	1,0000	0,3884	0,9695	0,3997	0,3932	0,3989	0,4375	0,6135	0,3916	0,3965
India	0,4151	0,4203	0,4731	0,4216	0,4459	0,8757	0,5157	0,4191	0,4064	0,6034	0,4061	0,4808	0,9866	1,0000	0,4279	0,4116	0,4413	0,9965
Indonesia	0,4904	0,4540	0,7662	0,4703	0,6576	1,0000	0,9997	0,4496	0,4299	1,0000	0,4269	0,8450	1,0000	1,0000	0,5265	0,4581	0,6808	1,0000
Ireland	0,4721	1,0000	0,4255	0,9574	0,4173	0,4086	0,3978	1,0000	1,0000	0,3982	0,9990	0,4143	0,4057	0,4141	0,4668	0,6823	0,4026	0,4105
Israel	1,0000	0,6962	0,7382	0,9731	0,7194	0,4935	0,5151	0,6472	0,5940	0,4771	0,5482	0,6371	0,4730	0,4928	0,9999	0,9998	0,5787	0,4857
Italy	1,0000	0,6415	0,7602	0,9232	0,7450	0,4895	0,5181	0,6008	0,5540	0,4752	0,5176	0,6493	0,4686	0,4873	1,0000	0,9929	0,5893	0,4808
Japan	0,5588	0,9973	0,4474	1,0000	0,4371	0,4148	0,4062	0,9629	0,9408	0,4041	0,7880	0,4300	0,4102	0,4194	0,5303	0,9692	0,4144	0,4156
Kenya	0,4131	0,4232	0,4608	0,4226	0,4378	0,7599	0,4831	0,4223	0,4087	0,5480	0,4088	0,4650	0,8979	0,9906	0,4252	0,4117	0,4323	0,9397
Korea	1,0000	0,6641	0,6125	0,9804	0,5945	0,4542	0,4633	0,6139	0,5665	0,4414	0,5218	0,5424	0,4408	0,4551	0,9783	1,0000	0,5017	0,4498
Latvia	1,0000	0,5482	0,8481	0,7506	0,8466	0,4869	0,5388	0,5231	0,4897	0,4775	0,4684	0,7073	0,4637	0,4808	1,0000	0,8565	0,6412	0,4752
Liberia	0,3911	0,4022	0,4095	0,3995	0,3999	0,5024	0,4105	0,4022	0,3935	0,4325	0,3941	0,4095	0,5520	0,6498	0,3971	0,3924	0,3963	0,5835
Lithuania	–	0,5330	0,7227	0,7513	0,7141	0,4572	0,4877	0,5083	0,4781	0,4483	0,4575	0,6073	0,4405	0,4539	1,0000	0,8816	0,5551	0,4494
Luxembourg	0,4606	–	0,4196	0,9323	0,4122	0,4047	0,3948	1,0000	1,0000	0,3953	0,9991	0,4096	0,4021	0,4098	0,4561	0,6485	0,3990	0,4064
Malaysia	0,8427	0,5091	–	0,5844	1,0000	0,7466	0,9992	0,4962	0,4668	0,8008	0,4560	1,0000	0,6476	0,6800	0,9259	0,5925	1,0000	0,6749
Malta	0,6608	0,9531	0,4716	–	0,4590	0,4232	0,4158	0,8723	0,8238	0,4115	0,6901	0,4474	0,4171	0,4276	0,6018	1,0000	0,4276	0,4233
Mauritius	0,8421	0,4849	1,0000	0,5553	–	0,6442	0,9671	0,4735	0,4492	0,6794	0,4398	1,0000	0,5691	0,5960	0,9300	0,5669	1,0000	0,5909
Mexico	0,4703	0,4454	0,6881	0,4580	0,5974	–	0,9805	0,4418	0,4239	1,0000	0,4214	0,7521	1,0000	1,0000	0,5003	0,4463	0,6098	1,0000
Montenegro	0,5284	0,4445	0,9816	0,4697	0,8844	0,9550	–	0,4392	0,4222	0,9998	0,4181	0,9999	0,8042	0,8242	0,5796	0,4634	0,9584	0,8324
Netherlands	0,4364	1,0000	0,4098	0,7832	0,4036	0,3997	0,3902	–	1,0000	0,3912	1,0000	0,4021	0,3978	0,4046	0,4353	0,5560	0,3934	0,4016
New Zealand	0,4224	1,0000	0,4006	0,7366	0,3957	0,3924	0,3852	1,0000	–	0,3859	1,0000	0,3945	0,3908	0,3961	0,4212	0,5232	0,3877	0,3938
North Macedonia	0,4789	0,4360	0,8001	0,4522	0,6748	1,0000	1,0000	0,4320	0,4166	–	0,4137	0,9032	0,9733	0,9732	0,5132	0,4438	0,7187	0,9816
Norway	0,4058	0,9868	0,3932	0,5772	0,3893	0,3885	0,3818	1,0000	1,0000	0,3828	–	0,3888	0,3875	0,3920	0,4064	0,4622	0,3834	0,3900

Продовження таблиці Е.5

Назва країни	Lithuania	Luxembourg	Malaysia	Malta	Mauritius	Mexico	Montenegro	Netherlands	New Zealand	North Macedonia	Norway	Panama	Paraguay	Philippines	Poland	Portugal	Romania	Russian Federation
Panama	0,7301	0,4930	1,0000	0,5502	1,0000	0,8274	1,0000	0,4825	0,4559	0,9080	0,4474	–	0,7054	0,7370	0,8212	0,5502	1,0000	0,7348
Paraguay	0,4407	0,4313	0,5711	0,4384	0,5137	1,0000	0,7757	0,4288	0,4139	0,9354	0,4124	0,6039	–	1,0000	0,4616	0,4277	0,5145	1,0000
Philippines	0,4455	0,4400	0,5690	0,4463	0,5142	1,0000	0,7268	0,4374	0,4204	0,8861	0,4190	0,5955	1,0000	–	0,4673	0,4337	0,5122	1,0000
Poland	1,0000	0,5448	0,8941	0,7329	0,8966	0,4972	0,5609	0,5210	0,4878	0,4884	0,4676	0,7501	0,4713	0,4895	–	0,8282	0,6807	0,4837
Portugal	0,8492	0,7340	0,4922	1,0000	0,4792	0,4225	0,4206	0,6600	0,6095	0,4124	0,5423	0,4596	0,4153	0,4251	0,7140	–	0,4371	0,4213
Romania	0,6795	0,4592	1,0000	0,5058	1,0000	0,6879	0,9999	0,4511	0,4317	0,7588	0,4251	1,0000	0,5913	0,6178	0,7724	0,5081	–	0,6147
Russian Federation	0,4477	0,4383	0,5860	0,4458	0,5254	1,0000	0,7872	0,4356	0,4190	0,9401	0,4174	0,6193	1,0000	1,0000	0,4705	0,4339	0,5257	–
Saudi Arabia	0,4404	0,4303	0,5729	0,4375	0,5146	1,0000	0,7871	0,4278	0,4131	0,9445	0,4117	0,6070	1,0000	1,0000	0,4613	0,4271	0,5160	1,0000
Singapore	0,4792	1,0000	0,4246	0,9923	0,4167	0,4058	0,3966	1,0000	1,0000	0,3965	0,9606	0,4132	0,4028	0,4106	0,4703	0,7381	0,4017	0,4072
Slovakia	1,0000	0,5241	0,8550	0,6999	0,8571	0,4798	0,5348	0,5026	0,4732	0,4720	0,4553	0,7073	0,4573	0,4732	1,0000	0,7967	0,6417	0,4681
Slovenia	0,8810	0,6890	0,4922	0,9999	0,4796	0,4204	0,4197	0,6234	0,5770	0,4110	0,5202	0,4589	0,4133	0,4226	0,7313	1,0000	0,4366	0,4190
South Africa	0,4545	0,4432	0,6061	0,4516	0,5402	1,0000	0,8237	0,4403	0,4226	0,9617	0,4209	0,6430	1,0000	1,0000	0,4792	0,4390	0,5412	1,0000
Spain	0,8139	0,9020	0,5123	1,0000	0,4962	0,4382	0,4323	0,8198	0,7632	0,4244	0,6559	0,4769	0,4298	0,4426	0,7148	1,0000	0,4502	0,4375
Sweden	0,4267	0,9999	0,4060	0,6961	0,4002	0,3981	0,3885	1,0000	1,0000	0,3899	1,0000	0,3992	0,3965	0,4031	0,4269	0,5186	0,3912	0,4001
Switzerland	0,4270	1,0000	0,4056	0,7077	0,4000	0,3975	0,3883	1,0000	1,0000	0,3895	1,0000	0,3988	0,3959	0,4023	0,4270	0,5221	0,3910	0,3994
Tanzania	0,4075	0,4216	0,4432	0,4190	0,4252	0,6400	0,4514	0,4211	0,4077	0,4960	0,4083	0,4447	0,7434	0,8895	0,4178	0,4081	0,4197	0,7943
Thailand	0,4963	0,4630	0,7585	0,4791	0,6550	1,0000	0,9970	0,4584	0,4366	1,0000	0,4335	0,8282	1,0000	1,0000	0,5334	0,4651	0,6721	1,0000
Trinidad and Tobago	0,4899	0,4462	0,8054	0,4636	0,6846	1,0000	1,0000	0,4418	0,4240	1,0000	0,4209	0,8979	0,9950	0,9943	0,5268	0,4534	0,7218	0,9971
Turkey	0,4325	0,4297	0,5321	0,4345	0,4873	0,9991	0,6542	0,4277	0,4129	0,8083	0,4119	0,5524	1,0000	1,0000	0,4506	0,4235	0,4846	1,0000
Ukraine	0,4759	0,4490	0,7045	0,4624	0,6103	1,0000	0,9871	0,4452	0,4265	1,0000	0,4239	0,7707	1,0000	1,0000	0,5074	0,4502	0,6239	1,0000
United Kingdom	0,4750	1,0000	0,4280	0,9537	0,4193	0,4107	0,3992	1,0000	1,0000	0,3998	0,9998	0,4164	0,4077	0,4166	0,4700	0,6834	0,4041	0,4128
United States	0,6491	1,0000	0,4934	1,0000	0,4772	0,4435	0,4292	0,9975	0,9943	0,4263	0,9250	0,4665	0,4364	0,4511	0,6128	0,9932	0,4420	0,4450
Uruguay	0,9998	0,5129	0,9969	0,6375	0,9988	0,5352	0,6740	0,4957	0,4671	0,5340	0,4527	0,9268	0,4971	0,5182	1,0000	0,6870	0,8745	0,5122

Продовження таблиці Е.5

Назва країни	Lithuania	Luxembourg	Malaysia	Malta	Mauritius	Mexico	Montenegro	Netherlands	New Zealand	North Macedonia	Norway	Panama	Paraguay	Philippines	Poland	Portugal	Romania	Russian Federation
Venezuela	0,3878	0,3979	0,4031	0,3954	0,3950	0,4784	0,4033	0,3979	0,3903	0,4214	0,3909	0,4030	0,5179	0,5984	0,3929	0,3891	0,3919	0,5439

Продовження таблиці Е.5

Назва країни	Saudi Arabia	Singapore	Slovakia	Slovenia	South Africa	Spain	Sweden	Switzer-land	Tanzania	Thailand	Trinidad and Tobago	Turkey	Ukraine	United Kingdom	United States	Uruguay	Venezuela
Australia	0,4082	1,0000	0,4844	0,7792	0,4169	0,9982	0,9817	0,9829	0,4298	0,4224	0,4088	0,4123	0,4148	1,0000	1,0000	0,4651	0,4090
Austria	0,3995	1,0000	0,4498	0,6426	0,4064	0,9504	0,9959	0,9967	0,4176	0,4103	0,3994	0,4029	0,4045	1,0000	1,0000	0,4374	0,4013
Bahrain	0,9985	0,4772	0,5701	0,4846	0,9991	0,5402	0,4725	0,4686	0,8741	1,0000	1,0000	0,9873	1,0000	0,4972	0,5632	0,6705	0,6281
Belgium	0,4155	1,0000	0,5404	0,9640	0,4256	1,0000	0,8941	0,8938	0,4381	0,4334	0,4179	0,4198	0,4241	0,9979	1,0000	0,5069	0,4134
Bolivia	0,9194	0,4051	0,4063	0,3982	0,9564	0,4148	0,4080	0,4063	1,0000	0,7941	0,5985	0,9998	0,7683	0,4143	0,4313	0,4159	0,9104
Botswana	1,0000	0,4156	0,4300	0,4112	1,0000	0,4341	0,4168	0,4149	0,9766	1,0000	0,9554	1,0000	1,0000	0,4262	0,4516	0,4517	0,6649
Brazil	1,0000	0,4280	0,4584	0,4262	1,0000	0,4562	0,4278	0,4255	0,9015	1,0000	1,0000	1,0000	1,0000	0,4405	0,4748	0,4964	0,6104
Bulgaria	0,7064	0,4532	0,6162	0,4770	0,7433	0,5257	0,4442	0,4415	0,5988	0,9135	0,9715	0,6698	0,8580	0,4663	0,5289	0,8054	0,4781
Canada	0,4062	1,0000	0,4591	0,6423	0,4146	0,9309	1,0000	1,0000	0,4291	0,4190	0,4056	0,4105	0,4120	1,0000	1,0000	0,4462	0,4095
Chile	0,5071	0,5888	1,0000	0,8317	0,5324	0,8966	0,5329	0,5282	0,5160	0,5847	0,5645	0,5080	0,5517	0,6010	0,7868	1,0000	0,4509
China	1,0000	0,4564	0,5120	0,4571	1,0000	0,5014	0,4548	0,4514	0,9168	1,0000	1,0000	0,9996	1,0000	0,4739	0,5253	0,5768	0,6485
Costa Rica	0,5077	0,5125	0,9993	0,6441	0,5323	0,7231	0,4813	0,4777	0,5047	0,5952	0,5853	0,5055	0,5594	0,5251	0,6550	1,0000	0,4416
Croatia	0,5227	0,4672	0,8718	0,5303	0,5484	0,5916	0,4498	0,4470	0,5037	0,6328	0,6413	0,5158	0,5899	0,4786	0,5646	1,0000	0,4379
Cyprus	0,4944	0,6079	1,0000	0,8899	0,5179	0,9373	0,5429	0,5381	0,5067	0,5628	0,5412	0,4963	0,5332	0,6179	0,8186	1,0000	0,4467
Czech Republic	0,4247	0,8032	0,7810	1,0000	0,4364	1,0000	0,6214	0,6169	0,4429	0,4497	0,4334	0,4283	0,4376	0,7700	0,9939	0,6716	0,4139
Denmark	0,3853	0,9145	0,4000	0,4459	0,3892	0,5562	1,0000	1,0000	0,3975	0,3906	0,3843	0,3876	0,3876	0,9985	0,8313	0,3964	0,3887
Dominican Rep.	1,0000	0,4194	0,4367	0,4152	1,0000	0,4401	0,4204	0,4183	0,9685	1,0000	0,9836	1,0000	1,0000	0,4307	0,4584	0,4616	0,6598
Estonia	0,3982	0,9891	0,4917	0,9522	0,4047	1,0000	0,7168	0,7152	0,4119	0,4099	0,4001	0,4009	0,4039	0,9387	1,0000	0,4653	0,3962

Продовження таблиці Е.5

Назва країни	Saudi Arabia	Singapore	Slovakia	Slovenia	South Africa	Spain	Sweden	Switzer-land	Tanzania	Thailand	Trinidad and Tobago	Turkey	Ukraine	United Kingdom	United States	Uruguay	Venezuela
Finland	0,3895	0,9791	0,4091	0,4715	0,3943	0,6187	1,0000	1,0000	0,4042	0,3961	0,3884	0,3922	0,3923	1,0000	0,9171	0,4044	0,3933
France	0,4262	1,0000	0,5881	0,9933	0,4385	1,0000	0,9064	0,9055	0,4529	0,4483	0,4296	0,4313	0,4369	0,9977	1,0000	0,5448	0,4228
Germany	0,4093	1,0000	0,4618	0,6361	0,4184	0,9151	1,0000	1,0000	0,4347	0,4228	0,4083	0,4140	0,4153	1,0000	1,0000	0,4491	0,4135
Ghana	0,9836	0,4054	0,4088	0,3993	0,9943	0,4164	0,4079	0,4062	1,0000	0,8772	0,6556	1,0000	0,8554	0,4145	0,4323	0,4200	0,8234
Greece	0,6502	0,4930	0,8187	0,5481	0,6882	0,6186	0,4753	0,4716	0,5943	0,8244	0,8608	0,6312	0,7665	0,5094	0,6053	0,9917	0,4829
Guatemala	0,9965	0,4116	0,4163	0,4047	0,9992	0,4247	0,4143	0,4124	1,0000	0,9295	0,7131	1,0000	0,9129	0,4221	0,4430	0,4298	0,8385
Hungary	0,5962	0,4646	0,7430	0,5075	0,6293	0,5648	0,4508	0,4480	0,5479	0,7597	0,8000	0,5796	0,7021	0,4775	0,5545	0,9717	0,4577
Iceland	0,3926	1,0000	0,4289	0,5665	0,3980	0,8623	0,9974	0,9981	0,4072	0,4010	0,3924	0,3953	0,3964	1,0000	1,0000	0,4200	0,3944
India	0,9826	0,4171	0,4199	0,4084	0,9938	0,4306	0,4207	0,4185	1,0000	0,8980	0,6882	1,0000	0,8770	0,4291	0,4518	0,4334	0,9296
Indonesia	1,0000	0,4516	0,5054	0,4524	1,0000	0,4946	0,4499	0,4467	0,9000	1,0000	1,0000	0,9990	1,0000	0,4681	0,5171	0,5682	0,6312
Ireland	0,4047	1,0000	0,4547	0,6282	0,4128	0,9171	1,0000	1,0000	0,4269	0,4169	0,4041	0,4089	0,4102	1,0000	1,0000	0,4426	0,4080
Israel	0,4720	0,7401	0,9997	0,9999	0,4924	0,9999	0,6190	0,6134	0,4942	0,5220	0,4972	0,4763	0,4991	0,7354	0,9582	0,9763	0,4428
Italy	0,4678	0,6771	1,0000	0,9947	0,4872	0,9972	0,5782	0,5731	0,4863	0,5176	0,4950	0,4713	0,4951	0,6775	0,9112	0,9926	0,4372
Japan	0,4094	1,0000	0,5113	0,9141	0,4183	1,0000	0,8959	0,8962	0,4296	0,4247	0,4111	0,4132	0,4167	0,9988	1,0000	0,4842	0,4081
Kenya	0,8852	0,4194	0,4176	0,4084	0,9310	0,4309	0,4243	0,4219	1,0000	0,7907	0,6092	0,9947	0,7634	0,4324	0,4545	0,4287	0,9976
Korea	0,4400	0,7138	0,9663	1,0000	0,4545	1,0000	0,5851	0,5804	0,4583	0,4740	0,4552	0,4436	0,4581	0,7014	0,9536	0,8547	0,4220
Latvia	0,4633	0,5676	1,0000	0,8588	0,4815	0,9103	0,5101	0,5062	0,4742	0,5155	0,4976	0,4651	0,4925	0,5750	0,7670	1,0000	0,4282
Liberia	0,5430	0,3993	0,3933	0,3905	0,5831	0,4034	0,4040	0,4024	1,0000	0,5203	0,4520	0,6508	0,5052	0,4080	0,4196	0,3975	1,0000
Lithuania	0,4401	0,5536	1,0000	0,8877	0,4542	0,9259	0,4953	0,4918	0,4509	0,4786	0,4633	0,4420	0,4614	0,5578	0,7544	0,9978	0,4154
Luxembourg	0,4012	1,0000	0,4454	0,5991	0,4085	0,8842	1,0000	1,0000	0,4215	0,4122	0,4006	0,4050	0,4062	1,0000	1,0000	0,4346	0,4044
Malaysia	0,6518	0,5133	0,8904	0,5837	0,6906	0,6625	0,4913	0,4872	0,6045	0,8185	0,8449	0,6356	0,7619	0,5312	0,6418	0,9994	0,4904
Malta	0,4162	0,9947	0,5760	0,9987	0,4264	1,0000	0,7984	0,7960	0,4371	0,4351	0,4198	0,4203	0,4255	0,9701	1,0000	0,5310	0,4121
Mauritius	0,5716	0,4893	0,8940	0,5595	0,6035	0,6302	0,4690	0,4656	0,5436	0,7084	0,7231	0,5617	0,6572	0,5035	0,6034	1,0000	0,4587
Mexico	1,0000	0,4428	0,4826	0,4412	1,0000	0,4785	0,4423	0,4394	0,9297	1,0000	1,0000	1,0000	1,0000	0,4582	0,5008	0,5312	0,6482

Продовження таблиці Е.5

Назва країни	Saudi Arabia	Singapore	Slovakia	Slovenia	South Africa	Spain	Sweden	Switzer-land	Tanzania	Thailand	Trinidad and Tobago	Turkey	Ukraine	United Kingdom	United States	Uruguay	Venezuela
Montenegro	0,8188	0,4442	0,5512	0,4581	0,8503	0,5003	0,4381	0,4355	0,6447	0,9882	0,9999	0,7613	0,9646	0,4570	0,5097	0,6784	0,4953
Netherlands	0,3970	0,9998	0,4270	0,5241	0,4034	0,7368	1,0000	1,0000	0,4161	0,4062	0,3958	0,4005	0,4010	1,0000	0,9873	0,4198	0,4013
New Zealand	0,3902	0,9998	0,4146	0,4958	0,3952	0,6887	1,0000	1,0000	0,4047	0,3973	0,3894	0,3929	0,3933	1,0000	0,9780	0,4087	0,3933
North Macedonia	0,9822	0,4346	0,4934	0,4392	0,9868	0,4743	0,4318	0,4294	0,7454	1,0000	1,0000	0,9336	1,0000	0,4472	0,4893	0,5623	0,5341
Norway	0,3869	0,8863	0,4016	0,4471	0,3912	0,5543	1,0000	1,0000	0,4005	0,3926	0,3857	0,3894	0,3893	0,9944	0,8169	0,3980	0,3909
Panama	0,7122	0,4952	0,7766	0,5419	0,7521	0,6122	0,4791	0,4753	0,6323	0,8968	0,9386	0,6857	0,8431	0,5129	0,6064	0,9693	0,5013
Paraguay	1,0000	0,4285	0,4490	0,4237	1,0000	0,4529	0,4297	0,4272	0,9819	1,0000	0,9928	1,0000	1,0000	0,4418	0,4742	0,4782	0,6986
Philippines	1,0000	0,4365	0,4540	0,4292	1,0000	0,4616	0,4388	0,4359	0,9989	1,0000	0,9704	1,0000	1,0000	0,4519	0,4870	0,4823	0,7957
Poland	0,4709	0,5625	1,0000	0,8287	0,4904	0,8888	0,5088	0,5048	0,4808	0,5283	0,5103	0,4724	0,5033	0,5713	0,7553	1,0000	0,4315
Portugal	0,4146	0,8167	0,6811	1,0000	0,4243	1,0000	0,6152	0,6113	0,4308	0,4347	0,4209	0,4178	0,4249	0,7733	0,9973	0,5962	0,4068
Romania	0,5958	0,4614	0,7268	0,5019	0,6286	0,5575	0,4483	0,4455	0,5459	0,7609	0,8038	0,5787	0,7029	0,4740	0,5483	0,9622	0,4564
Russia	1,0000	0,4352	0,4567	0,4294	1,0000	0,4617	0,4366	0,4339	0,9915	1,0000	0,9930	1,0000	1,0000	0,4499	0,4854	0,4880	0,7376
Saudi Arabia	–	0,4276	0,4487	0,4231	1,0000	0,4520	0,4287	0,4262	0,9758	1,0000	0,9951	1,0000	1,0000	0,4406	0,4728	0,4783	0,6852
Singapore	0,4020	–	0,4579	0,6722	0,4094	0,9698	0,9950	0,9958	0,4213	0,4137	0,4020	0,4056	0,4074	1,0000	1,0000	0,4440	0,4037
Slovakia	0,4570	0,5402	–	0,7975	0,4740	0,8605	0,4917	0,4882	0,4659	0,5070	0,4911	0,4584	0,4852	0,5479	0,7208	1,0000	0,4230
Slovenia	0,4126	0,7639	0,6978	–	0,4219	1,0000	0,5850	0,5812	0,4275	0,4322	0,4192	0,4156	0,4227	0,7271	0,9896	0,6044	0,4045
South Africa	1,0000	0,4400	0,4643	0,4343	–	0,4688	0,4414	0,4384	0,9913	1,0000	0,9973	1,0000	1,0000	0,4556	0,4939	0,4987	0,7438
Spain	0,4287	0,9661	0,6816	1,0000	0,4414	–	0,7574	0,7535	0,4522	0,4536	0,4351	0,4333	0,4413	0,9300	1,0000	0,6090	0,4209
Sweden	0,3957	0,9850	0,4196	0,4941	0,4019	0,6609	–	1,0000	0,4149	0,4042	0,3941	0,3992	0,3993	1,0000	0,9433	0,4139	0,4009
Switzerland	0,3951	0,9913	0,4197	0,4967	0,4012	0,6702	1,0000	–	0,4137	0,4035	0,3937	0,3985	0,3987	1,0000	0,9532	0,4138	0,3999
Tanzania	0,7287	0,4174	0,4113	0,4050	0,7892	0,4259	0,4235	0,4211	–	0,6697	0,5367	0,8982	0,6443	0,4305	0,4501	0,4196	1,0000
Thailand	1,0000	0,4600	0,5115	0,4589	1,0000	0,5045	0,4589	0,4554	0,9489	–	1,0000	1,0000	1,0000	0,4785	0,5306	0,5726	0,6838
Trinidad and Tobago	0,9975	0,4444	0,5055	0,4482	0,9982	0,4878	0,4417	0,4389	0,8127	1,0000	–	0,9770	1,0000	0,4590	0,5060	0,5760	0,5722
Turkey	1,0000	0,4266	0,4395	0,4197	1,0000	0,4472	0,4289	0,4264	0,9993	0,9993	0,9200	–	0,9989	0,4400	0,4697	0,4623	0,7867

Продовження таблиці Е.5

Назва країни	Saudi Arabia	Singapore	Slovakia	Slovenia	South Africa	Spain	Sweden	Switzer-land	Tanzania	Thailand	Trinidad and Tobago	Turkey	Ukraine	United Kingdom	United States	Uruguay	Venezuela
Ukraine	1,0000	0,4464	0,4887	0,4449	1,0000	0,4839	0,4457	0,4427	0,9331	1,0000	1,0000	1,0000	–	0,4624	0,5071	0,5402	0,6549
UK	0,4067	1,0000	0,4576	0,6301	0,4152	0,9139	1,0000	1,0000	0,4303	0,4195	0,4059	0,4111	0,4124	–	1,0000	0,4452	0,4104
United States	0,4350	1,0000	0,5858	0,9710	0,4492	1,0000	0,9809	0,9811	0,4679	0,4594	0,4374	0,4413	0,4466	1,0000	–	0,5474	0,4335
Uruguay	0,4974	0,5233	1,0000	0,6816	0,5206	0,7611	0,4875	0,4839	0,4984	0,5761	0,5630	0,4964	0,5433	0,5353	0,6773	–	0,4391
Venezuela	0,5105	0,3953	0,3896	0,3874	0,5442	0,3987	0,3996	0,3981	1,0000	0,4935	0,4374	0,5979	0,4808	0,4030	0,4129	0,3931	–

Додаток Ж

Результати розрахунків для обґрунтування таргетів та напрямків реформування системи забезпечення інформаційної безпеки в Україні

Таблиця Ж.1 – Результати розрахунків рейтингів та різниць за методами TOPSIS, MAAM та VIKOR

Назва країни	Фактичний рейтинг	TOPSIS			MAAM			VIKOR (v=1)			VIKOR (v=0.5)		
		Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом
Afghanistan	131	0,17	134	3	67	130,5	-0,5	0,12	133,5	2,5	0,06	135,0	4,0
Albania	68	0,39	71	3	231	70,5	2,5	0,45	67,0	-1,0	0,31	90,0	22,0
Algeria	122	0,20	122	0	86	122,0	0,0	0,14	124,0	2,0	0,07	128,5	6,5
Angola	144	0,14	144	0	33	148,5	4,5	0,09	145,5	1,5	0,04	146,0	2,0
Antigua and Barbuda	136	0,15	141	5	52	141,0	5,0	0,12	133,5	-2,5	0,06	135,0	-1,0
Argentina	55	0,46	52	-3	262	57,0	2,0	0,52	54,5	-0,5	0,51	49,0	-6,0
Armenia	91	0,34	84	-7	190	81,0	-10,0	0,33	89,0	-2,0	0,33	84,0	-7,0
Australia	36	0,54	37	1	323	37,0	1,0	0,65	35,5	-0,5	0,41	64,0	28,0
Austria	23	0,60	24	1	386	19,5	-3,5	0,75	23,0	0,0	0,71	20,0	-3,0
Azerbaijan	80	0,36	79	-1	194	79,0	-1,0	0,36	82,0	2,0	0,35	79,0	-1,0
Bahamas	103	0,27	105	2	130	101,0	-2,0	0,25	102,0	-1,0	0,21	104,5	1,5
Bahrain	100	0,27	104	4	150	100,0	0,0	0,28	100,0	0,0	0,30	91,0	-9,0

Продовження таблиці Ж.1

Назва країни	Фактичний рейтинг	TOPSIS			MAAM			VIKOR (v=1)			VIKOR (v=0.5)		
		Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом
Bangladesh	92	0,32	94	2	167	96,0	4,0	0,30	94,0	2,0	0,24	102,0	10,0
Barbados	121	0,18	130	9	93	117,5	-3,5	0,16	119,0	-2,0	0,25	101,0	-20,0
Belarus	46	0,52	40	-6	301	43,0	-3,0	0,58	45,5	-0,5	0,62	33,0	-13,0
Belgium	5	0,76	4	-1	465	5,0	0,0	0,94	5,0	0,0	0,89	7,0	2,0
Belize	152	0,09	150	-2	30	151,5	-0,5	0,04	151,0	-1,0	0,02	151,0	-1,0
Benin	57	0,44	58	1	261	58,0	1,0	0,51	58,5	1,5	0,42	63,0	6,0
Bhutan	115	0,24	114	-1	93	117,5	2,5	0,19	114,5	-0,5	0,09	123,5	8,5
Bolivia	95	0,33	93	-2	170	92,5	-2,5	0,30	94,0	-1,0	0,32	86,5	-8,5
Bosnia and Herzegovina	52	0,45	53	1	267	54,5	2,5	0,54	51,5	-0,5	0,43	60,0	8,0
Botswana	106	0,24	113	7	121	107,0	1,0	0,23	105,5	-0,5	0,20	107,0	1,0
Brazil	59	0,48	47	-12	255	60,0	1,0	0,51	58,5	-0,5	0,59	36,5	-22,5
Brunei Darussalam	79	0,35	83	4	189	82,0	3,0	0,38	77,5	-1,5	0,36	76,5	-2,5
Bulgaria	47	0,46	51	4	290	46,0	-1,0	0,57	47,0	0,0	0,53	43,0	-4,0
Burundi	158	0,07	158	0	15	156,0	-2,0	0,01	157,5	-0,5	0,01	157,5	-0,5
Cambodia	120	0,22	118	-2	86	122,0	2,0	0,16	119,0	-1,0	0,08	126,0	6,0
Cameroon	104	0,28	103	-1	111	112,0	8,0	0,23	104,0	0,0	0,20	106,0	2,0
Canada	39	0,51	42	3	307	42,0	3,0	0,62	39,0	0,0	0,39	70,0	31,0
Chad	114	0,23	116	2	103	114,0	0,0	0,19	114,5	0,5	0,09	123,5	9,5
Chile	41	0,53	38	-3	326	36,0	-5,0	0,61	42,0	1,0	0,64	32,0	-9,0

Продовження таблиці Ж.1

Назва країни	Фактичний рейтинг	TOPSIS			MAAM			VIKOR (v=1)			VIKOR (v=0.5)		
		Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом
China	78	0,39	75	-3	192	80,0	2,0	0,38	77,5	-0,5	0,27	93,5	15,5
Colombia	58	0,44	59	1	258	59,0	1,0	0,51	58,5	0,5	0,59	36,5	-21,5
Congo	156	0,08	154	-2	11	159,0	3,0	0,01	157,5	1,5	0,01	157,5	1,5
Costa Rica	51	0,45	54	3	288	49,0	-2,0	0,54	51,5	0,5	0,52	47,0	-4,0
Côte d'Ivoire	87	0,30	98	11	172	90,0	3,0	0,33	89,0	2,0	0,33	84,0	-3,0
Croatia	6	0,71	9	3	429	11,0	5,0	0,91	6,0	0,0	0,71	21,0	15,0
Cuba	128	0,25	111	-17	58	136,0	8,0	0,13	128,5	0,5	0,07	131,0	3,0
Cyprus	69	0,41	67	-2	228	72,0	3,0	0,45	67,0	-2,0	0,47	54,0	-15,0
Czech Republic	1	0,78	3	2	484	1,0	0,0	1,00	1,5	0,5	0,92	5,0	4,0
Denmark	9	0,70	10	1	434	9,0	0,0	0,90	9,0	0,0	0,87	8,5	-0,5
Dominica	153	0,08	155	2	21	155,0	2,0	0,03	154,0	1,0	0,01	154,0	1,0
Dominican Republic	67	0,43	63	-4	241	65,0	-2,0	0,45	67,0	0,0	0,47	54,0	-13,0
Ecuador	77	0,39	76	-1	202	76,0	-1,0	0,38	77,5	0,5	0,36	76,5	-0,5
Egypt	76	0,38	78	2	211	74,0	-2,0	0,38	77,5	1,5	0,44	59,0	-17,0
El Salvador	111	0,25	110	-1	128	102,0	-9,0	0,20	111,0	0,0	0,27	95,0	-16,0
Estonia	2	0,87	1	-1	466	4,0	2,0	1,00	1,5	-0,5	1,00	1,0	-1,0
Ethiopia	84	0,34	87	3	168	95,0	11,0	0,35	85,0	1,0	0,26	97,0	13,0
Finland	8	0,68	13	5	446	6,5	-1,5	0,90	9,0	1,0	0,70	22,0	14,0
France	7	0,76	5	-2	446	6,5	-0,5	0,91	7,0	0,0	0,96	3,0	-4,0
Georgia	45	0,49	46	1	289	47,5	2,5	0,58	45,5	0,5	0,46	58,0	13,0

Продовження таблиці Ж.1

Назва країни	Фактичний рейтинг	TOPSIS			MAAM			VIKOR (v=1)			VIKOR (v=0.5)		
		Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом
Germany	11	0,68	14	3	435	8,0	-3,0	0,88	11,5	0,5	0,86	10,0	-1,0
Ghana	88	0,33	92	4	169	94,0	6,0	0,33	89,0	1,0	0,33	84,0	-4,0
Greece	18	0,64	18	0	386	19,5	1,5	0,78	19,5	1,5	0,72	16,5	-1,5
Grenada	125	0,20	124	-1	90	119,0	-6,0	0,14	124,0	-1,0	0,07	128,5	3,5
Guatemala	94	0,34	91	-3	186	84,0	-10,0	0,30	94,0	0,0	0,40	65,5	-28,5
Guyana	149	0,12	149	0	33	148,5	-0,5	0,06	149,0	0,0	0,03	149,0	0,0
Haiti	137	0,17	135	-2	66	132,0	-5,0	0,10	140,0	3,0	0,05	141,0	4,0
Honduras	141	0,19	128	-13	62	134,0	-7,0	0,10	140,0	-1,0	0,05	141,0	0,0
Hungary	24	0,57	29	5	356	26,0	2,0	0,71	25,0	1,0	0,69	24,0	0,0
Iceland	60	0,43	62	2	240	66,0	6,0	0,51	58,5	-1,5	0,25	98,0	38,0
India	35	0,56	32	-3	346	30,5	-4,5	0,65	35,5	0,5	0,66	30,0	-5,0
Indonesia	73	0,39	72	-1	232	68,5	-4,5	0,42	72,5	-0,5	0,38	73,5	0,5
Iran	124	0,19	126	2	81	125,5	1,5	0,14	124,0	0,0	0,16	114,0	-10,0
Ireland	30	0,56	33	3	349	29,0	-1,0	0,70	28,5	-1,5	0,68	27,0	-3,0
Israel	26	0,59	25	-1	351	27,0	1,0	0,71	25,0	-1,0	0,69	24,0	-2,0
Italy	15	0,68	12	-3	406	15,0	0,0	0,84	15,0	0,0	0,84	12,0	-3,0
Jamaica	96	0,32	95	-1	182	86,0	-10,0	0,30	94,0	-2,0	0,40	65,5	-30,5
Japan	31	0,56	30	-1	327	35,0	4,0	0,68	32,5	1,5	0,51	51,0	20,0
Jordan	126	0,22	117	-9	85	124,0	-2,0	0,14	124,0	-2,0	0,16	114,0	-12,0
Kazakhstan	61	0,43	60	-1	267	54,5	-6,5	0,49	61,0	0,0	0,50	52,0	-9,0

Продовження таблиці Ж.1

Назва країни	Фактичний рейтинг	TOPSIS			MAAM			VIKOR (v=1)			VIKOR (v=0.5)		
		Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом
Kenya	75	0,35	81	6	196	78,0	3,0	0,38	75,0	0,0	0,27	93,5	18,5
Kiribati	150	0,09	152	2	30	151,5	1,5	0,04	151,0	1,0	0,02	151,0	1,0
Korea (Republic of)	34	0,56	31	-3	334	34,0	0,0	0,68	32,5	-1,5	0,59	34,5	0,5
Kyrgyzstan	112	0,28	99	-13	123	105,5	-6,5	0,20	111,0	-1,0	0,10	121,5	9,5
Lao PDR	116	0,21	120	4	97	116,0	0,0	0,17	116,0	0,0	0,17	111,0	-5,0
Latvia	20	0,61	23	3	385	21,0	1,0	0,78	19,5	-0,5	0,72	19,0	-1,0
Liberia	110	0,27	106	-4	111	112,0	2,0	0,20	111,0	1,0	0,18	109,5	-0,5
Libya	140	0,18	132	-8	50	143,0	3,0	0,10	140,0	0,0	0,05	141,0	1,0
Lithuania	3	0,75	7	4	470	3,0	0,0	0,97	3,5	0,5	0,90	6,0	3,0
Luxembourg	32	0,57	28	-4	340	33,0	1,0	0,68	32,5	0,5	0,59	34,5	2,5
Madagascar	127	0,17	136	9	67	130,5	3,5	0,13	128,5	1,5	0,07	131,0	4,0
Malawi	107	0,28	101	-6	111	112,0	5,0	0,22	107,5	0,5	0,11	120,0	13,0
Malaysia	17	0,64	17	0	384	22,0	5,0	0,80	17,0	0,0	0,65	31,0	14,0
Mali	109	0,25	107	-2	112	110,0	1,0	0,20	111,0	2,0	0,18	109,5	0,5
Malta	50	0,46	50	0	273	53,0	3,0	0,55	49,0	-1,0	0,53	45,0	-5,0
Mauritania	133	0,15	140	7	54	139,0	6,0	0,12	133,5	0,5	0,06	135,0	2,0
Mauritius	54	0,44	57	3	277	51,5	-2,5	0,52	54,5	0,5	0,51	49,0	-5,0
Mexico	74	0,35	80	6	207	75,0	1,0	0,39	74,0	0,0	0,36	75,0	1,0
Moldova	49	0,47	49	0	289	47,5	-1,5	0,55	49,0	0,0	0,53	45,0	-4,0
Mongolia	135	0,16	138	3	65	133,0	-2,0	0,12	133,5	-1,5	0,06	135,0	0,0

Продовження таблиці Ж.1

Назва країни	Фактичний рейтинг	TOPSIS			MAAM			VIKOR (v=1)			VIKOR (v=0.5)		
		Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом
Montenegro	83	0,34	86	3	180	87,0	4,0	0,36	82,0	-1,0	0,35	79,0	-4,0
Morocco	102	0,25	109	7	126	103,5	1,5	0,25	102,0	0,0	0,21	104,5	2,5
Mozambique	145	0,13	145	0	46	144,5	-0,5	0,09	145,5	0,5	0,04	146,0	1,0
Myanmar	139	0,15	139	0	56	137,0	-2,0	0,10	140,0	1,0	0,05	141,0	2,0
Namibia	134	0,18	133	-1	78	127,0	-7,0	0,12	133,5	-0,5	0,14	117,0	-17,0
Nepal	93	0,31	96	3	171	91,0	-2,0	0,30	94,0	1,0	0,32	86,5	-6,5
Netherlands	10	0,74	8	-2	433	10,0	0,0	0,90	9,0	-1,0	0,87	8,5	-1,5
New Zealand	43	0,51	43	0	299	45,0	2,0	0,61	42,0	-1,0	0,47	56,0	13,0
Nicaragua	105	0,25	112	7	126	103,5	-1,5	0,23	105,5	0,5	0,28	92,0	-13,0
Nigeria	44	0,49	45	1	310	41,0	-3,0	0,59	44,0	0,0	0,55	42,0	-2,0
North Macedonia	70	0,39	74	4	227	73,0	3,0	0,43	70,5	0,5	0,38	72,0	2,0
Norway	33	0,54	36	3	343	32,0	-1,0	0,68	32,5	-0,5	0,67	29,0	-4,0
Oman	82	0,38	77	-5	185	85,0	3,0	0,36	82,0	0,0	0,35	79,0	-3,0
Pakistan	62	0,41	65	3	246	63,0	1,0	0,46	63,0	1,0	0,40	68,0	6,0
Panama	53	0,45	56	3	277	51,5	-1,5	0,52	54,5	1,5	0,51	49,0	-4,0
Papua New Guinea	130	0,20	125	-5	72	128,0	-2,0	0,13	128,5	-1,5	0,15	116,0	-14,0
Paraguay	72	0,40	70	-2	231	70,5	-1,5	0,42	72,5	0,5	0,38	73,5	1,5
Peru	64	0,42	64	0	249	61,0	-3,0	0,46	63,0	-1,0	0,40	68,0	4,0
Philippines	86	0,34	89	3	188	83,0	-3,0	0,35	85,0	-1,0	0,34	81,5	-4,5
Poland	22	0,62	21	-1	380	23,0	1,0	0,77	22,0	0,0	0,80	14,0	-8,0

Продовження таблиці Ж.1

Назва країни	Фактичний рейтинг	TOPSIS			MAAM			VIKOR (v=1)			VIKOR (v=0.5)		
		Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом
Portugal	21	0,62	22	1	397	17,0	-4,0	0,78	19,5	-1,5	0,72	18,0	-3,0
Qatar	42	0,52	39	-3	311	40,0	-2,0	0,61	42,0	0,0	0,55	41,0	-1,0
Romania	19	0,63	19	0	387	18,0	-1,0	0,78	19,5	0,5	0,72	16,5	-2,5
Russian Federation	25	0,57	26	1	361	25,0	0,0	0,71	25,0	0,0	0,69	24,0	-1,0
Rwanda	97	0,30	97	0	162	97,0	0,0	0,29	98,5	1,5	0,31	88,5	-8,5
Saint Kitts and Nevis	143	0,18	131	-12	55	138,0	-5,0	0,10	140,0	-3,0	0,05	141,0	-2,0
Saint Lucia	146	0,13	146	0	40	146,0	0,0	0,09	145,5	-0,5	0,04	146,0	0,0
Saint Vincent and the Grenadines	147	0,12	148	1	53	140,0	-7,0	0,09	145,5	-1,5	0,13	118,0	-29,0
Samoa	151	0,09	153	2	31	150,0	-1,0	0,04	151,0	0,0	0,02	151,0	0,0
Saudi Arabia	37	0,54	35	-2	322	38,0	1,0	0,64	37,0	0,0	0,57	38,0	1,0
Senegal	119	0,19	129	10	81	125,5	6,5	0,16	119,0	0,0	0,08	126,0	7,0
Serbia	28	0,57	27	-1	350	28,0	0,0	0,70	28,5	0,5	0,68	27,0	-1,0
Seychelles	142	0,14	143	1	46	144,5	2,5	0,10	140,0	-2,0	0,05	141,0	-1,0
Sierra Leone	154	0,09	151	-3	24	153,0	-1,0	0,03	154,0	0,0	0,01	154,0	0,0
Singapore	12	0,75	6	-6	423	13,0	1,0	0,88	11,5	-0,5	0,94	4,0	-8,0
Slovakia	13	0,66	16	3	422	14,0	1,0	0,87	13,0	0,0	0,77	15,0	2,0
Slovenia	38	0,51	44	6	300	44,0	6,0	0,62	39,0	1,0	0,56	39,5	1,5
Solomon Islands	157	0,07	156,5	-0,5	12	157,5	0,5	0,01	157,5	0,5	0,01	157,5	0,5
South Africa	99	0,28	102	3	151	99,0	0,0	0,29	98,5	-0,5	0,31	88,5	-10,5

Продовження таблиці Ж.1

Назва країни	Фактичний рейтинг	TOPSIS			MAAM			VIKOR (v=1)			VIKOR (v=0.5)		
		Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом
South Sudan	160	0,03	160	0	9	160,0	0,0	0,00	160,0	0,0	0,00	160,0	0,0
Spain	4	0,79	2	-2	474	2,0	-2,0	0,97	3,5	-0,5	0,99	2,0	-2,0
Sri Lanka	98	0,34	90	-8	161	98,0	0,0	0,29	97,0	-1,0	0,23	103,0	5,0
Sudan	132	0,16	137	5	61	135,0	3,0	0,12	133,5	1,5	0,06	135,0	3,0
Suriname	113	0,25	108	-5	117	109,0	-4,0	0,20	111,0	-2,0	0,10	121,5	8,5
Sweden	40	0,51	41	1	312	39,0	-1,0	0,62	39,0	-1,0	0,56	39,5	-0,5
Switzerland	16	0,66	15	-1	401	16,0	0,0	0,81	16,0	0,0	0,82	13,0	-3,0
Syrian Arab Republic	117	0,20	121	4	86	122,0	5,0	0,16	119,0	2,0	0,08	126,0	9,0
Tajikistan	123	0,19	127	4	89	120,0	-3,0	0,14	124,0	1,0	0,16	114,0	-9,0
Tanzania	129	0,20	123	-6	68	129,0	0,0	0,13	128,5	-0,5	0,07	131,0	2,0
Thailand	63	0,43	61	-2	244	64,0	1,0	0,46	63,0	0,0	0,40	68,0	5,0
Tonga	101	0,28	100	-1	123	105,5	4,5	0,25	102,0	1,0	0,12	119,0	18,0
Trinidad and Tobago	108	0,23	115	7	118	108,0	0,0	0,22	107,5	-0,5	0,19	108,0	0,0
Tunisia	90	0,34	88	-2	170	92,5	2,5	0,33	89,0	-1,0	0,25	99,5	9,5
Turkey	65	0,40	69	4	232	68,5	3,5	0,45	67,0	2,0	0,47	54,0	-11,0
Turkmenistan	155	0,06	159	4	22	154,0	-1,0	0,03	154,0	-1,0	0,01	154,0	-1,0
Tuvalu	159	0,07	156,5	-2,5	12	157,5	-1,5	0,01	157,5	-1,5	0,01	157,5	-1,5
Uganda	48	0,47	48	0	285	50,0	2,0	0,55	49,0	1,0	0,53	45,0	-3,0
Ukraine	29	0,55	34	5	363	24,0	-5,0	0,70	28,5	-0,5	0,68	27,0	-2,0
United Arab Emirates	71	0,41	68	-3	248	62,0	-9,0	0,43	70,5	-0,5	0,47	57,0	-14,0

Продовження таблиці Ж.1

Назва країни	Фактичний рейтинг	TOPSIS			MAAM			VIKOR (v=1)			VIKOR (v=0.5)		
		Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом	Розраховане значення	Рейтинг	Різниця між фактичним та розрахованим рейтингом
United Kingdom	14	0,69	11	-3	425	12,0	-2,0	0,86	14,0	0,0	0,84	11,0	-3,0
United States	27	0,63	20	-7	346	30,5	3,5	0,70	28,5	1,5	0,43	61,0	34,0
Uruguay	56	0,45	55	-1	265	56,0	0,0	0,52	54,5	-1,5	0,43	62,0	6,0
Uzbekistan	89	0,34	85	-4	179	88,0	-1,0	0,33	89,0	0,0	0,25	99,5	10,5
Vanuatu	138	0,15	142	4	51	142,0	4,0	0,10	140,0	2,0	0,05	141,0	3,0
Venezuela	85	0,35	82	-3	199	77,0	-8,0	0,35	85,0	0,0	0,34	81,5	-3,5
Vietnam	81	0,39	73	-8	173	89,0	8,0	0,36	80,0	-1,0	0,26	96,0	15,0
Yemen	148	0,13	147	-1	37	147,0	-1,0	0,07	148,0	0,0	0,04	148,0	0,0
Zambia	66	0,41	66	0	238	67,0	1,0	0,45	67,0	1,0	0,39	71,0	5,0
Zimbabwe	118	0,21	119	1	100	115,0	-3,0	0,16	119,0	1,0	0,16	112,0	-6,0

Додаток И

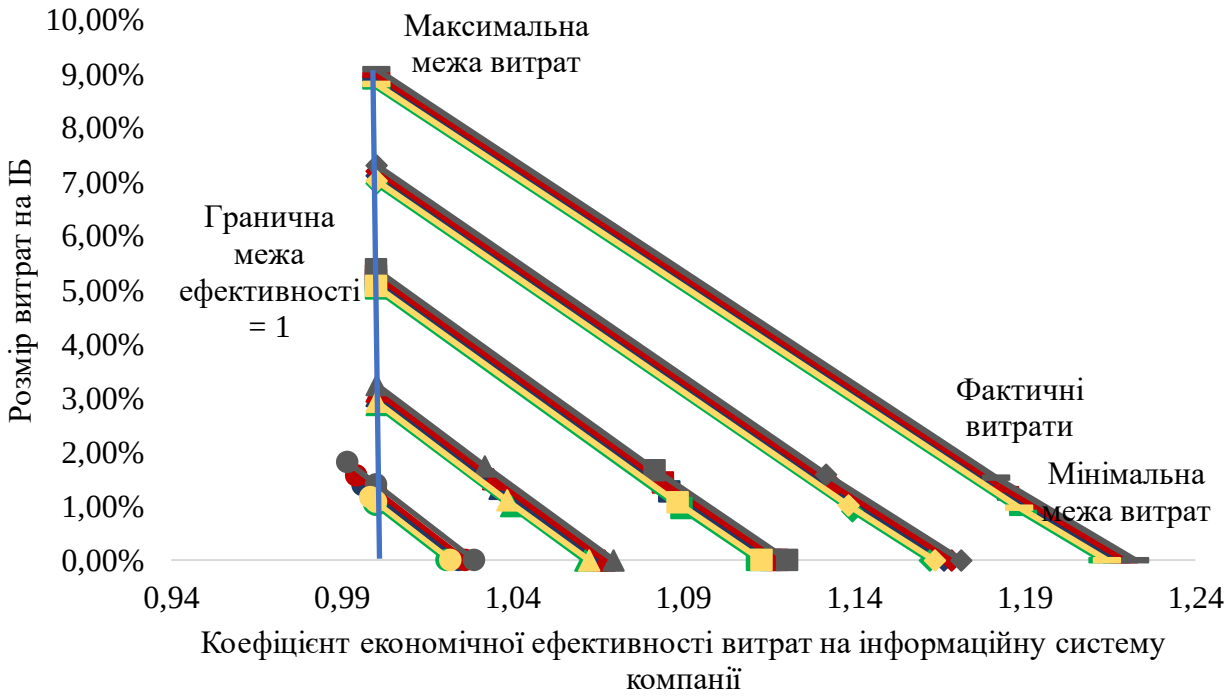


Рисунок И.1 – Співвідношення розміру витрат на інформаційну безпеку та коефіцієнту ефективності витрат на інформаційну систему для підприємств різних галузей із чисельністю від 501 до 1000 осіб (складено авторкою)

Пояснення форми позначки:

● – інформаційна система компанії генерує 1% прибутку;

▲ – інформаційна система компанії генерує 5% прибутку;

■ – інформаційна система компанії генерує 10% прибутку;

◆ – інформаційна система компанії генерує 15% прибутку;

▬ – інформаційна система компанії генерує 20% прибутку.

Пояснення кольору лінії:

синій – підприємства галузі роздрібної торгівлі / корпоративного банкінгу;

червоний – споживання / небанківських фінансових послуг;

сірий – страхування;

зелений – постачальників послуг;

жовтий – фінансових утиліт (бізнес-консалтингових компаній).

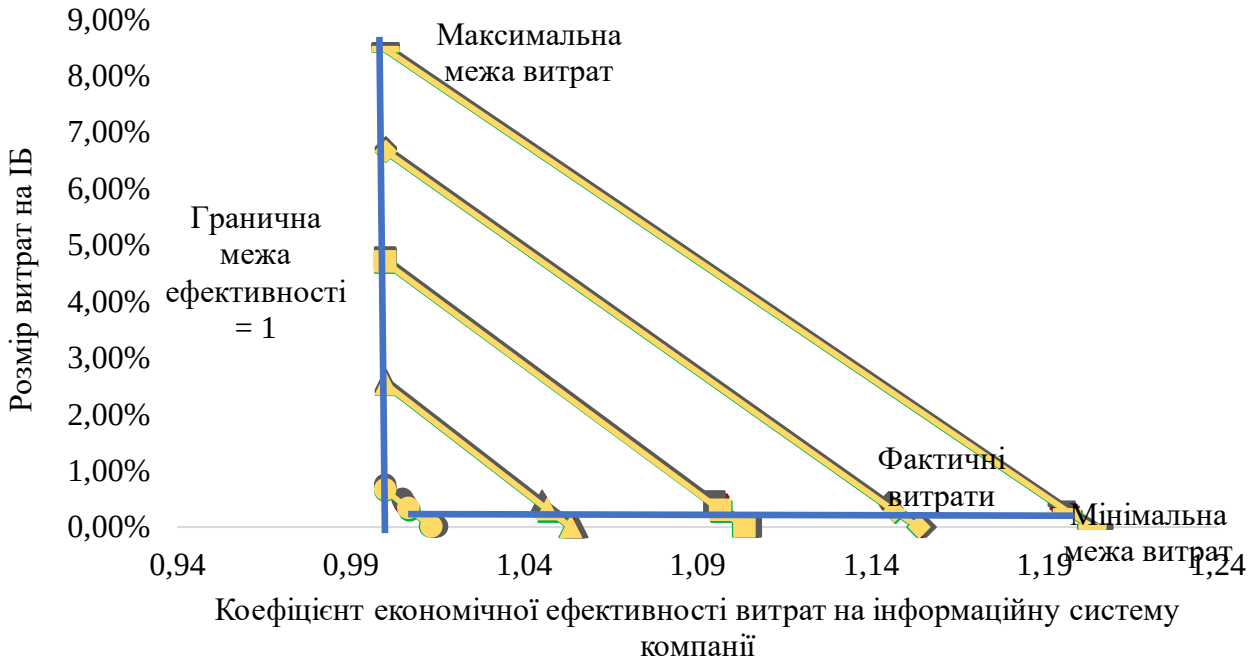


Рисунок И.2 – Співвідношення розміру витрат на інформаційну безпеку та коефіцієнту ефективності витрат на інформаційну систему для підприємств різних галузей із чисельністю від 1001 до 5000 осіб (складено авторкою)

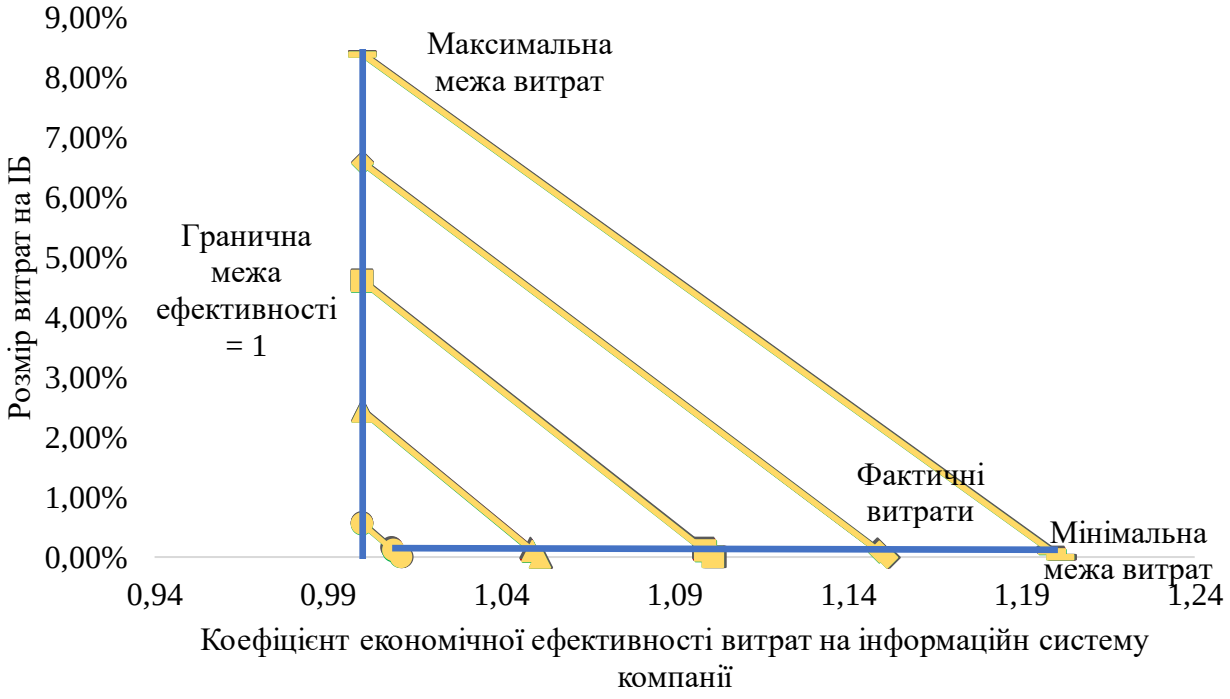


Рисунок И.3 – Співвідношення розміру витрат на інформаційну безпеку та коефіцієнту ефективності витрат на інформаційну систему для підприємств різних галузей із чисельністю від 5001 до 10000 осіб (складено авторкою)

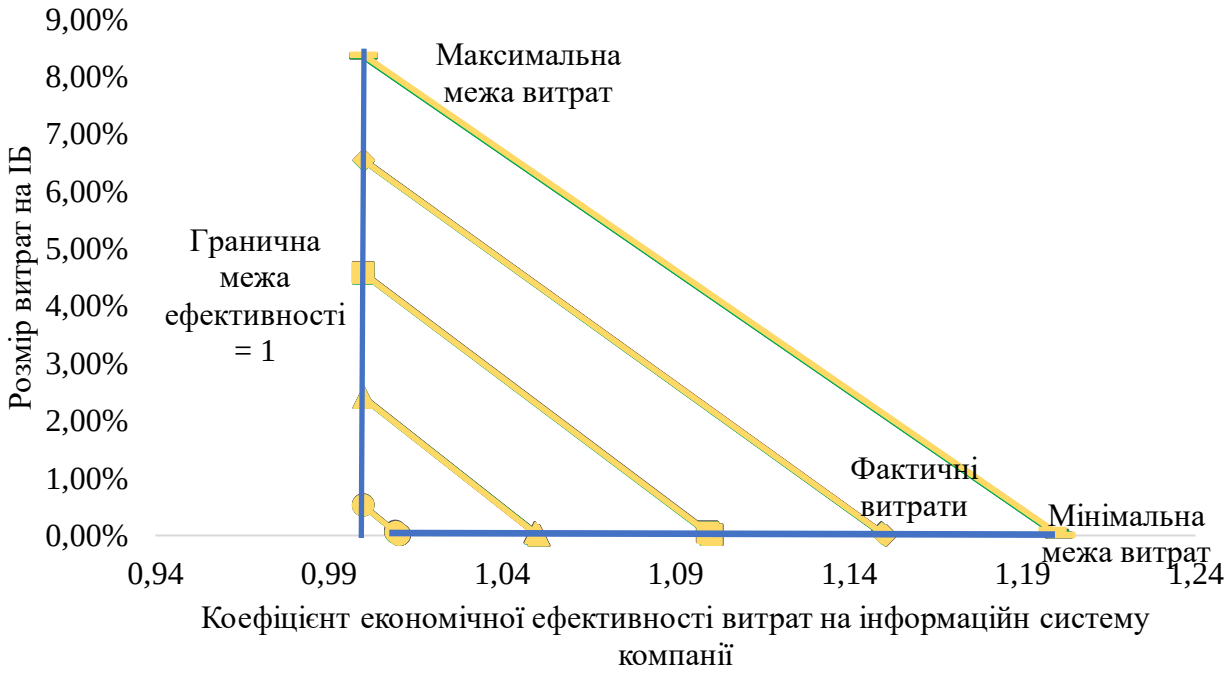


Рисунок И.4 – Співвідношення розміру витрат на інформаційну безпеку та коефіцієнту ефективності витрат на інформаційну систему для підприємств різних галузей із чисельністю від 10001 до 20000 осіб (складено авторкою)

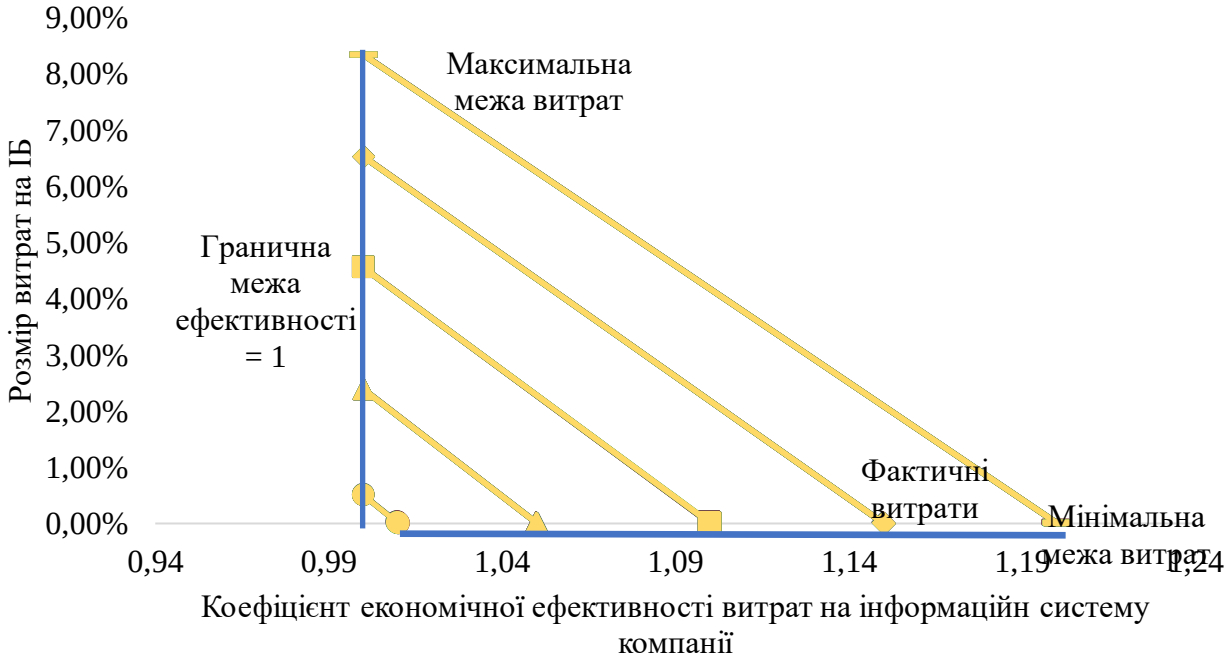


Рисунок И.5 – Співвідношення розміру витрат на інформаційну безпеку та коефіцієнту ефективності витрат на інформаційну систему для підприємств різних галузей із чисельністю більше 20000 осіб (складено авторкою)

Додаток К

Результати розрахунків за методикою побудови барицентричної моделі

Таблиця К.1 – Нормалізовані дані вхідних значень показників

Назва країни	GCI*	ICT DI	NRI	NCSI	DDL	CPI	DI	PCI	GEI	EDB	FD	GCI	EF	UEDI	HDI	SPI	HI
Albania	0,67	0,57	0,65	0,42	0,63	0,27	0,54	0,69	0,49	0,65	0,15	0,46	0,46	0,76	0,71	0,70	0,60
Algeria	0,27	0,52	0,53	0,13	0,54	0,25	0,24	0,38	0,36	0,23	0,10	0,39	0,01	0,42	0,65	0,62	0,69
Angola	0,10	0,21	0,00	0,07	0,23	0,03	0,25	0,51	0,21	0,11	0,09	0,00	0,10	0,06	0,31	0,18	0,50
Argentina	0,43	0,76	0,63	0,49	0,72	0,32	0,66	0,60	0,47	0,43	0,29	0,34	0,18	0,51	0,78	0,75	0,84
Armenia	0,53	0,64	0,71	0,31	0,70	0,25	0,39	0,48	0,46	0,74	0,22	0,48	0,55	0,66	0,65	0,69	0,57
Australia	0,96	0,91	0,92	0,61	0,95	0,85	0,91	0,86	0,85	0,87	0,91	0,85	0,82	0,89	0,97	0,97	0,95
Austria	0,89	0,89	0,90	0,71	0,92	0,83	0,81	0,83	0,81	0,84	0,65	0,87	0,62	0,83	0,93	0,94	0,94
Azerbaijan	0,70	0,69	0,71	0,37	0,72	0,11	0,14	0,41	0,44	0,70	0,16	0,75	0,45	0,48	0,64	0,58	0,68
Bahrain	0,63	0,84	0,85	0,25	0,87	0,27	0,15	0,37	0,50	0,63	0,42	0,69	0,53	0,58	0,79	0,62	0,80
Bangladesh	0,57	0,28	0,55	0,28	0,43	0,13	0,49	0,33	0,28	0,10	0,19	0,29	0,25	0,39	0,38	0,39	0,59
Belgium	0,87	0,87	0,90	0,89	0,91	0,82	0,75	0,70	0,74	0,70	0,66	0,86	0,52	0,86	0,94	0,95	0,91
Benin	0,52	0,21	0,48	0,47	0,36	0,32	0,51	0,56	0,32	0,30	0,07	0,14	0,28	0,14	0,21	0,34	0,54
Bhutan	0,18	0,41	0,63	0,17	0,54	0,72	0,45	0,88	0,55	0,59	0,16	0,41	0,40	0,50	0,39	0,60	0,67
Bolivia	0,14	0,48	0,55	0,28	0,53	0,17	0,50	0,52	0,38	0,28	0,28	0,14	0,00	0,13	0,55	0,60	0,75
Bosnia and Herzegovina	0,21	0,60	0,59	0,50	0,62	0,30	0,42	0,49	0,31	0,54	0,23	0,26	0,39	0,57	0,67	0,72	0,67
Botswana	0,47	0,51	0,58	0,21	0,56	0,62	0,75	0,85	0,54	0,57	0,22	0,55	0,58	0,29	0,59	0,57	0,47
Brazil	0,62	0,68	0,66	0,47	0,70	0,25	0,65	0,49	0,35	0,41	0,64	0,43	0,16	0,27	0,65	0,72	0,84
Bulgaria	0,77	0,77	0,69	0,53	0,75	0,35	0,66	0,72	0,53	0,69	0,35	0,65	0,54	0,67	0,75	0,77	0,65
Burundi	0,09	0,17	0,40	0,00	0,29	0,00	0,10	0,18	0,12	0,21	0,11	0,08	0,15	0,24	0,04	0,16	0,38

Продовження таблиці К.1

Назва країни	GCI*	ICT DI	NRI	NCSI	DDL	CPI	DI	PCI	GEI	EDB	FD	GCI	EF	UEDI	HDI	SPI	HI
Cambodia	0,16	0,37	0,57	0,14	0,48	0,04	0,25	0,62	0,32	0,36	0,11	0,33	0,33	0,40	0,33	0,31	0,58
Cameroon	0,46	0,27	0,50	0,21	0,39	0,11	0,21	0,23	0,27	0,21	0,07	0,17	0,17	0,20	0,29	0,28	0,65
Canada	0,96	0,87	0,93	0,58	0,93	0,90	0,91	0,86	0,88	0,85	0,94	0,90	0,75	0,86	0,94	0,97	0,96
Chad	0,10	0,14	0,36	0,17	0,26	0,03	0,01	0,21	0,09	0,04	0,04	0,04	0,12	0,07	0,00	0,00	0,56
Chile	0,47	0,73	0,77	0,58	0,77	0,70	0,77	0,71	0,72	0,70	0,48	0,76	0,70	0,46	0,81	0,84	0,85
China	0,89	0,62	0,70	0,35	0,68	0,31	0,22	0,52	0,58	0,57	0,65	0,81	0,31	0,34	0,65	0,59	0,69
Colombia	0,61	0,60	0,69	0,47	0,66	0,27	0,65	0,39	0,44	0,65	0,36	0,53	0,55	0,33	0,65	0,68	0,82
Congo (DR)	0,00	0,18	0,00	0,00	0,18	0,03	0,00	0,51	0,09	0,00	0,01	0,10	0,18	0,10	0,10	0,12	0,56
Costa Rica	0,23	0,71	0,74	0,54	0,76	0,55	0,79	0,72	0,55	0,66	0,26	0,66	0,48	0,57	0,71	0,85	0,93
Côte d'Ivoire	0,49	0,34	0,57	0,31	0,47	0,25	0,32	0,36	0,32	0,33	0,10	0,29	0,40	0,22	0,21	0,30	0,61
Croatia	0,90	0,80	0,71	0,86	0,79	0,44	0,61	0,81	0,57	0,69	0,48	0,47	0,38	0,79	0,79	0,83	0,70
Cyprus	0,70	0,87	0,77	0,42	0,84	0,59	0,73	0,73	0,68	0,70	0,55	0,54	0,53	0,50	0,85	0,88	0,75
Czech Republic	0,61	0,80	0,78	0,96	0,81	0,59	0,74	0,87	0,68	0,79	0,46	0,78	0,67	0,86	0,89	0,91	0,88
Denmark	0,91	0,97	0,93	0,85	0,98	1,00	0,92	0,84	0,91	0,95	0,66	0,91	0,73	0,96	0,96	1,00	0,99
Dominican Republic	0,46	0,50	0,59	0,42	0,57	0,18	0,60	0,60	0,36	0,48	0,14	0,26	0,39	0,50	0,62	0,60	0,69
Ecuador	0,39	0,53	0,65	0,35	0,61	0,24	0,57	0,57	0,40	0,43	0,13	0,31	0,10	0,38	0,65	0,68	0,78
Egypt	0,90	0,51	0,62	0,35	0,58	0,25	0,22	0,29	0,32	0,39	0,27	0,29	0,21	0,46	0,54	0,53	0,58
El Salvador	0,12	0,42	0,62	0,18	0,53	0,25	0,53	0,49	0,35	0,58	0,20	0,22	0,43	0,44	0,48	0,59	0,81
Estonia	0,98	0,90	0,90	0,94	0,93	0,79	0,77	0,75	0,75	0,88	0,25	0,79	0,78	0,80	0,87	0,89	0,75
Ethiopia	0,29	0,19	0,51	0,32	0,36	0,24	0,22	0,26	0,31	0,24	0,07	0,23	0,19	0,37	0,12	0,21	0,57
Finland	0,92	0,88	1,00	0,85	0,97	0,96	0,91	0,84	0,94	0,88	0,74	0,93	0,67	1,00	0,95	0,99	1,00
France	0,99	0,91	0,88	0,86	0,93	0,77	0,75	0,61	0,82	0,80	0,82	0,84	0,44	0,71	0,89	0,96	0,85
Georgia	0,92	0,64	0,71	0,54	0,70	0,58	0,48	0,48	0,61	0,92	0,26	0,52	0,72	0,54	0,70	0,69	0,57
Germany	0,91	0,93	0,93	0,83	0,96	0,89	0,86	0,75	0,85	0,85	0,75	0,96	0,67	0,82	0,97	0,98	0,91

Продовження таблиці К.1

Назва країни	GCI*	ICT DI	NRI	NCSI	DDL	CPI	DI	PCI	GEI	EDB	FD	GCI	EF	UEDI	HDI	SPI	HI
Ghana	0,47	0,46	0,58	0,31	0,53	0,34	0,61	0,59	0,41	0,42	0,09	0,21	0,27	0,39	0,35	0,52	0,61
Greece	0,57	0,80	0,69	1,00	0,77	0,39	0,69	0,64	0,54	0,64	0,50	0,38	0,30	0,77	0,85	0,88	0,70
Guatemala	0,26	0,38	0,58	0,28	0,49	0,14	0,49	0,46	0,30	0,50	0,17	0,40	0,43	0,26	0,45	0,52	0,84
Guyana	0,13	0,38	0,59	0,04	0,50	0,28	0,62	0,55	0,40	0,41	0,11	1,00	0,33	0,52	0,49	0,54	0,94
Haiti	0,04	0,19	0,42	0,08	0,31	0,04	0,41	0,43	0,00	0,04	0,07	0,09	0,26	0,04	0,18	0,33	0,47
Honduras	0,03	0,37	0,62	0,08	0,50	0,17	0,49	0,46	0,31	0,44	0,16	0,31	0,37	0,30	0,40	0,48	0,72
Hungary	0,87	0,77	0,73	0,67	0,78	0,41	0,61	0,79	0,58	0,71	0,39	0,57	0,51	0,73	0,80	0,84	0,74
Iceland	0,48	1,00	0,92	0,47	0,99	0,83	0,97	0,97	0,82	0,86	0,47	0,80	0,74	0,94	0,97	1,00	0,98
India	0,77	0,33	0,63	0,61	0,50	0,34	0,68	0,34	0,53	0,48	0,42	0,71	0,23	0,38	0,44	0,45	0,55
Indonesia	0,84	0,48	0,66	0,39	0,59	0,30	0,58	0,45	0,50	0,60	0,34	0,74	0,45	0,51	0,55	0,56	0,67
Iran (IR)	0,68	0,62	0,62	0,13	0,64	0,15	0,11	0,24	0,36	0,37	0,42	0,51	0,15	0,50	0,72	0,58	0,62
Ireland	0,84	0,89	0,88	0,65	0,92	0,79	0,91	0,87	0,80	0,86	0,68	0,83	0,81	0,91	0,98	0,98	0,91
Israel	0,84	0,88	0,90	0,67	0,92	0,62	0,75	0,36	0,75	0,72	0,58	0,89	0,63	0,40	0,91	0,87	0,94
Italy	0,90	0,78	0,73	0,79	0,78	0,49	0,74	0,69	0,56	0,72	0,79	0,69	0,41	0,83	0,87	0,93	0,79
Jamaica	0,43	0,53	0,65	0,28	0,61	0,38	0,66	0,71	0,58	0,61	0,25	0,50	0,56	0,59	0,59	0,75	0,77
Japan	0,95	0,93	0,93	0,64	0,96	0,79	0,78	0,87	0,87	0,78	0,93	0,94	0,63	0,90	0,93	0,99	0,78
Jordan	0,60	0,67	0,70	0,13	0,70	0,45	0,29	0,49	0,49	0,46	0,36	0,54	0,47	0,51	0,58	0,67	0,68
Kazakhstan	0,84	0,76	0,77	0,46	0,78	0,20	0,17	0,59	0,47	0,81	0,31	0,59	0,56	0,69	0,75	0,63	0,76
Kenya	0,80	0,32	0,63	0,35	0,49	0,14	0,43	0,29	0,36	0,57	0,14	0,35	0,24	0,24	0,32	0,44	0,58
Korea (Rep)	0,93	0,99	0,93	0,64	0,99	0,56	0,78	0,75	0,75	0,95	0,84	0,81	0,66	0,82	0,91	0,95	0,77
Kyrgyzstan	0,26	0,49	0,62	0,18	0,57	0,17	0,43	0,44	0,31	0,59	0,07	0,27	0,42	0,50	0,49	0,61	0,67
Laos	0,21	0,32	0,57	0,15	0,46	0,17	0,11	0,71	0,30	0,30	0,14	0,30	0,22	0,43	0,37	0,31	0,61
Latvia	0,80	0,81	0,80	0,74	0,83	0,58	0,70	0,71	0,71	0,85	0,22	0,61	0,66	0,70	0,82	0,82	0,78
Liberia	0,22	0,00	0,47	0,18	0,47	0,21	0,46	0,53	0,14	0,15	0,11	0,04	0,15	0,22	0,12	0,29	0,46
Lithuania	0,98	0,80	0,81	0,92	0,83	0,59	0,72	0,79	0,72	0,88	0,18	0,71	0,70	0,62	0,85	0,86	0,78
Luxembourg	0,96	0,94	0,94	0,64	0,98	0,90	0,87	0,96	0,89	0,65	0,75	0,86	0,72	0,93	0,92	0,98	0,91

Продовження таблиці К.1

Назва країни	GCI*	ICT DI	NRI	NCSI	DDL	CPI	DI	PCI	GEI	EDB	FD	GCI	EF	UEDI	HDI	SPI	HI
Madagascar	0,21	0,19	0,43	0,11	0,32	0,11	0,45	0,44	0,18	0,24	0,05	0,14	0,28	0,07	0,22	0,23	0,49
Malawi	0,29	0,19	0,45	0,19	0,33	0,21	0,48	0,48	0,29	0,45	0,03	0,06	0,18	0,16	0,15	0,32	0,47
Malaysia	0,96	0,71	0,81	0,75	0,79	0,42	0,64	0,66	0,72	0,83	0,66	0,84	0,68	0,59	0,73	0,72	0,83
Mali	0,09	0,24	0,48	0,18	0,37	0,21	0,47	0,05	0,22	0,34	0,08	0,12	0,30	0,28	0,05	0,27	0,58
Malta	0,51	0,88	0,80	0,51	0,86	0,52	0,80	0,93	0,70	0,57	0,56	0,74	0,55	0,87	0,88	0,91	0,87
Mauritania	0,11	0,26	0,42	0,10	0,34	0,14	0,28	0,43	0,29	0,30	0,05	0,05	0,22	0,40	0,23	0,22	0,57
Mauritius	0,95	0,66	0,73	0,49	0,71	0,48	0,80	0,83	0,67	0,84	0,42	0,68	0,69	0,77	0,72	0,75	0,77
Mexico	0,67	0,58	0,66	0,36	0,64	0,15	0,56	0,44	0,43	0,72	0,38	0,64	0,46	0,50	0,66	0,68	0,85
Moldova	0,71	0,72	0,66	0,51	0,71	0,23	0,52	0,49	0,35	0,73	0,17	0,36	0,32	0,62	0,56	0,64	0,74
Mongolia	0,50	0,56	0,71	0,10	0,65	0,28	0,60	0,82	0,41	0,62	0,38	0,28	0,26	0,44	0,60	0,60	0,67
Morocco	0,46	0,53	0,65	0,22	0,61	0,37	0,42	0,51	0,41	0,64	0,33	0,49	0,40	0,49	0,50	0,62	0,69
Mozambique	0,16	0,26	0,50	0,07	0,39	0,08	0,28	0,38	0,25	0,35	0,07	0,03	0,05	0,00	0,08	0,26	0,58
Myanmar	0,17	0,33	0,45	0,08	0,40	0,17	0,28	0,26	0,20	0,16	0,08	1,00	0,22	0,28	0,33	0,39	0,56
Namibia	0,07	0,43	0,59	0,10	0,53	0,51	0,57	0,78	0,49	0,48	0,38	0,36	0,32	0,21	0,44	0,63	0,58
Nepal	0,27	0,32	0,53	0,28	0,44	0,20	0,44	0,44	0,24	0,47	0,17	0,37	0,22	0,41	0,32	0,45	0,64
Netherlands	0,96	0,94	0,97	0,85	0,99	0,92	0,88	0,82	0,91	0,79	0,74	0,97	0,72	0,91	0,96	0,99	0,98
New Zealand	0,85	0,92	0,92	0,57	0,95	0,99	0,93	1,00	0,86	1,00	0,59	0,91	0,90	0,88	0,94	0,98	0,96
Nicaragua	0,13	0,37	0,47	0,21	0,43	0,11	0,26	0,35	0,27	0,38	0,09	0,34	0,33	0,24	0,45	0,56	0,80
Nigeria	0,70	0,29	0,53	0,56	0,42	0,14	0,35	0,04	0,21	0,30	0,20	0,11	0,32	0,19	0,24	0,14	0,68
Norway	0,96	0,94	0,97	0,64	0,98	0,94	1,00	0,90	0,92	0,92	0,66	0,92	0,68	0,98	1,00	1,00	0,99
Oman	0,93	0,71	0,71	0,33	0,74	0,49	0,18	0,77	0,51	0,62	0,40	0,56	0,38	0,62	0,78	0,64	0,90
Pakistan	0,43	0,27	0,57	0,43	0,43	0,23	0,32	0,00	0,31	0,33	0,20	0,18	0,23	0,43	0,29	0,34	0,72
Panama	0,39	0,54	0,71	0,49	0,65	0,28	0,66	0,67	0,46	0,59	0,32	0,64	0,51	0,36	0,71	0,71	0,84
Paraguay	0,64	0,47	0,57	0,58	0,53	0,17	0,57	0,58	0,34	0,45	0,13	0,20	0,40	0,28	0,58	0,59	0,74
Peru	0,42	0,54	0,63	0,40	0,60	0,25	0,61	0,53	0,40	0,64	0,36	0,49	0,55	0,33	0,65	0,67	0,74

Продовження таблиці К.1

Назва країни	GCI*	ICT DI	NRI	NCSI	DDL	CPI	DI	PCI	GEI	EDB	FD	GCI	EF	UEDI	HDI	SPI	HI
Philippines	0,68	0,52	0,66	0,32	0,61	0,27	0,62	0,31	0,47	0,40	0,34	0,60	0,47	0,52	0,56	0,57	0,72
Poland	0,88	0,77	0,74	0,72	0,78	0,61	0,62	0,73	0,62	0,82	0,45	0,72	0,55	0,82	0,85	0,85	0,80
Portugal	0,82	0,79	0,81	0,74	0,83	0,66	0,76	0,89	0,75	0,80	0,69	0,70	0,43	0,87	0,81	0,92	0,71
Qatar	0,92	0,80	0,86	0,57	0,86	0,63	0,20	0,77	0,61	0,58	0,47	0,82	0,64	0,54	0,81	0,68	0,83
Romania	0,61	0,72	0,69	0,74	0,72	0,42	0,58	0,61	0,40	0,73	0,27	0,51	0,57	0,69	0,75	0,75	0,78
Russian Federation	0,90	0,79	0,74	0,67	0,79	0,15	0,17	0,46	0,45	0,80	0,48	0,73	0,32	0,47	0,77	0,68	0,76
Rwanda	0,75	0,24	0,65	0,26	0,46	0,55	0,22	0,63	0,51	0,74	0,06	0,59	0,56	0,19	0,24	0,39	0,45
Saudi Arabia	0,95	0,74	0,80	0,60	0,79	0,45	0,05	0,45	0,54	0,51	0,40	0,79	0,35	0,53	0,82	0,59	0,83
Senegal	0,33	0,30	0,57	0,14	0,44	0,39	0,56	0,57	0,40	0,35	0,08	0,24	0,26	0,28	0,20	0,44	0,61
Serbia	0,68	0,73	0,66	0,81	0,72	0,31	0,59	0,60	0,49	0,74	0,20	0,44	0,41	0,61	0,72	0,72	0,71
Sierra Leone	0,14	0,00	0,00	0,01	0,00	0,18	0,38	0,57	0,19	0,25	0,00	0,07	0,17	0,17	0,07	0,27	0,60
Singapore	0,97	0,90	1,00	0,83	0,98	0,96	0,58	0,99	1,00	0,97	0,77	0,98	1,00	0,73	0,97	0,92	0,83
Slovakia	0,78	0,79	0,73	0,82	0,78	0,46	0,67	0,79	0,63	0,77	0,28	0,58	0,47	0,77	0,82	0,84	0,81
Slovenia	0,75	0,82	0,78	0,58	0,83	0,61	0,72	0,83	0,73	0,78	0,34	0,66	0,46	0,78	0,91	0,92	0,78
South Africa	0,70	0,56	0,70	0,26	0,64	0,37	0,69	0,54	0,54	0,56	0,65	0,56	0,42	0,30	0,55	0,61	0,62
Spain	0,97	0,87	0,80	0,92	0,86	0,58	0,79	0,67	0,70	0,82	0,89	0,76	0,47	0,77	0,89	0,95	0,83
Suriname	0,11	0,58	0,00	0,18	0,60	0,37	0,66	0,61	0,30	0,24	0,17	1,00	0,09	0,43	0,58	0,63	0,00
Sweden	0,87	0,93	0,97	0,58	0,98	0,96	0,94	0,84	0,90	0,89	0,79	0,95	0,72	0,92	0,97	0,98	0,96
Switzerland	0,85	0,97	0,97	0,79	1,00	0,96	0,90	0,95	0,95	0,78	1,00	0,99	0,84	0,89	0,99	1,00	0,98
Tajikistan	0,27	0,00	0,55	0,13	0,55	0,11	0,05	0,40	0,20	0,41	0,03	0,44	0,32	0,59	0,46	0,40	0,70
Tanzania	0,68	0,20	0,48	0,11	0,35	0,27	0,47	0,45	0,28	0,34	0,05	0,19	0,35	0,30	0,23	0,38	0,43
Thailand	0,86	0,63	0,70	0,43	0,69	0,27	0,37	0,39	0,55	0,82	0,75	0,77	0,51	0,54	0,66	0,63	0,80
Trinidad and Tobago	0,20	0,67	0,69	0,19	0,70	0,34	0,68	0,66	0,51	0,49	0,32	0,41	0,30	0,53	0,72	0,78	0,81
Tunisia	0,58	0,53	0,65	0,31	0,61	0,37	0,59	0,37	0,43	0,56	0,21	0,32	0,33	0,54	0,61	0,72	0,60

Продовження таблиці К.1

Назва країни	GCI*	ICT DI	NRI	NCSI	DDL	CPI	DI	PCI	GEI	EDB	FD	GCI	EF	UEDI	HDI	SPI	HI
Turkey	0,91	0,68	0,73	0,56	0,73	0,34	0,34	0,25	0,46	0,67	0,52	0,62	0,48	0,50	0,73	0,62	0,72
Uganda	0,66	0,24	0,51	0,51	0,39	0,13	0,44	0,41	0,31	0,40	0,05	0,19	0,40	0,30	0,23	0,40	0,55
Ukraine	0,71	0,62	0,70	0,65	0,68	0,21	0,50	0,11	0,36	0,62	0,16	0,42	0,17	0,69	0,63	0,66	0,54
United Arab Emirates	0,87	0,80	0,88	0,40	0,87	0,75	0,15	0,78	0,81	0,85	0,48	0,88	0,75	0,74	0,84	0,74	0,89
United Kingdom	1,00	0,97	0,94	0,81	0,99	0,89	0,84	0,61	0,79	0,92	0,94	0,94	0,76	0,64	0,94	0,98	0,89
United States	1,00	0,91	0,97	0,82	0,97	0,76	0,77	0,72	0,84	0,92	0,93	0,99	0,71	0,68	0,94	0,91	0,90
Uruguay	0,73	0,80	0,74	0,49	0,80	0,75	0,82	0,87	0,60	0,52	0,27	0,46	0,56	0,72	0,74	0,83	0,84
Vietnam	0,74	0,49	0,65	0,33	0,59	0,23	0,19	0,62	0,46	0,61	0,39	0,61	0,20	0,62	0,53	0,66	0,67
Zambia	0,47	0,28	0,53	0,42	0,42	0,25	0,49	0,62	0,33	0,54	0,08	0,16	0,23	0,01	0,34	0,44	0,57

** GCI – Глобальний індекс кібербезпеки; ICT DI – Індекс розвитку ІКТ; NRI – Індекс мережевої готовності; NCSI – Національний індекс кібербезпеки; DDL – Рівень цифрового розвитку; CPI – Індекс сприйняття корупції; DI – Індекс демократії; PCI – Індекс політичної стабільності; GEI – Індекс ефективності уряду; EDB – Індекс легкості ведення бізнесу; FD – Індекс фінансового розвитку; GCI – Індекс глобальної конкурентоспроможності; EF – Індекс економічної свободи; UEDI – Індекс нерівномірного економічного розвитку; HDI – Індекс людського розвитку; SPI – Індекс соціального прогресу; HI – Індекс щастя.*

Таблиця К.2 – Результати розрахованих значень інтегральних індексів для розвинутих країн

Назва країни	Вимір ЦСіКБ	Еконо-мічний вимір	Соціаль-ний вимір	Політичний вимір	Соціо-політичний	Економіко-ЦСіКБ
Switzerland	0,9106	0,8973	0,9876	0,9394	172,73	187,27
Denmark	0,9265	0,8321	0,9809	0,9184	171,10	188,90
Norway	0,8867	0,8191	0,9982	0,9390	165,45	194,55
Finland	0,9214	0,8338	0,9799	0,9106	171,45	188,55
Netherlands	0,9384	0,8212	0,9745	0,8812	173,82	186,18
Singapore	0,9334	0,8827	0,9045	0,8618	183,18	176,82
Sweden	0,8517	0,8504	0,9689	0,9111	168,69	191,31
New Zealand	0,8279	0,8422	0,9604	0,9429	165,06	194,94
Australia	0,8571	0,8681	0,9646	0,8641	173,51	186,49
Canada	0,8394	0,8556	0,9590	0,8866	170,35	189,65
Germany	0,9134	0,8053	0,9560	0,8360	175,27	184,73
Luxembourg	0,8809	0,7786	0,9355	0,9049	167,99	192,01
United Kingdom	0,9373	0,8306	0,9353	0,7715	184,33	175,67
United States	0,9303	0,8357	0,9177	0,7722	185,28	174,72
Ireland	0,8296	0,8149	0,9566	0,8418	170,01	189,99
Japan	0,8727	0,8262	0,8942	0,8251	178,68	181,32
Iceland	0,7285	0,7410	0,9850	0,8918	152,41	207,59
Austria	0,8578	0,7563	0,9357	0,8220	170,29	189,71
Korea (Rep)	0,8853	0,8129	0,8743	0,7042	188,87	171,13
Belgium	0,8863	0,7087	0,9328	0,7524	173,72	186,28
France	0,9137	0,7036	0,8985	0,7333	178,62	181,38
Estonia	0,9294	0,6399	0,8353	0,7650	175,96	184,04
Spain	0,8809	0,7246	0,8873	0,6810	183,11	176,89
Czech Republic	0,7840	0,6962	0,8917	0,7139	171,27	188,73
Portugal	0,7961	0,6796	0,8097	0,7626	172,46	187,54
Lithuania	0,8659	0,5485	0,8298	0,7013	168,71	191,29
Israel	0,8333	0,6221	0,9099	0,5954	177,55	182,45
Malta	0,6930	0,6446	0,8860	0,7219	159,66	200,34
Italy	0,7955	0,6714	0,8611	0,6126	180,70	179,30
Slovenia	0,7466	0,5766	0,8672	0,7182	159,22	200,78
Latvia	0,7960	0,5566	0,8061	0,6720	168,72	191,28
Slovakia	0,7810	0,5386	0,8244	0,6284	168,38	191,62
Cyprus	0,6952	0,5591	0,8280	0,6800	159,11	200,89
Greece	0,7507	0,4871	0,8065	0,5550	168,87	191,13

Таблиця К.3 – Результати розрахованих значень інтегральних індексів для країн, що розвиваються

Назва країни	Вимір ЦСіКБ	Еконо-мічний вимір	Соціаль-ний вимір	Політич-ний вимір	Соціо-політич-ний	Економіко-ЦСіКБ
Poland	0,7773	0,6533	0,8357	0,6410	176,98	183,02
United Arab Emirates	0,7353	0,7239	0,8220	0,5168	192,56	167,44
Mauritius	0,6912	0,6609	0,7457	0,6803	174,01	185,99
Uruguay	0,7001	0,4807	0,7977	0,7509	147,97	212,03
Croatia	0,8090	0,5411	0,7696	0,5915	177,82	182,18
Hungary	0,7595	0,5675	0,7908	0,5824	176,28	183,72
Qatar	0,7919	0,5998	0,7732	0,4966	191,77	168,23
Bulgaria	0,6932	0,5636	0,7214	0,5442	179,72	180,28
Costa Rica	0,5481	0,4973	0,8241	0,6440	142,81	217,19
Romania	0,6939	0,5242	0,7585	0,4957	178,17	181,83
Georgia	0,6934	0,5473	0,6498	0,5335	185,12	174,88
Serbia	0,7204	0,4415	0,7173	0,4804	175,62	184,38
Oman	0,6500	0,5021	0,7678	0,4342	178,85	181,15
Russia	0,7752	0,5283	0,7331	0,2718	215,84	144,16
Kazakhstan	0,7053	0,5659	0,7112	0,3108	210,71	149,29
Saudi Arabia	0,7685	0,4953	0,7402	0,2752	211,10	148,90
Panama	0,5441	0,4666	0,7522	0,4882	159,49	200,51
Jamaica	0,4806	0,4792	0,6980	0,5676	149,46	210,54
Bahrain	0,6294	0,5608	0,7316	0,2928	205,66	154,34
Colombia	0,6003	0,4697	0,7151	0,4152	177,16	182,84
Albania	0,5792	0,4336	0,6682	0,4695	167,59	192,41
Trinidad and Tobago	0,4140	0,4020	0,7680	0,5261	131,53	228,47
Peru	0,5122	0,4594	0,6871	0,4250	168,01	191,99
Moldova	0,6589	0,3913	0,6416	0,3759	183,58	176,42
Armenia	0,5536	0,4873	0,6323	0,3844	185,78	174,22
Jordan	0,4763	0,4636	0,6416	0,4202	168,83	191,17
Tunisia	0,5181	0,3685	0,6432	0,4308	159,46	200,54
Morocco	0,4635	0,4598	0,5959	0,4221	170,66	189,34
Azerbaijan	0,6211	0,4467	0,6314	0,2300	212,23	147,77
Mongolia	0,4162	0,3763	0,6230	0,4859	143,21	216,79
Bosnia and Herzegovina	0,4691	0,3734	0,6850	0,3707	159,90	200,10
Ukraine	0,6716	0,3478	0,6078	0,2517	201,21	158,79
Dominican Republic	0,5023	0,3200	0,6370	0,3946	155,82	204,18
Ecuador	0,4921	0,2304	0,6993	0,4204	131,59	228,41
Paraguay	0,5553	0,2639	0,6350	0,3690	155,70	204,30
Namibia	0,2440	0,3385	0,5442	0,5752	109,50	250,50
Guyana	0,2278	0,3781	0,6300	0,4408	118,79	241,21
El Salvador	0,3130	0,3446	0,6129	0,3919	136,33	223,67
Ghana	0,4578	0,2423	0,4809	0,4733	141,47	218,53

Продовження таблиці К.3

Назва країни	Вимір ЦСіКБ	Економічний вимір	Соціальний вимір	Політичний вимір	Соціополітичний	Економіко-ЦСіКБ
Guatemala	0,3789	0,3271	0,5811	0,3109	159,55	200,45
Kyrgyzstan	0,3812	0,2947	0,5860	0,3173	152,85	207,15
Bolivia	0,3524	0,1584	0,6276	0,3610	111,48	248,52
Kenya	0,4880	0,2787	0,4341	0,2820	185,68	174,32
Algeria	0,3486	0,1365	0,6542	0,3002	113,54	246,46
Nicaragua	0,2879	0,2458	0,5881	0,2275	147,67	212,33
Honduras	0,1986	0,3002	0,5183	0,3304	124,32	235,68
Suriname	0,2516	0,2761	0,3383	0,4591	135,61	224,39
Côte d'Ivoire	0,4245	0,2453	0,3353	0,3113	179,86	180,14
Tajikistan	0,2651	0,2545	0,5062	0,1467	175,42	184,58
Cameroon	0,3461	0,1549	0,3770	0,1961	163,66	196,34

Таблиця К.4 – Результати розрахованих значень інтегральних індексів для нових індустріальних країн

Назва країни	Вимір ЦСіКБ	Економічний вимір	Соціальний вимір	Політичний вимір	Соціополітичний	Економіко-ЦСіКБ
Malaysia	0,7993	0,7131	0,7568	0,6007	192,837	167,163
Chile	0,6527	0,6054	0,8333	0,7271	155,7614	204,2386
Thailand	0,6454	0,6683	0,6911	0,3815	206,7736	153,2264
Turkey	0,7120	0,5525	0,6895	0,3407	207,3914	152,6086
Argentina	0,5908	0,3328	0,7884	0,4951	143,6746	216,3254
Mexico	0,5688	0,5247	0,7266	0,3580	187,3892	172,6108
China	0,6199	0,5019	0,6383	0,3772	194,0797	165,9203
South Africa	0,5397	0,4837	0,5917	0,5203	170,5949	189,4051
Indonesia	0,5712	0,5120	0,5930	0,4459	185,7107	174,2893
Brazil	0,6196	0,3455	0,7327	0,4119	161,8422	198,1578
Philippines	0,5406	0,4572	0,6131	0,3957	181,0426	178,9574
Vietnam	0,5404	0,4471	0,6136	0,3330	189,1255	170,8745
India	0,5471	0,4179	0,4798	0,4507	183,1667	176,8333
Egypt	0,5648	0,3100	0,5486	0,2687	188,9465	171,0535
Iran (IR)	0,4616	0,3590	0,6342	0,1980	193,4692	166,5308
Bangladesh	0,3992	0,2201	0,4442	0,2757	162,2684	197,7316
Pakistan	0,4140	0,2594	0,4119	0,2031	193,1408	166,8592
Nigeria	0,4788	0,2097	0,2813	0,1478	223,9354	136,0646

Таблиця К.5 – Результати розрахованих значень інтегральних індексів для найменш розвинутих країн

Назва країни	Вимір ЦСіКБ	Еконо-мічний вимір	Соціаль-ний вимір	Політич-ний вимір	Соціо-політичний	Економіко-ЦСіКБ
Botswana	0,4390	0,4110	0,5409	0,6814	140,17	219,83
Bhutan	0,3356	0,3800	0,5400	0,6322	125,97	234,03
Rwanda	0,4279	0,3027	0,3478	0,4447	170,07	189,93
Nepal	0,3557	0,3056	0,4526	0,3102	165,68	194,32
Senegal	0,3212	0,2175	0,3788	0,4719	129,13	230,87
Zambia	0,4135	0,1119	0,4422	0,3982	119,07	240,93
Uganda	0,4404	0,2148	0,3685	0,2921	173,08	186,92
Benin	0,3886	0,1629	0,3423	0,4155	138,55	221,45
Laos	0,3051	0,2595	0,4110	0,2474	166,17	193,83
Tanzania	0,3026	0,2038	0,3367	0,3532	143,71	216,29
Cambodia	0,2957	0,2788	0,3891	0,2150	179,19	180,81
Myanmar	0,2450	0,2389	0,4174	0,2241	154,58	205,42
Malawi	0,2762	0,1174	0,2856	0,3435	124,07	235,93
Ethiopia	0,3177	0,1926	0,2475	0,2568	177,90	182,10
Mauritania	0,2078	0,1452	0,3059	0,2635	126,68	233,32
Madagascar	0,2261	0,1249	0,2916	0,2530	129,04	230,96
Mali	0,2323	0,1940	0,1954	0,1791	194,38	165,62
Mozambique	0,2238	0,0911	0,2311	0,2185	133,87	226,13
Liberia	0,2449	0,1178	0,2490	0,2901	132,10	227,90
Haiti	0,1548	0,0786	0,3059	0,1948	101,74	258,26
Sierra Leone	0,0295	0,0055	0,2211	0,2932	15,83	344,17
Angola	0,1170	0,0699	0,3016	0,1660	92,24	267,76
Chad	0,1855	0,0550	0,1455	0,0527	192,96	167,04
Burundi	0,1753	0,1459	0,1329	0,0983	217,28	142,72
Congo (DR)	0,0678	0,0761	0,1908	0,1307	98,95	261,05

Таблиця К.6 – Результати розрахованих координат центру мас та відхилень від еталонного значення

Назва країни	X	Y	Відхи-лення	Країни	X	Y	Відхи-лення
Albania	0,1132	-0,0103	0,1136	Ethiopia	0,0421	0,0165	0,0452
Algeria	0,1961	-0,0586	0,2047	Finland	0,0527	0,0007	0,0527
Angola	0,0591	-0,0265	0,0647	France	0,1263	0,0047	0,1264
Argentina	0,1888	-0,0244	0,1904	Georgia	0,0879	0,0047	0,0881
Armenia	0,0993	-0,0185	0,1010	Germany	0,0759	-0,0024	0,0759
Australia	0,0286	-0,0127	0,0312	Ghana	0,0920	0,0158	0,0934
Austria	0,0717	-0,0034	0,0717	Greece	0,1737	-0,0040	0,1738
Azerbaijan	0,1809	-0,0113	0,1812	Guatemala	0,0954	-0,0301	0,1000
Bahrain	0,1567	-0,0293	0,1594	Guyana	-0,0081	-0,0287	0,0299
Bangladesh	0,1186	-0,0046	0,1187	Haiti	0,0678	-0,0207	0,0709
Belgium	0,1195	-0,0025	0,1196	Honduras	0,0105	-0,0279	0,0298
Benin	0,0755	0,0302	0,0813	Hungary	0,1331	-0,0034	0,1332
Bhutan	-0,0450	0,0125	0,0467	Iceland	0,0238	-0,0133	0,0273
Bolivia	0,1650	-0,0435	0,1706	India	0,0543	0,0122	0,0556
Bosnia and Herzegovina	0,1248	-0,0325	0,1289	Indonesia	0,0673	-0,0086	0,0678
Botswana	-0,0330	0,0232	0,0403	Iran (IR)	0,1585	-0,0349	0,1623
Brazil	0,1987	-0,0164	0,1993	Ireland	0,0415	-0,0122	0,0432
Bulgaria	0,1010	-0,0055	0,1011	Israel	0,1713	-0,0134	0,1718
Burundi	0,0215	0,0018	0,0216	Italy	0,1208	-0,0138	0,1215
Cambodia	0,0578	-0,0171	0,0603	Jamaica	0,0392	-0,0173	0,0428
Cameroon	0,1273	-0,0042	0,1273	Japan	0,0383	-0,0027	0,0384
Canada	0,0176	-0,0102	0,0203	Jordan	0,0708	-0,0246	0,0750
Chad	0,0759	0,0095	0,0765	Kazakhstan	0,1717	-0,0148	0,1723
Chile	0,0497	-0,0100	0,0507	Kenya	0,1226	0,0095	0,1229
China	0,1220	-0,0114	0,1226	Korea (Rep)	0,0800	-0,0087	0,0804
Colombia	0,1362	-0,0208	0,1377	Kyrgyzstan	0,1081	-0,0297	0,1122
Congo (DR)	0,0115	-0,0093	0,0148	Laos	0,0644	-0,0158	0,0663
Costa Rica	0,0717	-0,0219	0,0750	Latvia	0,1294	0,0083	0,1296
Côte d'Ivoire	0,0727	0,0196	0,0753	Liberia	0,0433	0,0151	0,0459
Croatia	0,1522	0,0100	0,1525	Lithuania	0,1578	0,0181	0,1588
Cyprus	0,0953	-0,0072	0,0956	Luxembourg	0,0459	0,0065	0,0463
Czech Republic	0,0863	-0,0122	0,0872	Madagascar	0,0552	-0,0007	0,0552
Denmark	0,0530	0,0022	0,0530	Malawi	0,0561	0,0183	0,0590
Dominican Republic	0,1406	-0,0173	0,1417	Malaysia	0,0802	-0,0048	0,0804
Ecuador	0,1921	-0,0293	0,1943	Mali	0,0182	0,0033	0,0185
Egypt	0,1756	0,0009	0,1756	Malta	0,0674	-0,0167	0,0694
El Salvador	0,0484	-0,0317	0,0579	Mauritania	0,0388	-0,0039	0,0390
Estonia	0,1263	0,0249	0,1287	Mauritius	0,0314	-0,0044	0,0318

Продовження таблиці К.6

Назва країни	X	Y	Відхи-лення	Країни	X	Y	Відхи-лення
Mexico	0,1254	-0,0328	0,1296	Senegal	0,0156	0,0208	0,0260
Moldova	0,1774	0,0020	0,1775	Serbia	0,1745	0,0032	0,1746
Mongolia	0,0551	-0,0165	0,0575	Sierra Leone	0,0410	-0,0280	0,0497
Morocco	0,0544	-0,0197	0,0579	Singapore	0,0311	0,0012	0,0312
Mozambique	0,0625	0,0078	0,0630	Slovakia	0,1492	0,0006	0,1492
Myanmar	0,0560	-0,0240	0,0610	Slovenia	0,1086	-0,0041	0,1086
Namibia	-0,0477	0,0041	0,0479	South Africa	0,0422	-0,0029	0,0423
Nepal	0,0607	-0,0128	0,0620	Spain	0,1196	-0,0046	0,1197
Netherlands	0,0708	0,0014	0,0708	Suriname	-0,0469	0,0173	0,0500
New Zealand	0,0006	-0,0035	0,0036	Sweden	0,0189	-0,0068	0,0201
Nicaragua	0,1098	-0,0467	0,1194	Switzerland	0,0202	-0,0043	0,0206
Nigeria	0,1355	0,0366	0,1403	Tajikistan	0,0982	-0,0404	0,1062
Norway	0,0427	-0,0009	0,0427	Tanzania	0,0344	0,0100	0,0358
Oman	0,1522	-0,0222	0,1538	Thailand	0,0942	-0,0268	0,0979
Pakistan	0,1176	-0,0026	0,1176	Trinidad and Tobago	0,0714	-0,0343	0,0792
Panama	0,1056	-0,0271	0,1090	Tunisia	0,1189	-0,0145	0,1198
Paraguay	0,1933	-0,0097	0,1935	Turkey	0,1635	-0,0091	0,1637
Peru	0,0963	-0,0264	0,0999	Uganda	0,1090	0,0181	0,1105
Philippines	0,0959	-0,0148	0,0971	Ukraine	0,2214	0,0083	0,2216
Poland	0,1044	-0,0089	0,1048	United Arab Emirates	0,1011	-0,0275	0,1048
Portugal	0,0560	0,0067	0,0564	United Kingdom	0,0893	-0,0053	0,0895
Qatar	0,1533	-0,0047	0,1533	United States	0,0794	-0,0044	0,0796
Romania	0,1406	-0,0117	0,1411	Uruguay	0,1003	0,0110	0,1009
Russian Federation	0,2251	-0,0039	0,2252	Vietnam	0,1177	-0,0182	0,1191
Rwanda	0,0127	0,0266	0,0295	Zambia	0,1610	0,0090	0,1612
Saudi Arabia	0,2342	-0,0043	0,2343				

Додаток Л

Результати експрес-оцінювання ризиків втрати інформації

Таблиця Л.1 – Вхідні дані, які відображають втрати від витоків даних та частоту повторення факторів впливу

№	Назва фактору впливу	Суми грошових збитків від втрати інформації					Частота повторення				
		Людський фактор	Віруси та шкідливі програми	Технічний ризик	Кримінальний ризик	Пошкодження ПЗ	Людський фактор	Віруси та шкідливі	Технічний ризик	Кримінальний ризик	Пошкодження ПЗ
01	Навмисне видалення файлів даних або розділів тексту	100000	0	0	0	0	4	0	0	0	0
02	Ненавмисне видалення файлів даних або розділів тексту	120000	0	0	0	0	8	0	0	0	0
03	Навмисне не зберігання інформації	500000	0	0	0	0	7	0	0	0	0
04	Ненавмисне не зберігання інформації	120000	0	0	0	0	8	0	0	0	0
05	Перезапис важливих файлів	5000	0	0	0	0	1	0	0	0	0
06	Випадкове форматування жорсткого диска	400	0	0	0	0	1	0	0	0	0
07	Пролив рідини	8000	0	0	0	0	3	0	0	0	0
08	Навмисна помилка	700000	0	0	0	0	7	0	0	0	0
09	Ненавмисна помилка	50000	0	0	0	0	6	0	0	0	0
10	Використання інших імен користувачів та паролів	58000	0	0	0	0	4	0	0	0	0
11	Крадіжка інформації працівниками	466464	0	0	0	0	8	0	0	0	0
12	Порушення правил та процедур роботи з інформацією	2626	0	0	0	0	3	0	0	0	0
13	Відсутність антивірусних оновлень	0	6500	0	0	0	0	1	0	0	0
14	Відсутність сканування антивірусом	0	10000	0	0	0	0	1	0	0	0

Продовження таблиці Л.1

№	Назва фактору впливу	Суми грошових збитків від втрати інформації					Частота повторення				
		Людський фактор	Віруси та шкідливі програми	Технічний ризик	Криміналь ний ризик	Пошкод-ження ПЗ	Людський фактор	Віруси та шкідливі	Технічний ризик	Криміналь ний ризик	Пошкод-ження ПЗ
15	Втрата інформації через вірус	0	500000	0	0	0	0	9	0	0	0
16	Псування вірусом	0	300000	0	0	0	0	9	0	0	0
17	Навмисна активація електронною поштою вірусу користувачем	0	20000	0	0	0	0	6	0	0	0
18	Ненавмисна активація вірусного повідомлення користувачем	0	20000	0	0	0	0	6	0	0	0
19	Навмисне відключення антивірусного програмного забезпечення	0	25000	0	0	0	0	4	0	0	0
20	Ненавмисне відключення антивірусного програмного забезпечення	0	30000	0	0	0	0	4	0	0	0
21	Антивірусний помилковий сигнал	0	5000	0	0	0	0	1	0	0	0
22	Видалення важливої інформації антивірусом	0	800	0	0	0	0	1	0	0	0
23	Механічна несправність жорсткого диска	0	0	878	0	0	0	0	3	0	0
24	Пошкодження комп’ютера через перегрів	0	0	7000	0	0	0	0	1	0	0
25	Пошкодження комп'ютера через скупчення пилу в комп'ютері	0	0	15000	0	0	0	0	6	0	0
26	Навмисне падіння або поштовх комп’ютера	0	0	1000	0	0	0	0	1	0	0
27	Ненавмисне падіння або поштовх комп’ютера	0	0	5000	0	0	0	0	1	0	0
28	Смерч, землетрус та інші стихійні лиха	0	0	0	0	0	0	0	0	0	0
29	Вогонь	0	0	500000	0	0	0	0	7	0	0
30	Планове відключення електроенергії	0	0	0	0	0	0	0	0	0	0
31	Незаплановане відключення	0	0	40000	0	0	0	0	4	0	0

Продовження таблиці Л.1

№	Назва фактору впливу	Суми грошових збитків від втрати інформації					Частота повторення				
		Людський фактор	Віруси та шкідливі програми	Технічний ризик	Кримінальний ризик	Пошкодження ПЗ	Людський фактор	Віруси та шкідливі	Технічний ризик	Кримінальний ризик	Пошкодження ПЗ
	електроенергії										
32	Навмисне вимкнення комп'ютера без збереження інформації	0	0	700000	0	0	0	0	7	0	0
33	Ненавмисне вимкнення комп’ютера без збереження інформації	0	0	65000	0	0	0	0	6	0	0
34	Конфлікт між пристроями	0	0	5000	0	0	0	0	1	0	0
35	Вхід за допомогою чужого логіна	0	0	0	50000	0	0	0	0	4	0
36	Крадіжка комп’ютера	0	0	0	7000	0	0	0	0	1	0
37	Втрата комп’ютера	0	0	0	0	0	0	0	0	0	0
38	Копіювання інформації на знімний носій	0	0	0	100000	0	0	0	0	4	0
39	Надсилання інформації на зовнішню електронну адресу	0	0	0	250000	0	0	0	0	7	0
40	Крадіжка інформації	0	0	0	500000	0	0	0	0	7	0
41	Заміна інформації	0	0	0	54000	0	0	0	0	4	0
42	Несанкціоноване використання прав адміністратора	0	0	0	80000	0	0	0	0	4	0
43	Соціальна інженерія	0	0	0	400	0	0	0	0	2	0
44	DoS-атака	0	0	0	10000	0	0	0	0	1	0
45	Напад смурфа	0	0	0	0	0	0	0	0	0	0
46	UDP шторм	0	0	0	0	0	0	0	0	0	0
47	UDP-бомба	0	0	0	0	0	0	0	0	0	0
48	Нюхаючи	0	0	0	0	0	0	0	0	0	0
49	IP викрадення	0	0	0	0	0	0	0	0	0	0
50	Фіктивний DNS-сервер	0	0	0	10000000	0	0	0	0	7	0
51	IP-спуфінг	0	0	0	45000	0	0	0	0	4	0

Продовження таблиці Л.1

№	Назва фактору впливу	Суми грошових збитків від втрати інформації					Частота повторення				
		Людський фактор	Віруси та шкідливі програми	Технічний ризик	Криміналь ний ризик	Пошкод-ження ПЗ	Людський фактор	Віруси та шкідливі	Технічний ризик	Криміналь ний ризик	Пошкод-ження ПЗ
52	Втрата інформації через шифрування / дешифрування	0	0	0	52525	0	0	0	0	4	0
53	Злом ключів шифрування	0	0	0	626262	0	0	0	0	7	0
54	Несподівані або неправильні вимкнення програмного забезпечення	0	0	0	0	1000	0	0	0	0	1
55	Відсутність оновлень програмного забезпечення	0	0	0	0	20000	0	0	0	0	4
56	Переформатування під час оновлення системи	0	0	0	0	15000	0	0	0	0	4
57	Помилки в реєстрах Windows	0	0	0	0	12000	0	0	0	0	5
58	Програма не відповідає	0	0	0	0	20001	0	0	0	0	4
59	Неточне видалення або встановлення програмного забезпечення	0	0	0	0	25000	0	0	0	0	5
60	Помилки в драйверах	0	0	0	0	10000	0	0	0	0	2
61	Помилки обчислення	0	0	0	0	500000	0	0	0	0	9
62	Логічні помилки	0	0	0	0	120000	0	0	0	0	9
63	Помилки вводу-виводу даних	0	0	0	0	25000	0	0	0	0	6
64	Помилки обробки даних	0	0	0	0	35000	0	0	0	0	6
65	Помилки сумісності	0	0	0	0	66500	0	0	0	0	4
66	Помилки сполучення	0	0	0	0	30000	0	0	0	0	4

	A	B	C	D	E	F	G	I	J	K	L	M	O	P	Q	R	S	U	V	W	X	Y
1	1																					
2			HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC
7	05	Перезапис важливих файлів	1	0	0	0	0	4	0	0	0	0	1	1	1	1	1	4	1	2	3	5
8	06	Випадкове форматування жорсткого диска	1	0	0	0	0	4	0	0	0	0	1	1	1	1	1	4	1	2	3	5
15	13	Відсутність антивірусних оновлень	0	1	0	0	0	0	1	0	0	0	1	1	1	1	1	4	1	2	3	5
16	14	Відсутність сканування антивірусом	0	1	0	0	0	0	1	0	0	0	1	1	1	1	1	4	1	2	3	5
23	21	Антивірусний помилковий сигнал	0	1	0	0	0	0	1	0	0	0	1	1	1	1	1	4	1	2	3	5
24	22	Видалення важливої інформації антивірусом	0	1	0	0	0	0	1	0	0	0	1	1	1	1	1	4	1	2	3	5
26	24	Пошкодження комп'ютера через перегрів	0	0	1	0	0	0	0	2	0	0	1	1	1	1	1	4	1	2	3	5
28	26	Навмисне падіння або поштовх комп'ютера	0	0	1	0	0	0	0	2	0	0	1	1	1	1	1	4	1	2	3	5
29	27	Ненавмисне падіння або поштовх комп'ютера	0	0	1	0	0	0	0	2	0	0	1	1	1	1	1	4	1	2	3	5
36	34	Конфлікт між пристроями	0	0	1	0	0	0	0	2	0	0	1	1	1	1	1	4	1	2	3	5
38	36	Крадіжка комп'ютера	0	0	0	1	0	0	0	0	3	0	1	1	1	1	1	4	1	2	3	5
46	44	DoS-атака	0	0	0	1	0	0	0	0	3	0	1	1	1	1	1	4	1	2	3	5
56	54	Несподівані або неправильні вимкнення програмного забезпечення	0	0	0	0	1	0	0	0	0	5	1	1	1	1	1	4	1	2	3	5
69			2	4	4	2	1	0	0	0	0	0	13	13	13	13	13	4	1	2	3	5
70			1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	5	2	3	4	6
71			4	1	2	3	5	0,2	0,5	0,333	0,25	0,167	1	1	1	1	1	20				
72								5										0,25				

Рисунок Л.1 – Результати розрахунків для 1-го сектору карти ризиків

	A	B	C	D	E	F	G	I	J	K	L	M	O	P	Q	R	S	U	V	W	X	Y
1	2																					
2			HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC
45	43	Соціальна інженерія	0	0	0	1	0	0	0	0	2	0	1	1	1	1	1	3	3	3	2	1
62	60	Помилки в драйверах	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	3	3	3	2	1
69			0	0	0	1	1	0	0	0	1	0	2	2	2	2	2	3	3	3	2	1
70			0	0	0	1	1	0	0	0	2	1	0	0	0	1	1	3	3	3	3	2
71			3	3	3	2	1	0	0	0	0,667	0,5	1	1	1	1	1	14				
72								3										0,21				

Рисунок Л.2 – Результати розрахунків для 2-го сектору карти ризиків

	A	B	C	D	E	F	G	I	J	K	L	M	O	P	Q	R	S	U	V	W	X	Y
1	3																					
2			H	M	T	C	S	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC
9	07	Пролив рідини	1	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	3	2	3	3
14	12	Порушення правил та процедур роботи з інформацією	1	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	3	2	3	3
25	23	Механічна несправність жорсткого диска	0	0	1	0	0	0	0	2	0	0	1	1	1	1	1	1	3	2	3	3
69			2	0	1	0	0	0	0	0	0	0	3	3	3	3	3	1	3	2	3	3
70			1	0	1	0	0	1	0	1	0	0	1	0	1	0	0	2	3	3	3	3
71			1	3	2	3	3	0,5	0	0,33	0	0	1	1	1	1	1	14				
72								2										0,14				

Рисунок Л.3 – Результати розрахунків для 3-го сектору карти ризиків

	A	B	C	D	E	F	G	I	J	K	L	M	O	P	Q	R	S	U	V	W	X	Y
1	5																					
2			H	M	T	C	S	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC
59	57	Помилки в реєстрах Windows	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	2	2	2	2	1
61	59	Неточне видалення або встановлення програмного забезпечення	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	2	2	2	2	1
69			0	0	0	0	2	0	0	0	0	1	2	2	2	2	2	2	2	2	2	1
70			0	0	0	0	1	0	0	0	0	2	0	0	0	0	1	2	2	2	2	2
71			2	2	2	2	1	0	0	0	0	1	1	1	1	1	1	10				
72								2										0,20				

Рисунок Л.4 – Результати розрахунків для 5-го сектору карти ризиків

	A	B	C	D	E	F	G	I	J	K	L	M	O	P	Q	R	S	U	V	W	X	Y
1	6																					
2			H	M	T	C	S	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC
11	09	Ненавмисна помилка	1	0	0	0	0	3	0	0	0	0	1	1	1	1	1	3	4	1	5	2
19	17	Навмисна активація електронною поштою вірусу користувачем	0	1	0	0	0	0	4	0	0	0	1	1	1	1	1	3	4	1	5	2
20	18	Ненавмисна активація вірусного повідомлення користувачем	0	1	0	0	0	0	4	0	0	0	1	1	1	1	1	3	4	1	5	2
27	25	Пошкодження комп'ютера через скупчення пилу в комп'ютері	0	0	1	0	0	0	0	1	0	0	1	1	1	1	1	3	4	1	5	2
35	33	Ненавмисне вимкнення комп'ютера без збереження інформації	0	0	1	0	0	0	0	1	0	0	1	1	1	1	1	3	4	1	5	2
65	63	Помилки вводу-виводу даних	0	0	0	0	1	0	0	0	0	2	1	1	1	1	1	3	4	1	5	2
66	64	Помилки обробки даних	0	0	0	0	1	0	0	0	0	2	1	1	1	1	1	3	4	1	5	2
69			1	2	2	0	2	0	1	0	0	0	7	7	7	7	7	3	4	1	5	2
70			1	1	1	0	1	1	2	1	0	1	1	1	1	0	1	4	5	2	5	3
71			3	4	1	5	2	0,25	0,4	0,5	0	0,33	1	1	1	1	1	19				
72								5										0,26				

Рисунок Л.5 – Результати розрахунків для 6-го сектору карти ризиків

	A	B	C	D	E	F	G	I	J	K	L	M	O	P	Q	R	S	U	V	W	X	Y
1	4																					
2			H	M	T	C	S	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC
3	01	Навмисне видалення файлів даних або розділів тексту	1	0	0	0	0	2	0	0	0	0	1	1	1	1	1	2	4	5	1	3
12	10	Використання інших імен користувачів та паролів	1	0	0	0	0	2	0	0	0	0	1	1	1	1	1	2	4	5	1	3
21	19	Навмисне відключення антивірусного програмного забезпечення	0	1	0	0	0	0	4	0	0	0	1	1	1	1	1	2	4	5	1	3
22	20	Ненавмисне відключення антивірусного програмного забезпечення	0	1	0	0	0	0	4	0	0	0	1	1	1	1	1	2	4	5	1	3
33	31	Незаплановане відключення електроенергії	0	0	1	0	0	0	0	5	0	0	1	1	1	1	1	2	4	5	1	3
37	35	Вхід за допомогою чужого логіна	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	2	4	5	1	3
40	38	Копіювання інформації на знімний носій	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	2	4	5	1	3
43	41	Заміна інформації	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	2	4	5	1	3
44	42	Несанкціоноване використання прав адміністратора	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	2	4	5	1	3
53	51	IP-спуфінг	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	2	4	5	1	3
54	52	Втрата інформації через шифрування / дешифрування	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	2	4	5	1	3
57	55	Відсутність оновлень програмного забезпечення	0	0	0	0	1	0	0	0	0	3	1	1	1	1	1	2	4	5	1	3
58	56	Переформатування під час оновлення системи	0	0	0	0	1	0	0	0	0	3	1	1	1	1	1	2	4	5	1	3
60	58	Програма не відповідає	0	0	0	0	1	0	0	0	0	3	1	1	1	1	1	2	4	5	1	3
67	65	Помилки сумісності	0	0	0	0	1	0	0	0	0	3	1	1	1	1	1	2	4	5	1	3
68	66	Помилки сполучення	0	0	0	0	1	0	0	0	0	3	1	1	1	1	1	2	4	5	1	3
69			2	2	1	5	5	0	0	0	0	0	16	16	16	16	16	2	4	5	1	3
70			1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	5	6	2	4
71			2	4	5	1	3	0,33	0,2	0,17	0,5	0,25	1	1	1	1	1	20				
72								5										0,25				

Рисунок Л.6 – Результати розрахунків для 4-го сектору карти ризиків

	A	B	C	D	E	F	G	I	J	K	L	M	O	P	Q	R	S	U	V	W	X	Y
1	8																					
2			H	M	T	C	S	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC
4	02	Ненавмисне видалення файлів даних або розділів тексту	1	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	2	2	2	2
6	04	Ненавмисне не зберігання інформації	1	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	2	2	2	2
13	11	Крадіжка інформації працівниками	1	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	2	2	2	2
69			3	0	0	0	0	1	0	0	0	0	3	3	3	3	3	1	2	2	2	2
70			1	0	0	0	0	2	0	0	0	0	1	0	0	0	0	2	2	2	2	2
71			1	2	2	2	2	1	0	0	0	0	1	1	1	1	1	10				
72								2										0,20				

Рисунок Л.7 – Результати розрахунків для 8-го сектору карти ризиків

	A	B	C	D	E	F	G	I	J	K	L	M	O	P	Q	R	S	U	V	W	X	Y
1	7																					
2			H	M	T	C	S	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC
5	03	Навмисне не зберігання інформації	1	0	0	0	0	2	0	0	0	0	1	1	1	1	1	2	4	2	1	4
10	08	Навмисна помилка	1	0	0	0	0	2	0	0	0	0	1	1	1	1	1	2	4	2	1	4
31	29	Вогонь	0	0	1	0	0	0	0	2	0	0	1	1	1	1	1	2	4	2	1	4
34	32	Навмисне вимкнення комп'ютера без збереження інформації	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	2	4	2	1	4
41	39	Надсилання інформації на зовнішню електронну адресу	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	2	4	2	1	4
42	40	Крадіжка інформації	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	2	4	2	1	4
52	50	Фіктивний DNS-сервер	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	2	4	2	1	4
55	53	Злом ключів шифрування	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	2	4	2	1	4
69			2	0	1	4	0	0	0	0	0	0	8	8	8	8	8	2	4	2	1	4
70			1	0	1	1	0	1	0	1	1	0	1	0	1	1	0	3	4	3	2	4
71			2	4	2	1	4	0,33	0	0,33	0,5	0	1	1	1	1	1	16				
72								3										0,19				

Рисунок Л.8 – Результати розрахунків для 7-го сектору карти ризиків

	A	B	C	D	E	F	G	I	J	K	L	M	O	P	Q	R	S	U	V	W	X	Y
1	9																					
2			HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC	HE	MW	TR	CR	SC
17	15	Втрата інформації через вірус	0	1	0	0	0	0	1	0	0	0	1	1	1	1	1	3	1	3	3	2
18	16	Псування вірусом	0	1	0	0	0	0	1	0	0	0	1	1	1	1	1	3	1	3	3	2
63	61	Помилки обчислення	0	0	0	0	1	0	0	0	0	2	1	1	1	1	1	3	1	3	3	2
64	62	Логічні помилки	0	0	0	0	1	0	0	0	0	2	1	1	1	1	1	3	1	3	3	2
69			0	2	0	0	2	0	0	0	0	1	4	4	4	4	4	3	1	3	3	2
70			0	1	0	0	1	0	1	0	0	2	0	1	0	0	1	3	2	3	3	3
71			3	1	3	3	2	0	0,5	0	0	0,667	1	1	1	1	1	14				
72								3										0,21				

Рисунок Л.9 – Результати розрахунків для 9-го сектору карти ризиків

Додаток М

Результати симуляцій побудованих моделей бізнес-процесів інформаційної безпеки банку

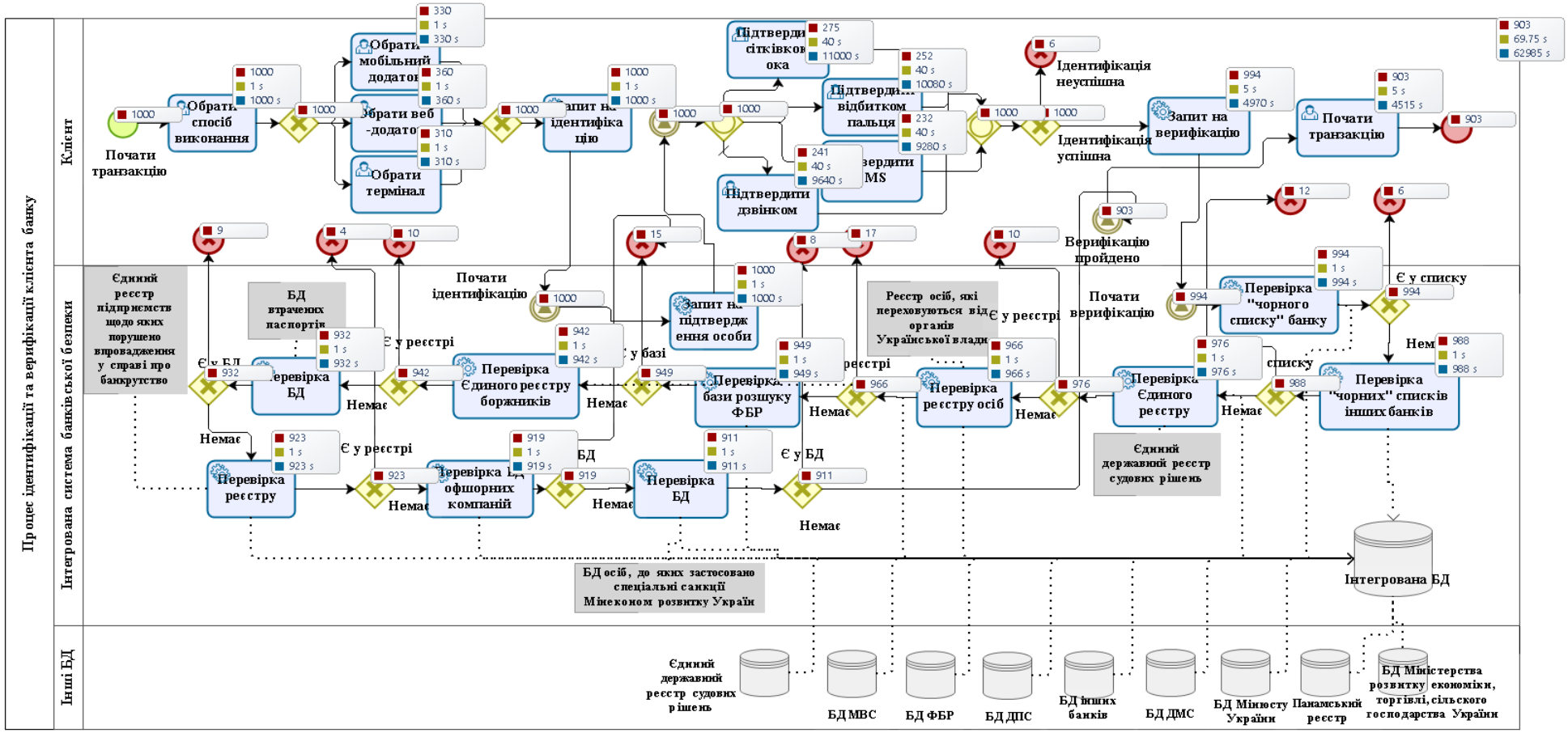


Рисунок М.1 – Результати симуляції за часом для бізнес-моделі процесу ідентифікації та верифікації клієнта (складено авторкою)

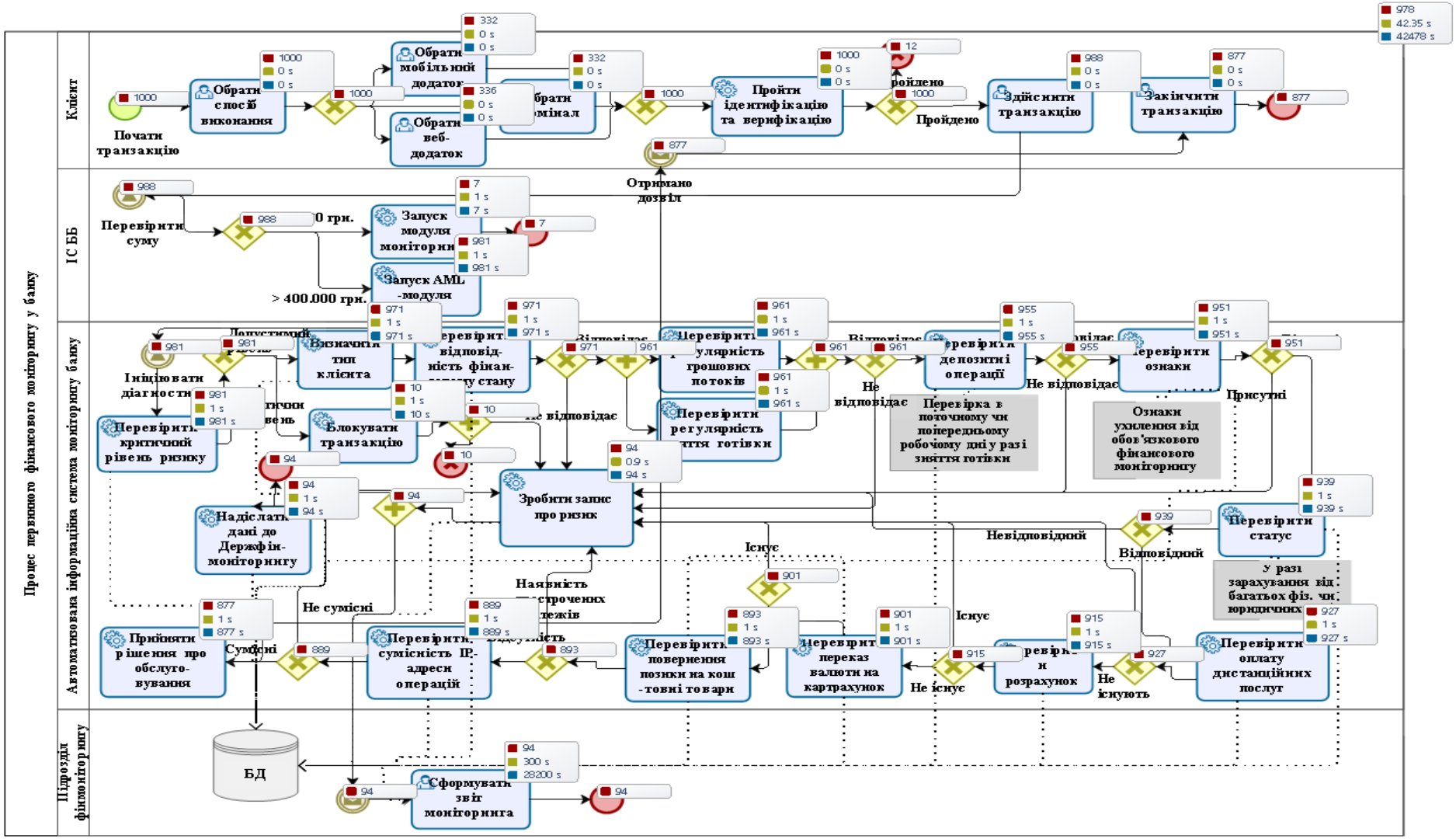


Рисунок М.2 – Результати симуляції за часом для бізнес-моделі процесу автоматизованого фінансового моніторингу (складено авторкою)

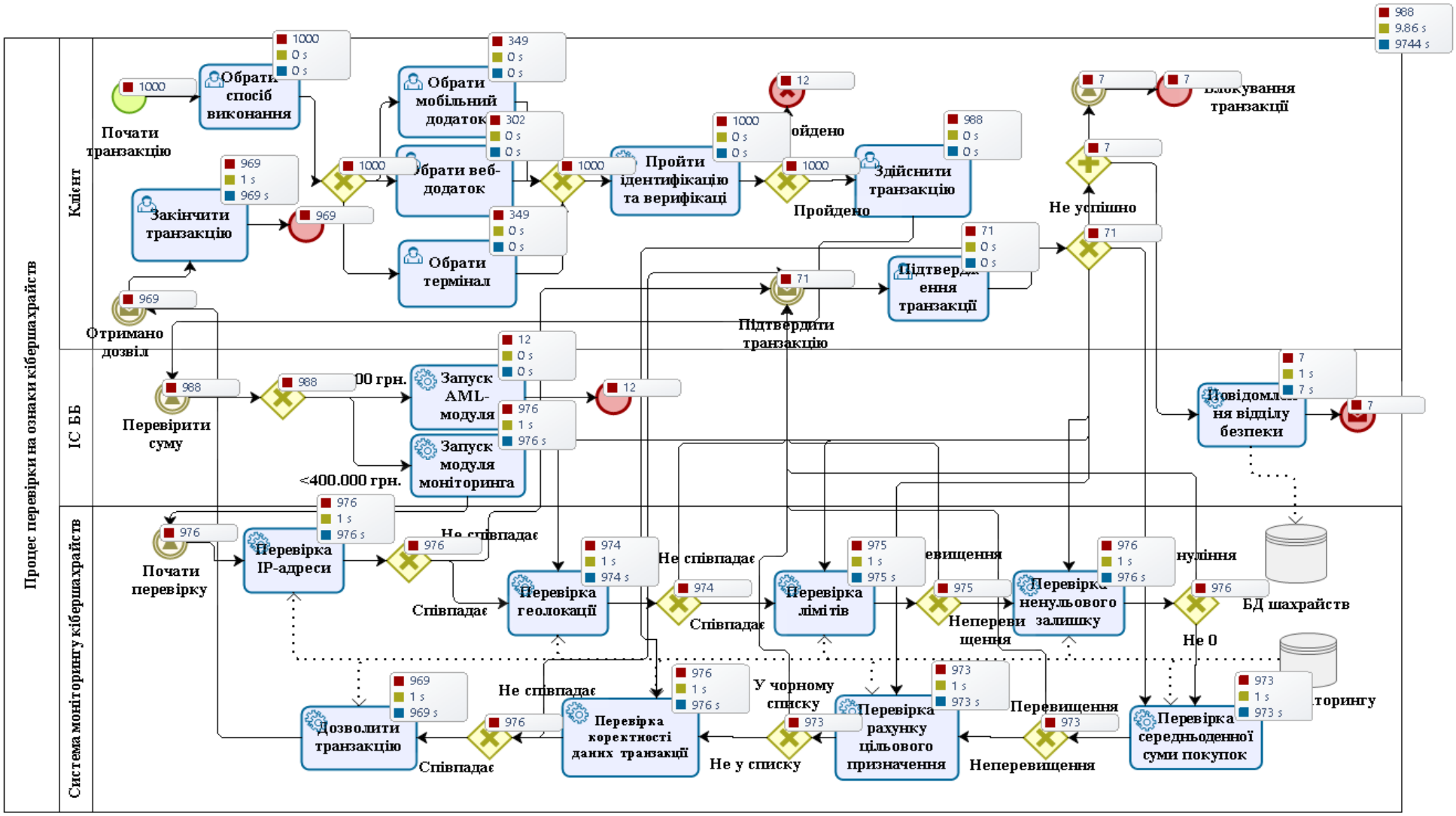


Рисунок М.3 – Симуляція бізнес-моделі процесу перевірки транзакцій на ознаки зовнішніх кібершахрайств (складено авторкою)

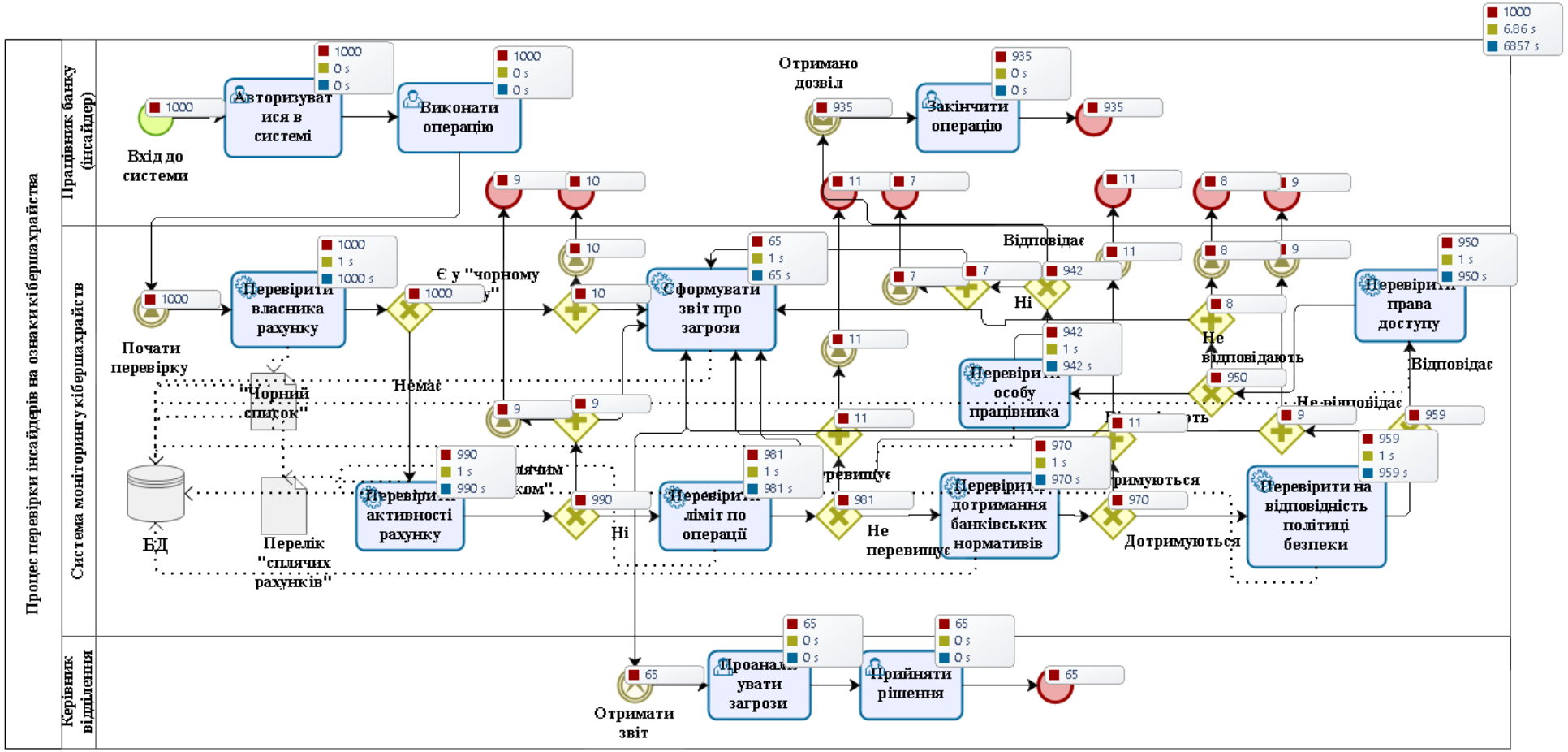


Рисунок М.4 – Симуляція бізнес-моделі процесу перевірки транзакцій на ознаки кібершахрайств з боку інсайдерів (складено авторкою)

Додаток Н

HLB UKRAINE
ADVISORY, TAX AND AUDIT

Вих. №375-03/21
від 04.03.2021 р.

До Спеціалізованої вченої ради
Д 55.051.06
Сумського державного університету

ДОВІДКА
про впровадження результатів дисертаційної роботи
Яровенко Ганни Миколаївни
на тему «Інформаційна безпека як драйвер розвитку національної економіки»

Результати досліджень автора, а саме пропозиції щодо створення чотириполюсної барицентричної моделі сталого розвитку держави, яка інтегрує композитні таргети вимірів інформаційної безпеки, економіки, соціальної та політичної сфер, розглянуті та взяті до уваги міжнародною аудиторською компанією ТОВ «ЕЙЧ ЕЛ БІ ЮКРЕЙН» (код за ЄДРПОУ – 23731031).

Запропонований автором науково-методичний підхід дозволяє виявляти сфери діяльності, які є найбільш незбалансованими в країні, що сприяє посиленню та удосконаленню відповідних ним заходів реформування. Також модель надає можливість оцінити поточний рівень розвитку країни як центр мас, де відбувається забезпечення рівноваги економічної, соціальної, політичної сфер та сфери інформаційної безпеки, що дозволяє визначити його відхилення від пріоритетного вектора та рівень розбалансованості пар соціально-політичного та економіко-інформаційного вимірів.

Положення щодо створення чотириполюсної барицентричної моделі сталого розвитку держави на основі інтеграції композитних таргетів економічного, політичного, соціального виміру та виміру інформаційної безпеки були враховані міжнародною аудиторською компанією ТОВ «ЕЙЧ ЕЛ БІ ЮКРЕЙН» при проведенні аналітичних досліджень щодо розробки концепції сталого розвитку країни.

Валерій Бондар

Професор, д.е.н.
Генеральний директор
ТОВ «ЕЙЧ ЕЛ БІ ЮКРЕЙН»

Контактні номери:
+38 067 466 17 77
+38 067 465 59 96
+38 044 291 30 10

www.hlb.com.ua
01011, Україна, м. Київ, вул. Гусовського, 11/11, оф. 3
T: +38 044 291 30 10 +38 044 291 30 12
M: +38 067 465 59 96 +38 067 466 17 77 **E:** office@hlb.com.ua

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
«ЄВРОПЕЙСЬКИЙ КОНСАЛТИНГОВИЙ СЕРВІС»
01042, місто Київ, вулиця Чигоріна, будинок 49, офіс 9

Вих. № 110-12/19
від 04.12.2019 р.

До спеціалізованої вченої ради
Д 55.051.06
Сумського державного університету

ДОВІДКА
про впровадження результатів дисертаційної роботи
к.е.н., доцента, доцента кафедри економічної кібернетики
Сумського державного університету
Яровенко Ганни Миколаївни
на тему «Інформаційна безпека як драйвер розвитку національної економіки»

Даною довідкою підтверджується, що в практичній діяльності ТОВ «Європейський Консалтинговий Сервіс» враховуються наукові рекомендації, викладені у дисертаційному дослідженні Яровенко Ганни Миколаївни на тему «Інформаційна безпека як драйвер розвитку національної економіки», поданому у спеціалізовану вчену раду Д 55.051.06 Сумського державного університету на здобуття наукового ступеня доктора економічних наук за спеціальністю 08.00.03 – економіка та управління національним господарством.

Методичні рекомендації до оцінювання ризиків, які асоціюються із втратою інформації та знань, ґрунтуються на використанні карти ризиків, модифікованої шляхом формалізації двійкових оцінок факторів ризику та інцидентів, як елементів теорії множин. Розроблені положення до оцінювання даного виду ризику були використані ТОВ «Європейський Консалтинговий Сервіс» в процесі підвищення ефективності організації інформаційної безпеки компанії. Застосування даної методики у практичній діяльності дозволяє швидко інтерпретувати рівень ризику в компанії, виявити слабкі місця в системі інформаційної безпеки та передбачити майбутні збитки.

Директор Сафонов Д.Г.

Товариство з обмеженою відповідальністю "ЄВРОПЕЙСЬКИЙ КОНСАЛТИНГОВИЙ СЕРВІС" Україна м. Київ Ідентифікаційний код 40955576

ПРАВЕКС БАНК

Акціонерне товариство
«ПРАВЕКС БАНК»

ВІДДІЛЕННЯ «СУМСЬКА ОБЛАСНА ДИРЕКЦІЯ»
вул. Горького, 5А, м. Суми, 40004, Україна
тел. 0 800 500 450, факс +38 044 201 17 80
e-mail: bank@pravex.ua, www.pravex.com.ua
S.W.I.F.T.: PRAVUAUK, REUTERS/BLOOMBERG: PRVX
к/р: 32006102801026 в НБУ, МФО 300001
код ЄДРПОУ 14360920

09.10.2019 № 534-10/19

На № _____

До спеціалізованої вченої ради

Д55.051.06

Сумського державного університету

ДОВІДКА

про впровадження результатів дисертаційної роботи

Яровенко Ганни Миколаївни

на тему «Інформаційна безпека як драйвер розвитку національної економіки»

Результати дисертаційної роботи Яровенко Г.М. «Інформаційна безпека як драйвер розвитку національної економіки» свідчать, що сьогодні основною проблемою для банків є забезпечення належного рівня інформаційної безпеки у зв'язку із зростанням кількості інформаційних та кібернетичних загроз, які мають негативні наслідки для клієнтів та установи в цілому.

Запропоновані рекомендації щодо здійснення оптимізації таких процесів, як ідентифікація та верифікації клієнта в інтегрованій системі банківської безпеки, перевірка транзакцій та інсайдерів на наявність ознак кібершахрайств, автоматизований фінансовий моніторинг банку, реалізовані із використанням нотації моделювання BPMN 2.0 та виконанням симуляції, виходячи із витрат часу та ресурсів на забезпечення даних процесів.

Запропоновані науково-методичні положення Яровенко Г.М. були використані фахівцями Відділення Сумської ОД АТ «ПРАВЕКС БАНК» під час підготовки внутрішніх нормативно-правових документів, які забезпечують організацію заходів інформаційної безпеки у банківській установі. Застосування даних рекомендацій у практичній діяльності дозволить банку виявляти слабкі місця у бізнес-процесах інформаційної безпеки та усувати їх шляхом проведення оптимізації.

Директор
Відділення Сумської ОД
АТ «ПРАВЕКС БАНК» Безносик Є.А.

№ 05/20 від 28.09.2020 р.

До спеціалізованої вченої ради
Д 55.051.06
Сумського державного університету

ДОВІДКА
про впровадження результатів дисертаційної роботи
к.е.н., доцента, доцента кафедри економічної кібернетики
Сумського державного університету
Яровенко Ганни Миколаївни
на тему «Інформаційна безпека як драйвер розвитку національної економіки»

Даною довідкою підтверджується, що в практичній діяльності Громадської організації «Освітньо-правозахисний координаційний центр» враховуються методичні рекомендації, викладені у дисертаційному дослідженні Яровенко Г.М. на тему «Інформаційна безпека як драйвер розвитку національної економіки», поданому у спеціалізовану вчену раду Д 55.051.06 Сумського державного університету на здобуття наукового ступеня доктора економічних наук за спеціальністю 08.00.03 – економіка та управління національним господарством.

Результати дослідження пройшли апробацію шляхом організації і проведення серії вебінарів та круглих столів із залученням населення м. Суми та Сумської області, присвячених питанням організації персональної інформаційної безпеки та уникнення ситуацій, пов'язаних із кібершахрайствами та застосуванням методів соціальної інженерії. Зокрема, положення дисертації щодо методів індивідуального кіберзахисту, визначених на основі аналізу практик та досвіду населення Європейського Союзу, як найбільш ефективних та дієвих, використані при розробці інструктивного матеріалу для населення щодо підвищення рівня його персонального захисту.

Керівник
Громадської організації
«Освітньо-правозахисний
координаційний центр» В.В.Винниченко

Громадська організація «ОСВІТНЬО-ПРАВОЗАХИСНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР» № 40871422 Україна м.Суми

Державний ощадний банк України
Акціонерне товариство
ТВБВ№10018/0172
Філії — Сумського обласного управління
Україна, 40000
м. Суми, вул. Зеленко, 4
Тел.: +380(542)635289

ОЩАДБАНК
МІЙ БАНК. МОЯ КРАЇНА

№ 17/20 від 07.09.2020 р.

До спеціалізованої вченої ради
Д 55.051.06
Сумського державного університету

ДОВІДКА
про впровадження результатів дисертаційної роботи
к.е.н., доцента, доцента кафедри економічної кібернетики
Сумського державного університету
Яровенко Ганни Миколаївни
на тему «Інформаційна безпека як драйвер розвитку національної економіки»

Результати дисертаційної роботи Яровенко Г.М. на тему «Інформаційна безпека як драйвер розвитку національної економіки», подану на здобуття наукового ступеня доктора економічних наук за спеціальністю 08.00.03 – економіка та управління національним господарством, мають теоретичну та практичну цінність для банківської діяльності.

Висновки щодо впливу рівня інформаційної безпеки на ризик здійснення операцій, пов'язаних із відмиванням коштів, отриманих незаконним шляхом, підтверджені в роботі Яровенко Г.М. за допомогою проведеного гравітаційного моделювання оцінки рівня привабливості країн для легалізації кримінальних доходів, прийняті до уваги в роботі ТВБВ№10018/0172 Філії – Сумського обласного управління АТ «Ощадбанк» та використані для коректування положень внутрішньобанківського фінансового моніторингу. Також побудована Яровенко Г.М. нейромережева модель для виявлення ознак кібершахрайств в операціях із банківськими картками застосовується в практичній діяльності філії в якості одного з упереджуючих заходів щодо протидії різним формам соціальної інженерії та для забезпечення захисту інтересів споживачів банківських послуг.

* 000000

Керуючий
ТВБВ№10018/0172 Філії –
Сумського обласного управління
АТ «Ощадбанк» Т.В. Доценко

oschadbank.ua
0800 210 800
в межах України дзвінки безкоштовні

Ліцензія НБУ № 148 від 05.10.2011 р.

1 місце ОЩАДБАНК
Ощадбанк №1 серед провідних банків України

#ощадбанкдіє

ЗАТВЕРДЖУЮ
Перший проректор
Сумського державного
університету
_____ В. Д. Карпуша
“___”_____2020 р.

АКТ

Про впровадження результатів дисертаційної роботи
Яровенко Ганни Миколаївни
«Інформаційна безпека як драйвер розвитку національної економіки»
у навчальний процес Навчально-наукового інституту бізнес-технологій
«УАБС» Сумського державного університету

“02” листопада 2020 р. м. Суми

Акт складено комісією у складі:
голова: директор ННІ БТ «УАБС» доктор економічних наук, професор Д’яконова І.І.
члени комісії:
– завідувач кафедри економічної кібернетики, доктор економічних наук, професор Кузьменко О.В.
– заступник директора ННІ БТ «УАБС» з методичної роботи, кандидат економічних наук Мірошниченко О.В.
– начальник навчально-методичного відділу, кандидат економічних наук, доцент Криклій О.А.

В період з 26 жовтня по 02 листопада 2020 р. комісія виконала роботи з визначення фактичного впровадження результатів дисертаційного дослідження Яровенко Ганни Миколаївни «Інформаційна безпека як драйвер розвитку національної економіки» у навчальний процес ННІ БТ «УАБС» СумДУ.
Комісія розглянула такі матеріали:
1. Дисертаційну роботу Яровенко Г.М. «Інформаційна безпека як драйвер розвитку національної економіки» та робочі програми дисциплін:
- «Ефективність інформаційних систем» (викладається для студентів освітнього ступеня магістр за спеціальністю 051 «Економіка», освітня програма «Економічна кібернетика»);
- «Моделювання емерджентної економіки» (викладається для студентів освітнього ступеня магістр за спеціальністю 051 «Економіка», освітня програма «Економічна кібернетика»);

- «Прогнозування соціально-економічних процесів» (викладається для студентів освітнього ступеня бакалавр за спеціальністю 051 «Економіка», освітня програма «Економічна кібернетика»).

2. Видані навчально-методичні матеріали для вивчення вказаних дисциплін.

За результатами проведеної роботи комісією встановлено:

1. Розроблені у дисертаційній роботі Яровенко Г.М. «Інформаційна безпека як драйвер розвитку національної економіки» науково-методичні положення, а також практичні рекомендації впроваджені в навчальний процес з наступних дисциплін:

– «*Ефективність інформаційних систем*». Розділи: «Методологія оцінки ефективності інформаційних систем», «Концепція сукупної вартості володіння», «Оцінка ефективності роботи IT-служби підприємства»;

– «*Моделювання емерджентної економіки*». Розділи: «Концептуальні засади математичного моделювання економіки», «Прикладні математичні моделі фінансово- економічних процесів», «Моделі аналізу макроекономічної політики»;

– «*Прогнозування соціально-економічних процесів*». Розділи: «Нейронні мережі в прогнозуванні соціально-економічних процесів», «Макроекономічні моделі прогнозування».

2. Методичні підходи, розроблені у дисертаційній роботі Яровенко Г.М. «Інформаційна безпека як драйвер розвитку національної економіки», покладено в основу ряду лабораторних занять з наступних дисциплін: «*Ефективність інформаційних систем*», «*Моделювання емерджентної економіки*», «*Прогнозування соціально-економічних процесів*».

3. Застосування результатів дисертаційної роботи Яровенко Ганни Миколаївни «Інформаційна безпека як драйвер розвитку національної економіки» в навчальному процесі Навчально-наукового інституту бізнес-технологій «УАБС» Сумського державного університету дало змогу адаптувати зазначені дисципліни до умов сучасних трансформаційних процесів в освіті, поглибити їх теоретико-методологічний базис, підвищити якість підготовки фахівців з економічних спеціальностей у відповідності із вимогами практичної діяльності та роботодавців.

Голова комісії: І.І. Д’яконова

Члени комісії: О.В. Кузьменко

О.В. Мірошниченко

О.А. Криклій

Додаток П

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ

Монографії:

1. Яровенко Г. М., Бояджян М. М. Оцінка впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері. *Сучасні інструменти боротьби з кібершахрайствами у банках* / за заг. ред. О. В. Кузьменко, Г. М. Яровенко. Суми : Видавництво «Ярославна», 2018. С. 47–61 (0,50 друк. арк.). *Особистий внесок: розроблено методику оцінювання впливу макроекономічних факторів на схильність до фінансових кібершахрайств (0,40 друк. арк.).*

2. Інформаційна система фінансового моніторингу: особливості розробки та реалізації в сучасних умовах протидії легалізації кримінальних доходів / О. В. Кузьменко, Г. М. Яровенко, А. О. Бойко, С. В. Миненко; за заг. ред. О. В. Кузьменко. Суми : Видавництво «Ярославна», 2019. 145 с. (9,9 друк. арк.).

3. Яровенко Г. М. Моделювання та автоматизація обліку, контролю, аудиту. Суми : Видавництво ПП Вінниченко М. Д., ФОП Литовченко Є. Б., 2016. 156 с. (9,07 друк. арк.).

Публікації в наукових фахових виданнях України:

4. Яровенко Г. М. Наслідки інформаційних війн як фактор економічної дестабілізації країни. *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки»* (Index Copernicus та ін.). 2020. № 9 (1). С. 94–103 (0,85 друк. арк.).

5. Yarovenko H., Kuzmenko O., Stumpo M. Strategy for Determining Country Ranking by Level of Cybersecurity. *Financial Markets, Institutions and Risks* (Index Copernicus та ін.). 2020. № 4 (3). P. 124–137 (1,17 друк. арк.). *Особистий внесок: розроблений підхід до реформування системи ІБ України (1,05 друк. арк.).*

6. Yarovenko H., Kuzmenko O., Stumpo M. DEA-Analysis Of The Effectiveness Of The Country's Information Security System. *SocioEconomic Challenges* (Index Copernicus та ін.). 2020. № 4 (3). P. 142–153 (1,04 друк. арк.). *Особистий внесок: проведено оцінювання ресурсного потенціалу ІБ країн (0,94 друк. арк.).*

7. Yarovenko H. Evaluating the threat to national information security. *Problems and Perspectives in Management* (Scopus та ін.). 2020. Vol. 18, Issue 3. P. 195–210 (1,23 друк. арк.).

8. Яровенко Г. М. Бібліометричний аналіз досліджень інформаційної безпеки в розрізі розвитку національної економіки. *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки»* (Index Copernicus та ін.). 2020. № 8 (40). С. 53–63 (0,90 друк. арк.).

9. Яровенко Г. М. Використання карт Кохонена для аналізу рівня інформаційної безпеки країн з урахуванням їх розвитку. *Економічний простір* (Index Copernicus та ін.). 2020. № 157. С. 118–124 (0,73 друк. арк.).

10. 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 (Index Copernicus та ін.). 2020. № 31. С. 160–167 (0,83 друк. арк.).

11. Яровенко Г. М. Вплив рівня економічного розвитку країни на залежність використання персональних засобів інформаційної безпеки та наслідків кіберзлочинів. *Вісник Сумського державного університету. Серія «Економіка»* (Scientific Indexing Services та ін.). 2020. № 1. С. 188–198 (0,87 друк. арк.).

12. Яровенко Г. М., Доценко Т. В., Кушнерьов О. С. Формування інтегрального індексу загрози національної економіки. *Вісник Сумського державного університету. Серія «Економіка»* (Scientific Indexing Services та ін.). 2020. № 2. С. 16–28 (0,93 друк. арк.). *Особистий внесок: обґрунтовано механізм врахування ІБ під час оцінювання загроз НЕ (0,05 друк. арк.).*

13. Яровенко Г. М., Колотіліна О. В. Оцінка ризиків соціо-економіко-політичного розвитку України. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Економіка і управління* (Index Copernicus та ін.). 2020. Т. 31 (70), № 4. С. 151–159 (0,71 друк. арк.). *Особистий внесок: досліджено ризик зменшення ІБ в системі макроекономічних ризиків (0,35 друк. арк.).*

14. Яровенко Г. М., Ковач В. О. Перспективи застосування технології блокчейн в системах забезпечення кібербезпеки банків. *Підприємництво та інновації* (Index Copernicus та ін.). 2020. № 12. С. 206–214 (0,90 друк. арк.). *Особистий внесок: проведено порівняльний аналіз перспектив використання технології блокчейн та штучного інтелекту в системах кіберзахисту (0,45 друк. арк.).*

15. Кузьменко О. В., Бойко А. О., Яровенко Г. М., Доценко Т. В. Сценарії реформування національної системи фінансового моніторингу. *Економіка та держава* (Index Copernicus та ін.). 2020. № 1. С. 9–15 (0,74 друк. арк.). *Особистий внесок: досліджено місце системи забезпечення кібербезпеки в національній системі фінансового моніторингу (0,07 друк. арк.).*

16. Кузьменко О. В., Яровенко Г. М., Бойко А. О., Миненко С. В. Розробка інтерфейсів автоматизованого модуля фінансового моніторингу. *Інвестиції: практика та досвід* (Index Copernicus та ін.). 2020. № 1. С. 11–18 (0,73 друк. арк.). *Особистий внесок: розроблено пропозиції щодо підсилення кіберзахисту в процесі автоматизації фінансового моніторингу (0,65 друк. арк.).*

17. Яровенко Г. М. Тенденції розвитку національної економіки в умовах її цифровізації. *Причорноморські економічні студії* (Index Copernicus та ін.). 2019. № 39, ч. 1. С. 159–164 (0,63 друк. арк.).

18. Lyeonov S., Kuzmenko O., Yarovenko H., Dotsenko T. The Innovative Approach to Increasing Cybersecurity of Transactions Through Counteraction to Money Laundering. *Marketing and Management of Innovations* (Web of Science та ін.). 2019. № 3. P. 308–326 (1,65 друк. арк.). *Особистий внесок: побудовано гравітаційну модель для врахування рівня кібербезпеки країни під час оцінювання її привабливості для відмивання кримінальних доходів (1,25 друк. арк.).*

19. Яровенко Г. М. Аналіз макропоказників, що характеризують рівень складових інформаційної безпеки. *Вісник Хмельницького національного університету*. *Економічні науки* (Index Copernicus). 2019. № 4, т. 3. С. 47–54 (0,79 друк. арк.).

20. Кузьменко О. В., Яровенко Г. М., Левченко В. П., Миненко С. В. Автоматизація процесу фінансового моніторингу легалізації коштів, отриманих незаконним шляхом. *Наукові записки Національного університету «Острозька академія» серія «Економіка»* (Index Copernicus та ін.). 2019. № 43. С. 162–171 (0,97 друк. арк.). *Особистий внесок: розроблено автоматизовану систему кіберзахисту для боротьби з легалізацією коштів (0,25 друк. арк.).*

21. Яровенко Г. М. Аналіз видів загроз та їх наслідків щодо забезпечення інформаційної безпеки держави. *Вісник Хмельницького національного університету*. *Економічні науки* (Index Copernicus). 2018. № 6, т. 3. С. 103–109 (0,87 друк. арк.).

22. Яровенко Г. М. Системний підхід до формалізації поняття «Інформаційна безпека». *Причорноморські економічні студії* (Index Copernicus та ін.). 2018. № 34. С. 239–244 (0,80 друк. арк.).

23. Яровенко Г. М. Розробка інформаційної моделі виявлення ознак шахрайств у банках. *Інвестиції: практика та досвід* (Index Copernicus та ін.). 2018. № 14. С. 23–28 (0,57 друк. арк.).

24. Яровенко Г. М., Сковронська А. І., Бояджян М. М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу. *Ефективна економіка* (WorldCat та ін.). 2018. № 7. URL: http://www.economy. nayka.com.ua/pdf/7_2018/39.pdf (0,61 друк. арк.). *Особистий внесок: розроблено нейромережеву модель виявлення ознак кіберзагроз (0,49 друк. арк.).*

25. Яровенко Г. М., Бояджян М. М. Аналіз наслідків кібершахрайств в банківській системі України. *Економіка та суспільство* (Google Scholar та ін.). 2018. № 18. С. 836–843. URL: http://economyandsociety.in.ua/journals/18_ukr/116.pdf (0,54 друк. арк.). *Особистий внесок: проаналізовано макроекономічні наслідки фінансових кібершахрайств (0,43 друк. арк.)*.

26. 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* (Web of Science та ін.). 2018. № 4. P. 221–233 (1,27 друк. арк.). *Особистий внесок: запропоновано методологію побудови чотириполюсної барицентричної моделі (1,02 друк. арк.).*

27. Яровенко Г. М., Ковач В. О. Моделювання портретів потенційних шахрая та жертви банківських шахрайств. *Ефективна економіка* (Index Copernicus та ін.). 2018. № 10. URL: http://www.economy.nayka.com.ua/pdf/10_2018/63.pdf (0,65 друк. арк.). *Особистий внесок: розроблено портрет потенційного кібершахрая щодо кредитних операцій (0,33 друк. арк.).*

28. Яровенко Г. М., Коркішко А. В. Моделювання ймовірності виникнення шахрайських операцій з кредитними картками. *Проблеми і перспективи розвитку банківської системи України: збірник наукових праць*. 2015. № 41. С. 237–248 (0,49 друк. арк.). *Особистий внесок: досліджено напрями фінансових кібершахрайств та запропоновано інструменти боротьби з ними (0,39 друк. арк.).*

29. Яровенко Г. М. Автоматизація як перспективний напрям розвитку зовнішнього аудиту. *Інвестиції: практика та досвід* (Index Copernicus та ін.). 2012. № 4. С. 34–38 (0,48 друк. арк.).

30. Яровенко Г. М. Моделювання в бухгалтерському обліку як засіб підвищення ефективності його автоматизації. *Інвестиції: практика та досвід* (Index Copernicus та ін.). 2012. № 6. С. 100–104 (0,58 друк. арк.).

31. Яровенко Г. М., Титаренко А. К. Методи дослідження ринку автоматизованих інформаційних систем. *Ефективна економіка*. 2011. № 6. URL: http:// www.economy.nayka.com.ua/index.php?operation=1&iid=590 (0,42 друк. арк.). *Особистий внесок: проведено кластеризацію сегмента ринку інформаційних систем у межах латерального зрушення (0,34 друк. арк.).*

Публікації в інших наукових виданнях:

32. Subeh Musa A., Yarovenko H. Data Mining of Operations with Card Accounts of Bank Clients. *Financial Markets, Institutions and Risks* (Index Copernicus та ін.). 2017. № 1 (4). P. 87–95 (0,58 друк. арк.). *Особистий внесок: розроблено нейромережеву модель виявлення кіберзагроз у транзакціях (0,50 друк. арк.).*

Тези доповідей на наукових конференціях:

33. Yarovenko H. Research of relationship between information security and country development factors. *Theoretical and empirical scientific research: concept and trends* : Collection of scientific papers «ΛΌГОΣ» with Proceedings of the International Scientific and Practical Conference, July 24, 2020. Oxford, UK : Oxford Sciences Ltd. & European Scientific Platform, 2020. Vol. 1. P. 37–38 (0,12 друк. арк.).

34. Sadigov M., Kuzmenko O., Yarovenko H. Blockchain technology based system-dynamic simulation modeling of enterprise's cyber security system. *Economic and Social Development* : Book of Proceedings 55th International Scientific Conference on Economic and Social Development Development, 2020. Vol. 1/4. P. 399–408. URL: https://www.esd-conference.com/upload/book_of_proceedings/ Book_of_Proceedings_esdBaku2020_Vol1_Online.pdf (0,75 друк. арк.). *Особистий внесок: розроблено системно-динамічну модель системи ІБ (0,68 друк. арк.).*

35. Leonov S., Yarovenko H., Boiko A., Dotsenko T. Information system for monitoring banking transactions related to money laundering. *CEUR Workshop Proceedings* (Scopus). 2019. Vol. 2422. P. 297–307. URL: http://ceur-ws.org/Vol-2422/paper24.pdf (0,62 друк. арк.). *Особистий внесок: розроблено прототип інформаційної системи фінансового моніторингу (0,45 друк. арк.).*

36. Яровенко Г. М., Нечепоренко І. Д. Сучасні технології кіберзахисту щодо виявлення шахрайств, які здійснюються персоналом банку. *Проблеми та перспективи розвитку фінансово-кредитної системи України* : зб. матеріалів IV

Всеукр. наук.-практ. on-line-конф., 21–22 листоп. 2019 р. Суми : Сумський державний університет, 2019. Ч. 2. С. 149–153 (0,17 друк. арк.). *Особистий внесок: проаналізовано технологію машинного навчання для попередження кіберзагроз із боку інсайдерів (0,09 друк. арк.).*

37. Яровенко Г. М. Системний підхід до побудови інформаційної моделі виявлення передумов виникнення шахрайств в банках. *Актуальні проблеми моделювання та управління соціально-економічними системами в умовах глобалізації* : матеріали Міжнар. наук.-практ. конф. Дрогобич, 2018. С. 66–69 (0,15 друк. арк.).

38. Яровенко Г. М., Бояджян М. М. Концептуальна модель виявлення ознак кібершахрайств в банках. *Сучасні міжнародні економічні відносини: становлення та шляхи перспективного розвитку* : зб. тез наук. робіт учасн. Всеукр. наук.-практ. конф., 9–10 лют. 2018 р. Одеса : ЦЕДР, 2018. С. 98–100 (0,14 друк. арк.). *Особистий внесок: сформовано гіпотези ознак кібершахрайств (0,07 друк. арк.).*

39. Яровенко Г. М., Бояджян М. М. Оцінка впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері. *Проблеми та перспективи розвитку фінансово-кредитної системи України* : зб. матеріалів ІІІ Всеукр. наук.-практ. on-line-конф., 22–23 листоп. 2018 р. Суми : ННІ БТ «УАБС» СумДУ, 2018. С. 294–297 (0,13 друк. арк.). *Особистий внесок: класифіковано методи кібершахрайств* (0,07 друк. арк.).

40. Яровенко Г. М. Методика визначення витрат на обробку інформації при впровадженні автоматизованої системи управління. *Сучасні шляхи стабілізації економічного стану країни* : матеріали Міжнар. наук.-практ. конф., 1–2 квіт. 2016 р. Дніпро : НО «Перспектива», 2016. Ч. 2. С. 99–101 (0,14 друк. арк.).

41. Яровенко Г. М. Формування інформації для оцінки джерел ефективності використання автоматизованої інформаційної системи підприємства. *Економіка, менеджмент, фінанси: теоретичні та практичні аспекти розвитку* : зб. тез наук. робіт учасн. Міжнар. наук.-практ. конф., 22–23 трав. 2015. Київ : Аналітичний центр «Нова Економіка». 2015. Ч. 2. С. 101–102 (0,14 друк. арк.).

42. Яровенко Г. М. Метод оцінки економічної ефективності автоматизованих інформаційних систем на основі статистики результатів впроваджень. *Формування фінансової системи в умовах глобалізації* : XXIV Міжнар. наук.-практ. конф., 9–10 серп. 2013 р. Київ, 2013. С. 71–74 (0,21 друк. арк.).

43. Яровенко Г. М. Використання математичних методів та моделей у забезпеченні ефективності корпоративних інформаційних систем. *Актуальні проблеми теорії та практики менеджменту* : зб. матеріалів Міжнар. наук.-практ. конф., 16–17 серп. 2013 р. Сімферополь, 2013. С. 92–94 (0,21 друк. арк.).