МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 37.012.4:004.056:330.34
DOI: https://doi.org/10.32782/2224-6282/157-21

Яровенко Г. М.
кандидат економічних наук, доцент,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-8760-6835

Yarovenko Hanna
Sumy State University

ВИКОРИСТАННЯ КАРТ КОХОНЕНА ДЛЯ АНАЛІЗУ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРАЇН З УРАХУВАННЯМ ЇХ РОЗВИТКУ[1]

Розвиток комп'ютерних технологій призводить до появи інформаційних загроз у країні, пов'язаних із виникненням інформаційних війн та кібертероризмом. Саме тому є потреба в аналізі рівня інформаційної безпеки країни з урахуванням її розвитку. Задля цього вибрано дві групи показників, а саме індекси інформаційної безпеки та розвитку. Набір даних сформовано для 159 країн світу за 2018 рік. Для виявлення показників із тісним статистичним зв'язком проведено кореляційний аналіз, за результатами якого відібрано 12 показників розвитку. Для приведення даних у співставні величини проведено нелінійну нормалізацію. За допомогою аналітичної платформи "Deductor Academic" дані перевірено на якість, наявність викидів, дублікатів та протиріч. Відкориговані дані використано для побудови карт Кохонена. В результаті цього отримано 7 кластерів країн: 0-й та 1-й включають країни з найвищими показниками розвитку та безпеки, 2-й – країни з показниками вище середнього, 3-й – із середнім рівнем розвитку та безпеки, 4-й – рівнем нижче середнього, 5-й – низьким рівнем, 6-й – дуже низьким.

Ключові слова: *інформаційна безпека, карти Кохонена, матриця відстаней, матриця помилок квантування, матриця щільності попадання, нелінійна нормалізація, розвиток.*

USE OF KOHONEN MAPS TO ANALYZE THE INFORMATION SECURITY LEVEL OF COUNTRIES TAKING INTO ACCOUNT THEIR DEVELOPMENT

The development of computer technology leads to the emergence of information threats in the country associated with the appearance of information wars and cyber terrorism. There is a need to analyze the level of information security of the country because of this reason. It is also necessary to take into account the level of country development. Two groups of indicators were selected for analysis – information security indexes and development indicators. Global Cybersecurity Index, National Cyber Security Index, ICT Development Index, Networked Readiness Index, Digital Development Level formed a group of information security indicators. Thirty-seven indicators of world development were included in another group. The dataset was generated for 159 world countries in 2018. A correlation analysis was carried out in this work to identify indicators with a close statistical relationship. As a result, 12 development indicators were selected. Non-linear normalization was also performed to bring the data into comparable values. Further research was carried out using an analytical platform Deductor Academic. Data were checked for quality, outliers, duplicates and inconsistencies. As a result, outliers were identified for three observations of the indicator "Life expectancy", after which the data were replaced with probable values. Kohonen maps were constructed, taking into account different combinations of parameters, as a result of which the option with the lowest quantization errors and optimal hit density was chosen. Based on the results of the experiments, it was selected the method for determining the initial weights of neurons "From eigenvectors", the neighborhood function "Stepped", the error level for data recognition is less than 0.05, the size of the map is 24:18. As a result, seven clusters were obtained, which characterize groups of countries by the level of information security, taking into account the indicators of their development. Clusters "0" and "1" include countries with the highest level of development and information security. Group "2" characterizes countries with above-average indicators. The third cluster identifies countries with an average level of development and protection. Group "4" includes countries with indicators for which the degree is below average. The fifth cluster assesses countries with a low level of development and information security, and the sixth cluster characterizes the level of countries as very low.

Keywords: *information security, Kohonen maps, distance matrix, quantization error matrix, hit density matrix, nonlinear normalization, development.*

JEL classification: *C10, C43, O30.*

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

Постановка проблеми. Сьогодні дуже важко уявити різні сфери діяльності суспільства без використання комп'ютерних та інформаційних технологій. Особливо це відчувається в бізнесі, політиці, повсякденному житті людини. Процесу інформатизації та комп'ютеризації також сприяють результати Четвертої промислової революції, яка впливає на підвищення можливостей кіберфізичних систем для вирішення потреб країни, суспільства, суб'єктів господарювання, окремої людини. Однак такий стрімкий розвиток приводить також до того, що новітні технології стають інструментами незаконного збагачення різних злочинців. Це проявляється у збільшенні випадків хакерських атак на бізнес підприємств задля отримання фінансової інформації. Також збільшується кількість кібершахраїв, які застосовують програмно-технологічні можливості для ошукування населення. Це може бути інформаційний вплив на суспільство з використанням соціальних мереж, що призводить до інформаційних війн та політичної дестабілізації у країні.

Названі факти є одними з видів загроз, які призводять до зниження ефективності інформаційної безпеки як окремого суб'єкта, так і країни загалом, тому важливо розуміти, які проблеми в галузі інформаційної безпеки існують, що є фактором їх виникнення, як його наслідки впливатимуть на рівень розвитку країни загалом. Поняття інформаційної безпеки є комплексним, яке охоплює мікро- та макрорівень, а також включає різні її аспекти, зокрема правову, освітню, інституційну, програмно-технологічну безпеку. Досліджуючи рівень інформаційної безпеки країни, маємо також враховувати ці аспекти. Варто зазначити, що фактори економічного, соціального та політичного розвитку країни також можуть впливати на рівень безпеки, оскільки країна з високими соціальними стандартами та рівнем життя вживає найбільш ефективних заходів безпеки. Таким чином, дослідження рівня інформаційної безпеки країн з урахуванням їх розвитку є актуальним та потребує системного вивчення.

Аналіз останніх досліджень і публікацій. Сучасними проблемами інформаційної безпеки займається широке коло закордонних та вітчизняних учених. Загальні питання в цій сфері висвітлювали Е. Косевич [1], В. Кіріленко, Г. Алексєєв [2], А. Сінгх, М. Гупта [3], А. Ключніков, Л. Мура, Д. Скленар [4] та інші науковці.

Низка вчених досліджувала специфічні сфери інформаційної безпеки. Так, М. Садігов, О. Кузьменко, Г. Яровенко вивчали питання застосування блокчейн-технологій у галузі кібербезпеки [5]. М. Дорош, М. Войцеховська, І. Бальченко досліджували підхід до використання методу "Fuzzy Logic" для підвищення ефективності персонального захисту [6]. С. Шмітц та С. Пейп запропонували предметно-орієнтовану структуру для підтримки прийняття рішень з інформаційної безпеки [7]. Також можна виділити роботу С. Євсєєва, В. Алексієва, С. Балакірєва, Ю. Пелешка, О. Милова, О. Петрова, О. Раєвнєвої, Б. Томашевського, І. Тишика, О. Шматька, яка стосується розроблення інформаційної системи захисту [8].

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

Мета статті полягає у проведенні аналізу рівня інформаційної безпеки країни з урахуванням їх розвитку, що відбуватиметься з використанням самоорганізованих карт Кохонена.

Виклад основного матеріалу. Для проведення дослідження вибрано вхідні дані, які характеризують два аспекти, а саме рівень інформаційної безпеки країни та рівень розвитку. Задля цього проведено дослідження офіційних джерел у галузі інформаційної безпеки, в результаті чого виділено п'ять основних показників, які характеризують її окремі сфери. Отже, Global Cybersecurity Index характеризує рівень кібербезпеки для країн-членів Міжнародного союзу електрозв'язку; National Cyber Security Index визначає рівень готовності країни протидіяти кіберзагрозам; ICT Development Index вимірює рівень розвитку інформаційних технологій у країні; Networked Readiness Index визначає ступінь технологічної готовності країни для застосування новітніх інформаційно-комунікаційних технологій у різних сферах; Digital Development Level характеризує рівень цифровізації країни [9]. Оскільки на практиці не існує показника, який би вимірював рівень інформаційної безпеки, то поєднання наведених індексів можна використовувати для оцінювання її окремих напрямів.

Як показники розвитку проаналізовано базу даних Світового банку, серед яких виділено 37 індикаторів, для яких зроблено припущення, що вони мають зв'язок із показниками безпеки. В результаті проведеного кореляційного аналізу виділено 12 показників, для яких рівень їх статистичного зв'язку з показниками безпеки характеризується як тісний, тобто коефіцієнт кореляції перевищує 0,5 або -0,5. Таким чином, відібрано GDP per capita (current US$); Life expectancy; Wage and salaried workers, total (% of total employment); Control of Corruption: Estimate; Government Effectiveness: Estimate; Regulatory Quality: Estimate; Rule of Law: Estimate; GNI per capita, PPP (current international $); Mobile cellular subscriptions (per 100 people); Revenue, excluding grants (% of GDP); Individuals using the Internet (% of population); General government expenditure (% of GDP) [10].

Розрахунки проводилися для 159 країн світу. Як розрахунковий період вибрано 2018 рік. Це було зроблено з огляду на повноту та наявність даних для кожного з вибраних показників.

Для того щоб дані можна було піддавати подальшому аналізу, необхідно провести їх нормалізацію, оскільки кожен з відібраних показників має різні виміри та значення. Задля цього вибрано метод нелінійної нормалізації, оскільки він дає змогу отримати більш ефективні оцінки, ніж лінійна нормалізація, в межах [0, 1]. Таку процедуру проведено за формулою:

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

де Z_{ij} – нормалізоване значення j-го показника в розрізі і-ї країни; $\overline{y_j}$ – середнє значення j-го показника в межах досліджуваного переліку країн; y_{ij} – фактичне значення j-го показника в розрізі і-ї країни; $\sigma(y_j)$ – середнє квадратичне відхилення j-го показника в межах досліджуваного переліку країн.

Після проведення нормалізації вхідних даних необхідно здійснити їх перевірку на якість, виявлення викидів, дублікатів та протиріч. Такий процес проведено за допомогою аналітичної платформи "Deductor Academic". В результаті аналізу якості даних виявлено 3 викиди за індикатором "Life expectancy", що свідчить про необхідність корегування даних за цим показником. Однак загалом отриманий показник якості перебуває в межах (0,7299; 0,9842), що говорить про високу якість початкового набору даних. Перевірка даних на наявність дублікатів та протиріч виявила, що вони відсутні в наборі даних. В результаті проведених перевірок здійснено корегування тільки даних індикатора "Life expectancy", для чого вибрано розрахунок ймовірного значення для спостережень, які є викидами.

Після підготовки даних проведено аналіз рівня інформаційної безпеки країн з урахуванням їх розвитку, що здійснювалося з використанням самоорганізованих карт Кохонена на платформі "Deductor Academic". Карти Кохонена є видом нейронної мережі з некерованим навчанням, яка проєктує дані з багатовимірного простору у двовимірний. Цей інструментарій розроблено фінським ученим Теуво Кохоненом у 1982 році [11].

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

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

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

3) під час налаштування параметрів карти вибрано розміри 24:18, оскільки стандартний розмір 16:12 не дав змогу виявити всі кластери;

4) кількість епох становила 500, а рівень похибки для розпізнавання вибрано менше 0,05;

5) для визначення початкових вагів нейронів вибрано спосіб «З власних векторів», який дає змогу 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 порівняно зі способами «З навчальної множини» та «Випадковими значеннями»;

6) як функція сусідства вибрано «Ступінчату», оскільки результати порівняння матриці похибок квантування та матриці щільності квантування для цієї функції виявилися кращими, ніж для функції «Гауссова»;

7) під час порівняння результатів автоматичного визначення кількості кластерів та ручного визначення, зрештою, вибрано автоматичне визначення з рівнем значущості 0,5%. Кількість кластерів за ручного режиму виставлялося рівним 5, бо саме стільки кластерів було отримано під час ручної перевірки з використанням методу k-means, однак результати автоматичного визначення виявилися кращими.

Після виконання процедур алгоритму побудови карт Кохонена отримано 7 кластерів, а для кожного з відібраних показників побудовано карту. Результати представлено на рис. 1. Також виведено спеціальні карти, які дали змогу зробити порівняння з іншими варіантами карт, побудованих для різних функцій сусідства та методів ініціалізації початкових вагів. Кінцевий результат матриць помилок квантування, щільності попадання та відстаней представлено на рис. 2. В процесі аналізу карт виявлено 16 країн, помилка квантування для яких перевищує 10%, що становить близько 10% від загальної кількості країн. Можна вважати, що це допустимий рівень відхилення для моделей кластеризації.

Так, до 0-го кластеру увійшла 21 країна, а саме Австралія, Австрія, Бельгія, Великобританія, Данія, Естонія, Ізраїль, Ісландія, Ірландія, Канада, Люксембург, Нідерланди, Німеччина, Нова Зеландія, Норвегія, Сінгапур, США, Фінляндія, Франція, Швеція, Швейцарія. Цей кластер сформували розвинуті країни з потужним економічним потенціалом та високим рівнем інформаційної безпеки (рис. 1, табл. 1). Отже, за виникнення різних загроз інформаційній безпеці ці країни зможуть швидше подолати наслідки інформаційної кризи. Також високий рівень їх безпеки говорить про те, що вони для системи безпеки застосовують сучасні комп'ютерні технології та програмні засоби, які дають їм змогу швидко попереджати загрози.

Кластер 1 сформували 4 країни, а саме Японія, Іспанія, Катар та Арабські Емірати. Вони мають також високі показники розвитку та інформаційної безпеки, які представлені у табл. 1 та на рис. 1. Однак порівняно з країнами 0-го кластеру країни 1-го кластеру мають рівень інформаційної безпеки значно нижчий, що проявляється у таких показниках, як ICT Development Index, Networked Readiness Index, Digital Development Level, National Cyber Security Index. Це говорить про те, що, ймовірно, є певні проблеми в системі інформаційної безпеки цих країн, які потребують вирішення шляхом зміни стратегії інформаційної безпеки.

До 2-го кластеру увійшли 20 країн, а саме Болгарія, Чилі, Хорватія, Кіпр, Чехія, Греція, Угорщина, Італія, Латвія, Литва, Малайзія, Мальта, Маврикій, Польща, Португалія, Румунія, Саудівська Аравія, Словаччина, Словенія, Уругвай, тобто сюди увійшла частина розвинутих країн та ті, що розвиваються, які мають середні показники розвитку, що говорить про їх достатні можливості подолання інформаційної кризи (рис. 1, табл. 1). Однак показники безпеки є нижчими порівняно з країнами 1-го кластеру, особливо це стосується ICT Development Index, Networked Readiness Index, Digital Development Level, Global Cyber Security Index. Проблемами інформаційної безпеки країн цього кластеру можуть бути ті, які пов'язані з правовими аспектами в цій сфері, рівнем організації освіти, недостатнім рівнем інвестування у новітні інформаційні технології.

До 3-го кластеру увійшли 8 країн, а саме Багами, Бахрейн, Барбадос, Бруней, Південна Корея, Чорногорія, Оман, Сербія. Низка показників розвитку країн

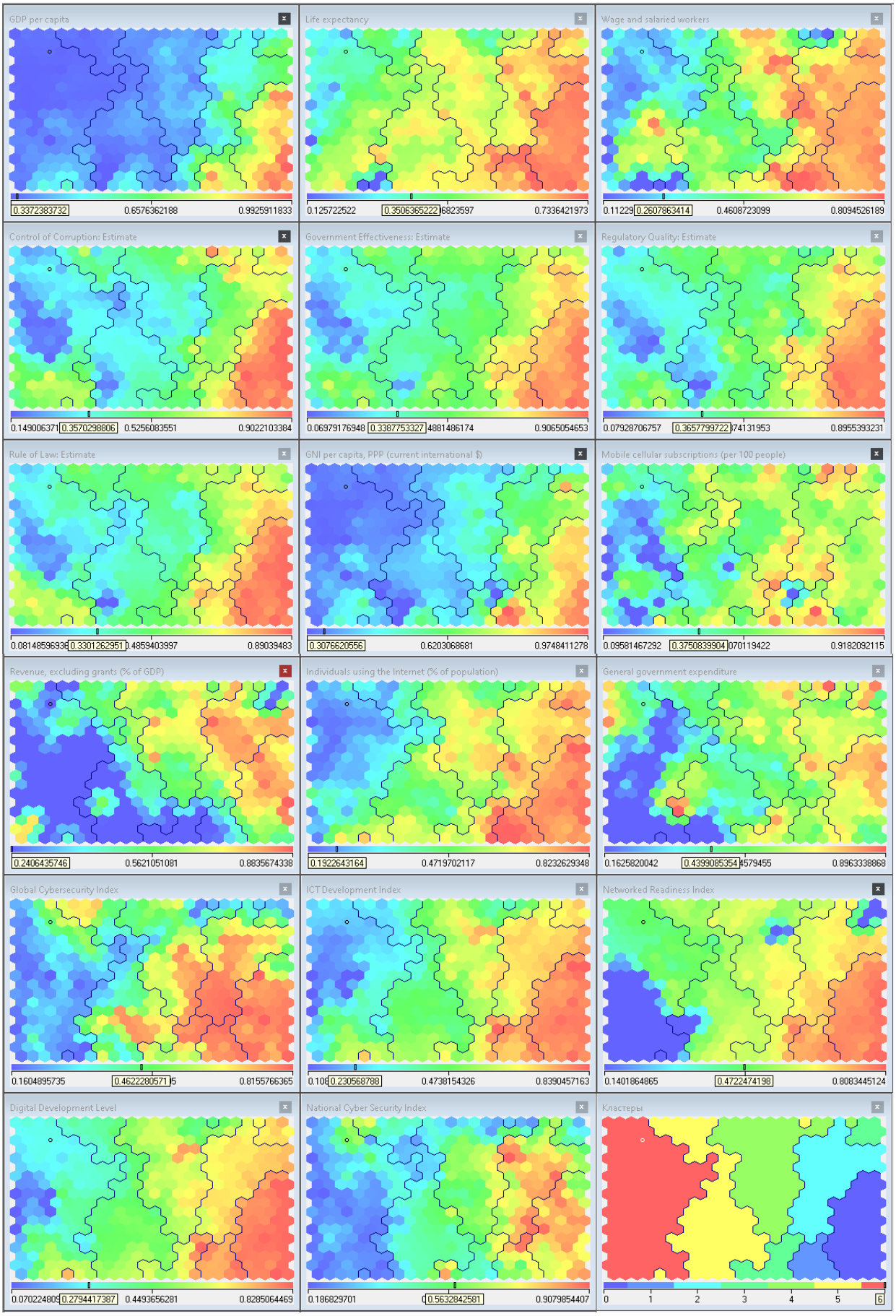

Рис. 1. Карти Кохонена показників інформаційної безпеки та розвитку

Таблиця 1

Середні значення показників згідно з профілем кластеру

Назва показника	0-й кластер	1-й кластер	2-й кластер	3-й кластер	4-й кластер	5-й кластер	6-й кластер
GDP per capita	58 179,42	45 353,09	19 481,37	21 216,71	7 133,42	5 018,98	2 825,30
Life expectancy	81,85	81,36	78,12	77,29	73,82	69,87	63,90
Wage and salaried workers	87,59	92,34	82,18	84,82	63,97	49,86	32,86
Control of Corruption	1,81	0,98	0,43	0,46	-0,22	-0,40	-0,70
Government Effectiveness	1,64	1,19	0,71	0,50	0,01	-0,23	-0,87
Regulatory Quality	1,67	0,93	0,79	0,45	0,05	-0,40	-0,80
Rule of Law	1,68	1,01	0,64	0,40	-0,21	-0,44	-0,69
GNI per capita	56 525,24	61 757,50	32 200,00	27 756,25	16 200,77	94 50,69	5 560,59
Mobile cellular subscriptions	122,33	151,94	128,07	111,12	124,97	106,35	58,79
Revenue, excluding grants	32,38	8,21	34,35	2,05	27,40	9,98	6,06
Individuals using the Internet	90,45	93,87	77,35	85,17	66,51	53,09	26,28
General government expenditure	19,72	16,85	17,42	19,46	16,26	11,57	6,26
Global Cybersecurity Index	84,00	86,25	72,25	56,88	55,81	46,45	20,73
ICT Development Index	82,81	76,50	70,20	70,63	57,19	43,38	24,73
Networked Readiness Index	80,29	74,75	65,05	41,50	56,35	47,79	22,65
Digital Development Level	81,50	75,62	67,50	68,97	58,21	48,15	31,04
National Cyber Security Index	71,37	61,69	67,53	38,47	38,81	30,32	15,89

Рис. 2. Матриці помилок квантування, щільності попадання, відстаней

цього кластеру перевищує показники країн 2-го кластеру, а саме GDP per capita, Wage and salaried workers, Individuals using the Internet, General government expenditure (рис. 1, табл. 1). Це свідчить про те, що ці країни перебувають на стадії свого активного розвитку, як і країни 2-го кластеру. Однак щодо рівня інформаційної безпеки, то є проблеми стосовно розвитку загальної стратегії інформаційної безпеки, про що свідчать низькі показники National Cyber Security Index, Global Cybersecurity Index та Networked Readiness Index. Окрім цього, можна виділити проблему, пов'язану з низьким рівнем технологічної готовності країни до забезпечення надійної системи інформаційної безпеки.

До 4-го кластеру увійшли 26 країн, а саме Албанія, Аргентина, Вірменія, Азербайджан, Білорусь, Боснія та Герцеговина, Ботсвана, Бразилія, Колумбія, Коста Ріка, Грузія, Ямайка, Йорданія, Казахстан, Мексика, Молдова, Монголія, Марокко, Намібія, Північна Македонія, Російська Федерація, Сейшели, Південна Африка, Тайланд, Туреччина, Україна. Частину країн цього кластеру сформували колишні республіки Радянського Союзу, а також низка країн, які пережили становлення через минулі військові події. Нині їх усіх можна віднести до групи країн, що розвиваються, але вони мають низку суттєвих проблем в економічній, соціальній та політичній сферах. Це підтверджується їх низькими значеннями показників розвитку порівняно з країнами попередніх кластерів (рис. 1, табл. 1). Щодо їх стану інформаційної безпеки, то отримані показники безпеки свідчать про їх невисокий рівень, тобто для розвитку сфери безпеки є потреба залучення коштів для забезпечення змін не тільки на рівні стратегії інформаційної безпеки, але й на рівні її окремих складових частин, зокрема рівня технологічного розвитку, впровадження нових комп'ютерних програм, зміни стандартів, реформування законодавства.

До 5-го кластеру увійшли 29 країн, а саме Алжир, Бутан, Болівія, Китай, Кот-д'Івуар, Куба, Домініканська республіка, Еквадор, Єгипет, Ель Сальвадор, Гана, Гватемала, Індія, Індонезія, Іран, Кенія, Киргизстан, Панама, Парагвай, Перу, Філіппіни, Руанда, Сан Кітс и Невіс, Сенегал, Тринідад і Тобаго, Туніс, Узбекистан, Венесуела, В'єтнам. Цей кластер сформували країни, які розвиваються, але мають низькі показники розвитку та низький рівень інформаційної безпеки (рис. 1, табл. 1). Хоча до цього кластеру увійшли також країни, які є новими індустріальними, а саме Індія, Індонезія, Китай, Філіппіни, але вони мають досить низький рівень безпеки, що дало змогу віднести їх до цієї групи. Головними проблемами цього кластеру є передусім

вирішення питань, пов'язаних з економічним розвитком, але ці країни мають відповідний потенціал для розвитку та інформаційної безпеки. Про це свідчить їх достатній рівень розвитку інформаційних технологій, цифровізації різних сфер та технологічної готовності.

До 6-го кластеру увійшла 51 країна, що належать до групи найменш розвинутих країн, які характеризуються дуже низькими показниками розвитку економіки, соціальної та політичної сфер (рис. 1, табл. 1). Більшість країн цього кластеру складають країни Африки та Близького Сходу, де тривають озброєні конфлікти. Для таких країн першочерговими завданнями 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 зміні програмно-технічної інфраструктури на мікрорівні, а потім на рівні держави.

Висновки. Проблеми, пов'язані з інформаційною безпекою, є актуальними у світі, тому є потреба проведення аналізу країн щодо відповідності їх рівня розвитку рівню інформаційної безпеки. Це дасть змогу виділити не тільки групи країн, які слабко розвиваються у напрямі підвищення ефективності системи інформаційної безпеки, але й ті сфери, які потребують додаткової уваги з боку відповідних державних органів, які займаються питаннями безпеки країни. Одним із дієвих інструментів для проведення такого аналізу є самоорганізовані карти Кохонена, які дають змогу не тільки зробити візуалізацію кластерів, але й детально проаналізувати отримані профілі згідно з досліджуваними показниками.

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

В подальшому дослідження планується спрямувати на розроблення конкретних рекомендацій для кожного кластеру країн з огляду на більш детальний аналіз складових частин інформаційної безпеки та показників їх розвитку, що сприятиме виробленню конкретних моделей удосконалення та розвитку діючої системи інформаційної безпеки для відповідної групи країн.

Список використаних джерел:

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

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

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

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

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

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

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

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

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

10. World Development Indicators. *The World Bank.* URL: https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on (дата звернення: 20.08.2020).

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

References:

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

2. Kirilenko, V.P., Alexeyev, G.V. (2018). Political technologies and international conflicts in the information space of the Baltic Sea region. *Baltic Region,* 10(4), 20–38. DOI: 10.5922/2079-8555-2018-4-2.

3. Singh, A.N., Gupta, M.P. (2019). Information Security Management Practices: Case Studies from India. *Global Business Review,* 20(1), 253–271. DOI: 10.1177/0972150917721836.

4. Ključnikov, A., Mura, L., Sklenár, D. (2019). Information security management in smes: Factors of success. *Entrepreneurship and Sustainability Issues,* 6(4), 2081–2094. DOI: 10.9770/jesi.2019.6.4(37).

5. Sadigov, M., Kuzmenko, O., Yarovenko, H. (2020, June). Blockchain technology based system-dynamicsimulation modeling of enterprise's syber security system. In proceedings of the 55th International Scientific Conference on Economic and Social (Azerbaijan, Baku, 18–19 June 2020). *Varazdin Development and Entrepreneurship Agency*, vol. 1/4, pp. 399–408. Available at: https://www.esd-conference.com/upload/book_of_proceedings/Book_of_Proceedings_esdBaku2020_Vol1_Online.pdf (accessed 20 August 2020).

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

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

8. Yevseiev S., Aleksiyev V., Balakireva S., Peleshok Y., Milov O., Petrov O., Rayevnyeva O., Tomashevsky B., Tyshyk I., Shmatko O. (2019) 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,* vol. 3, no. 9–99, pp. 49–63. DOI: 10.15587/1729-4061.2019.169527.

9. National Cyber Security Index. NCSI. Available at: https://ncsi.ega.ee/ncsi-index (accessed 20 August 2020).

10. World Development Indicators. *The World Bank.* Available at: https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on (accessed 20 August 2020).

11. Kohonen, T. (1982). Self-Organized Formation of Topologically Correct Feature Maps. *Biological Cybernetics,* 43 (1), pp. 59–69. DOI: 10.1007/BF00337288.