УДК 37.012.4:004.056:330.34
DOI: https://doi.org/10.32782/2413-9971/2020-31-26

Яровенко Г. М.
кандидат економічних наук,
доцент, доцент кафедри економічної кібернетики
Сумського державного університету

Yarovenko Hanna
PhD, Associate Professor,
Associate Professor of the Economic Cybernetics Department
Sumy State University

КАНОНІЧНИЙ АНАЛІЗ ВЗАЄМОЗВ'ЯЗКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СОЦІО-ЕКОНОМІКО-ПОЛІТИЧНОГО РОЗВИТКУ КРАЇНИ[1]

Анотація. Одним з драйверів сучасного розвитку країни може виступати її інформаційна безпека, тому у статті автором було висунуто гіпотезу щодо існування взаємозв'язку між інформаційною безпекою країни та її соціо-економіко-політичним розвитком, що доводилося за допомогою канонічного аналізу. Для дослідження було вибрано дані національного індексу кібербезпеки та фактори соціо-економіко-політичного розвитку для 159 країн світу за 2018 рік. Побудовано карту країн світу із зазначенням національного індексу кібербезпеки. Це дало змогу зробити попередній висновок про справедливість висунутої гіпотези. Канонічний аналіз проводився в аналітичному пакеті STATISTICA, в результаті чого було визначено канонічні корені, факторну структуру, дисперсію та надмірність, канонічні ваги для факторів, регресійні рівняння. Результати аналізу підтвердили справедливість гіпотези, що фактори розвитку обумовлюють рівень інформаційної безпеки та навпаки, рівень безпеки може впливати на розвиток країни.

Ключові слова: канонічний аналіз, кореляційний аналіз, інформаційна безпека, національний індекс кібербезпеки, соціо-економіко-політичний розвиток, STATISTICA.

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

З іншого боку, цифровізація та комп'ютеризація суспільства приводять до того, що отримання інформації стає метою злочинців та шахраїв, які здійснюють хакерські атаки для незаконного отримання інформації компанії, викрадають дані клієнтів платіжних систем, провадять вірусні атаки для руйнування інформаційного середовища та усунення конкурентів компанії тощо, тому зростає необхідність підвищення заходів кібербезпеки зокрема та інформаційної безпеки загалом. Це питання є актуальним не тільки для окремих компаній, різних установ, банків, але й для країни загалом. Інформаційна безпека на рівні держави є досить складним поняттям, яке уособлює низку інститутів, заходів, які сприяють захисту інформаційного простору країни та суспільства від здійснення зовнішніх, незаконних інформаційних атак, кібертероризму, які завдають шкоди національним інтересам, соціальному, економічному та політичному життю країни, тому для ефективної організації системи інформаційної безпеки важливо розуміти, яким чином вона формується та від яких чинників залежить. Відповідно, можна сформувати гіпотезу про те, що ефективність системи інформаційної безпеки на державному рівні обумовлюється факторами соціально-економічного розвитку країни, тобто розвинуті країни з потужним соціально-економічним потенціалом та стабільною політичною ситуацією мають підвищений рівень інформаційної безпеки та навпаки, збільшення її рівня впливає на розвиток країни. Ця гіпотеза потребує перевірки та підтвердження або відхилення.

Аналіз останніх досліджень і публікацій. З появою новітніх технологій та зі збільшенням кількості й видів кібершахрайств зросла також кількість публікацій, присвячених теоретичним та практичним питанням інформаційної безпеки на рівні підприємств, банків та держави. Галузі, в яких здійснюються дослідження науковців, пов'язані з різними напрямами інформаційної безпеки, зокрема з комп'ютерними науками, інженерією, математикою, соціальними науками, бізнесом, економікою, менеджментом. Хоча це питання є актуальним передусім для комп'ютерної галузі, оскільки саме ця сфера відповідає за програмну, технічну, методологічну та інформаційну складові частини захисту інформації незалежно від сфери діяльності людини.

Серед українських учених можна виділити низку науковців, які досліджують проблему інформаційної безпеки. Так, її вирішенням на макрорівні, а саме процесом реформування системи інформаційної безпеки країн, які належать до НАТО, займаються М. Лошицький,

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

О. Костенко, І. Коропатник, Г. Терещук, В. Карелін [1]. Також важливим є розроблення захисту критичної інфраструктури держави, що здійснюють С. Гнатюк, В. Сидоренко, А. Положенцев, А. Фесенко [2]. Вагомий аспект інформаційної безпеки – це виникнення та попередження загроз, серед яких найбільший вплив здійснює інформаційна війна, тому цей аспект з боку інформаційної безпеки держави висвітлюють К. Чижмар, О. Дніпров, О. Коротюк, Р. Шаповал, О. Сидоренко [3]. Вплив інформаційних війн на інформаційну та економічну безпеку підприємств досліджує О. Сороківська [4]. Також можна виділити науковців, які займаються розробленням системи комплексної оцінки рівня культури інформаційної безпеки на рівні персоналу, таких як С. Шкарлет, В. Литвинов, М. Дорош, Е. Трунова, М. Войцеховська [5]. Для боротьби з інформаційними загрозами та забезпечення належного рівня безпеки існує потреба розроблення та впровадження низки комплексних підходів. В цій сфері можна виділити дослідження С. Євсєєва, В. Алексієва, С. Балакірєва, Ю. Пелешка, О. Милова, О. Петрова, О. Раєвнєвої, Б. Томашевського, І. Тишика, О. Шматька [6].

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

Метою статті є доведення або відхилення за допомогою канонічного аналізу висунутої гіпотези щодо обопільної обумовленості ефективності системи інформаційної безпеки факторами соціо-економіко-політичного розвитку країни.

Результати дослідження. Для доведення висунутої гіпотези як показника, що характеризує рівень інформаційної безпеки країни, вибрано національний індекс кібербезпеки, який використовується для оцінювання підготовленості країни протидіяти різним кіберзагрозам та можливості керувати різними кібер-інцидентами. Хоча цей показник звужує рамки прийнятого в Україні поняття інформаційної безпеки, у світовій практиці саме він застосовується для надання актуальної та точної інформації щодо розвитку національних систем кібербезпеки (інформаційної безпеки), порівняння дій влади в галузі безпеки інформації та отримання інформації щодо найкращих практик у цій сфері [7]. Також складові частини національного індексу кібербезпеки характеризують безпеку за 12 напрямами, такими як розроблення політики та стратегії в галузі кібербезпеки; аналіз та інформація щодо кіберзагроз; організація освіти та професійного розвитку у галузі кібербезпеки; оцінювання внеску у глобальну кібербезпеку; рівень захисту цифрових послуг, таких як відповідальність, стандарти, органи; організація захисту основних послуг; електронна ідентифікація та послуги довіри; захист персональних даних; реагування на кібер-інциденти; кіберрегулювання кризи; боротьба з кіберзлочинністю; військові кібер-операції [7]. Отже, на нашу думку, цей індикатор та його складові частини дадуть змогу в повному обсязі здійснити оцінювання рівня інформаційної безпеки країни загалом.

Використовуючи значення національного індикатора кібербезпеки за 2018 рік для 159 країн світу, побудуємо карту, яка дасть змогу зробити візуальний аналіз географії країн та оцінити, для яких країн характерний високий рівень безпеки, а для яких країн – низький (рис. 1).

Аналізуючи дані, представлені на рис. 1, можемо сказати, що держави, які належать до розвинутих, зокрема країни Європи, США, Канада, Австралія, мають високі значення національного індексу кібербезпеки. Хоча якщо порівнювати країни, що розвиваються, наприклад Украї-

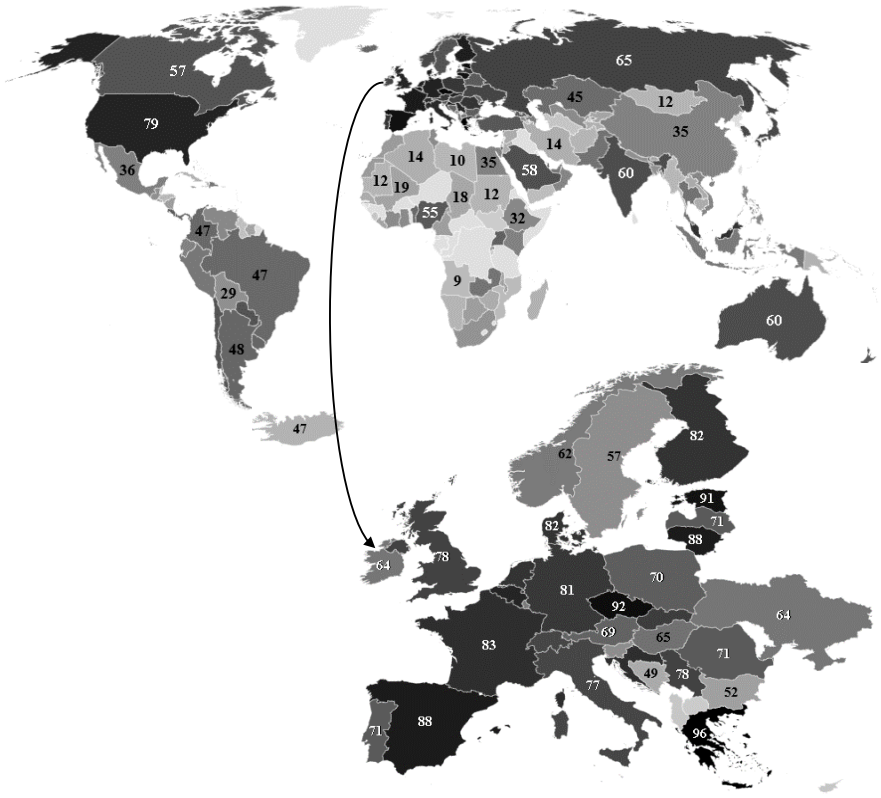

Рис. 1. Карта країн світу з визначеним національним індексом кібербезпеки

Джерело: побудовано автором на основі джерела [8]

їну, яка має індекс 64, та розвинуту країну Австралію з індексом 60, то можна дійти висновку, що рівень безпеки в Україні вищий. Також цей показник у України є вищим порівняно з такими розвинутими країнами, як Канада (57), Швеція (57), Норвегія (62), Японія (62). Це характерно також для Малайзії, Росії, Індії та низки інших країн, що розвиваються, тобто за рівнем національного індексу кібербезпеки вони випереджають низку розвинутих країн. Можна виділити також Нігерію, показник якої дорівнює 55, тобто за рівнем кібербезпеки ця країна наздоганяє Канаду та Швецію. Щодо країн, які є найменш розвинутими, то вони мають досить низькі показники кібербезпеки, тобто візуальний аналіз нам дав змогу зробити висновок, що переважно країни, які є розвинутими, мають дійсно високі показники національного рівня кібербезпеки, що свідчить про їх високий рівень загалом. Частина країн, які вважаються такими, що розвиваються, також мають високий рівень кібербезпеки. Можна попередньо прийняти нашу гіпотезу щодо існування впливу рівня економіко-соціо-політичного розвитку країн на рівень інформаційної безпеки країни.

Для подальшого підтвердження гіпотези проведемо канонічний аналіз, який дасть нам змогу математично прийняти або відхилити висунуту гіпотезу. Цей інструмент дає змогу досліджувати залежності між двома множинами змінних та виявляти зв'язки між ними, що дасть змогу оцінити ступінь впливу однієї множини на іншу та обґрунтувати її статистичну значимість [9, с. 185].

Для проведення дослідження вибрано низку показників для 159 країн світу. Їх вибір здійснювався з огляду на те, яким чином ці індикатори відображають розвиток країни, зокрема економічний, соціальний або політичний. Так, базу даних сформували індикатори економічного розвитку за 2018 рік, а саме [10] ВВП на душу населення (у поточних доларах США); загальнодержавні витрати на кінцеве споживання (% від ВВП); чисті портфельні інвестиції (платіжний баланс у поточних доларах США); загальний рівень безробіття (% від загальної робочої сили); інфляція, дефлятор ВВП (річний у %); загальні резерви (включаючи золото у поточних доларах США); сальдо поточного рахунку (платіжний баланс у поточних доларах США); оплачувані та наймані працівники (% від загальної кількості зайнятих); індекс GINI; експорт товарів та послуг (% від ВВП); високотехнологічний експорт (% від промислового експорту); запаси зовнішньої заборгованості, загальна заборгованість (погашена та непогашена заборгованість у поточних доларах США); чистий приплив прямих іноземних інвестицій (платіжний баланс у поточних доларах США); ВВП (поточні долари США); приріст ВВП (річний у %); ВНД на душу населення за паритетом купівельної здатності (у поточних міжнародних доларах); ВНД за паритетом купівельної здатності (у поточних міжнародних доларах); валовий капітал (% від ВВП); імпорт товарів та послуг (% від ВВП); промисловість, включаючи будівництво, додана вартість (% від ВВП); дохід без урахування грантів (% від ВВП); податкові надходження (% від ВВП).

Також було вибрано індикатори, які характеризують соціо-політичний рівень розвитку країни [10], такі як оцінка контролю корупції; оцінка ефективності уряду; оцінка політичної стабільності та відсутності насильства/тероризму; оцінка якості регуляторів; оцінка верховенства права; оцінка потужності статистичної системи країни; ймовірна тривалість життя; кількість підписок на послуги мобільного зв'язку (на 100 осіб); кількість осіб, які користуються Інтернетом (% від населення країни); кількість захищених інтернет-серверів (на 1 мільйон людей); плата за використання інтелектуальної власності, платежі (BoP, поточні долари США); збори за використання інтелектуальної власності, квитанції (BoP, поточні долари США); патентні заявки, нерезиденти; патентні заявки, резиденти; статті науково-технічних журналів.

На першому кроці було проведено кореляційний аналіз у аналітичному пакеті STATISTICA між вибраними соціо-економіко-політичними показниками розвитку країн та складовими частинами індикатора національної кібербезпеки. Цей аналіз дав нам змогу вибрати саме ті показники, між якими існує статистичний зв'язок. Як правило, на практиці пріоритет надається тільки тим показникам, між якими існує тісний зв'язок, але нами було враховано всі показники, які мали хоча б слабкий зв'язок, тобто значення коефіцієнта кореляції для них перевищувало рівень 0,3. Це було зроблено задля визначення всього набору показників, які мають хоча б якійсь зв'язок з інформаційною безпекою. В результаті було вибрано тільки 19 показників соціо-економіко-політичного розвитку та 12 складових частин національного індикатору кібербезпеки.

На наступному кроці було проведено канонічний аналіз, мета якого полягає у визначенні лінійних залежностей між групами змінних, що дає змогу оцінити вплив однієї групи факторів на іншу та навпаки. Загальну ідею аналізу зобразимо у вигляді таких рівнянь (формула 1):

$$Y = a_1 y_1 + a_2 y_2 + \ldots + a_{12} y_{12}; X = b_1 x_1 + b_2 x_2 + \ldots + b_{19} x_{19}, . \quad (1)$$

де $y_1, y_2, ..., y_{12}$ – множина змінних, які відображають складові частини національного індексу кібербезпеки; $x_1, x_2, ..., x_{19}$ – множина змінних, які відображають відібрані показники соціо-економіко-політичного розвитку країни; Y та X – зважені суми змінних кожної множини, які є канонічними змінними та які визначають канонічний корень; $a_1, a_2, ..., a_{12}$; $b_1, b_2, ..., b_{19}$ – вагові коефіцієнти, які розраховуються з огляду на максимальну корельованість обох множин.

В результаті виконання модуля канонічного аналізу в пакеті STATISTICA отримано підсумки, представлені на рис. 2.

З рис. 2 можна побачити, що значення канонічної кореляції R = 0,89935, тобто між множиною відібраних соціо-економіко-політичних факторів та складових частин індексу кібербезпеки існує сильний кореляційний зв'язок. Як наслідок, збільшення впливу соціо-економіко-політичних факторів викликає підвищення рівня кібербезпеки країни, а посилення рівня кібербезпеки позитивно впливає на соціо-економіко-політичний розвиток країни.

Значимість коефіцієнта кореляції підтверджує високе значення критерія Пірсона (χ^2=535,10), рівень значущості якого не перевищує 0,05 (p = 0,0000). Також можна побачити, що значення надмірності для лівої множини, яка відповідає складовим частинам показника кібербезпеки, дорівнює 49,1399 %, тобто змінні правої множини, які відповідають вибраним індикаторам соціо-економіко-політичного розвитку країни, на 49,1399 % пояснюють мінливість показників кібербезпеки, що є досить високим показником. Фактори кібербезпеки на 38,4118 % пояснюють мінливість факторів соціо-економіко-політичного розвитку країни, тобто приблизно на 40 % розвиток країни залежить також від рівня захищеності інформаційного та кібернетичного простору держави, що є досить значним для такої специфічної сфери, як інформаційна безпека.

Для подальшого аналізу необхідно вибрати ті канонічні корені, які є статистично значущими. Результат отриманих коренів та перевірки їх статистичної значущості представлений на рис. 3.

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

Рис. 2. Підсумки канонічного аналізу

Джерело: побудовано автором самостійно

З рис. 3 визначаємо, що Хі-квадрат у першому рядку, який відповідає аналізу без видалення коренів, є статистично значущим ($p < 0,05$), тому хоча б один канонічний корінь є також статистично значущим. За видалення першого найбільш значущого кореня (другий рядок таблиці на рис. 3) отримуємо, що інші корені, які залишилися, є також значущими. Процедуру повторюємо доти, доки $p > 0,05$. В результаті отримали три статистично значущих корені, тобто доцільно розглядати три пари канонічних змінних. Однак 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 [9, с. 190], тому приймаємо рішення, що будемо розглядати тільки перший найбільш значущий корінь. Для підтвердження своїх висновків визначимо факторну структуру та надмірність (рис. 4, 5).

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

Рис. 3. Оцінка статистичної значущості канонічних коренів

Джерело: побудовано автором самостійно

Найбільші факторні навантаження мають показники, що відповідають першому кореню як для лівої, так і для правої множин. Оскільки факторні навантаження є кореляціями між показниками множини, то показники національної безпеки демонструють середній та вище середнього кореляційний зв'язок. Щодо факторів розвитку, то між ними зустрічаються ті, які демонструють слабкий зв'язок.

Однак оскільки нам важливо виявити показники, які мають будь-який рівень зв'язку, то будемо мати на увазі, що оцінка політичної стабільності та відсутності насильства/тероризму, експорт товарів та послуг, оцінка потужності статистичної системи країни, кількість захищених інтернет-серверів, платежі за використання інтелектуальної власності чинять слабкий вплив на рівень національної кібербезпеки.

Проаналізуємо отримані частки та надмірності дисперсії. В разі аналізу складових частин національної кібербезпеки 100 % дисперсії будуть пояснювати всі вилучені корені, в разі факторів розвитку країни – тільки 74,8 %. Перший канонічний корінь вилучає 49,1119 % дисперсії зі складових частин національної кібербезпеки

Root Variable	Factor Structure, left set		
	Root 1	Root 2	Root 3
1. Cyber Security Policy Development	0.760024	0.002491	-0.186045
2. Cyber Threat Analysis and Information	0.804363	0.223792	-0.221587
3. Education and Professional Development	0.829012	-0.085878	0.070746
4. Contribution to global cyber security	0.687848	0.309192	-0.028693
5. Protection of digital services	0.481421	0.564479	0.326512
6. Protection of essential services	0.640548	0.376292	0.366621
7. E-identification and trust services	0.693371	-0.233652	0.395539
8. Protection of personal data	0.677602	-0.036897	0.190406
9. Cyber incidents response	0.616932	-0.004646	0.156909
10. Cyber crisis management	0.690835	-0.005328	0.244479
11. Fight against cybercrime	0.795608	-0.300298	0.119870
12. Military cyber operations	0.659978	0.026670	-0.313077

Рис. 4. Факторна структура для складових частин національної кібербезпеки (фрагмент)

Джерело: побудовано автором самостійно

та 38,2117 % дисперсії з факторів розвитку країни, тобто пояснює 49,1119 % та 38,2117 % зміни рівня національної кібербезпеки та рівня соціо-економіко-політичного розвитку. Інші корені, хоча ми не братимемо їх до уваги, пояснюють від 2 % до 6 % змін, що є незначним. З огляду на надмірність 39,7229 % факторів розвитку пояснюють зміни показників лівої множини, тобто складових частин національної кібербезпеки. 30,9065 % факторів національної кібербезпеки пояснюють зміни, пов'язані з розвитком країни. Як наслідок, фактори розвитку є більш інформативними для передбачення рівня національної кібербезпеки країни.

Для подальшого аналізу визначимо канонічні ваги, які є коефіцієнтами регресійних рівнянь, де канонічні змінні є відповідними відкликами (рис. 6, 7).

Значення канонічних вагів дає змогу визначити внесок кожного показника у формування значень канонічних змінних. В національну кібербезпеку вноситимуть найбільший вклад (рис. 6) захист персональних даних; аналіз та інформація щодо кіберзагроз; організація освіти та професійного розвитку у галузі кібербезпеки; найменший вклад – організація захисту основних послуг; електронна ідентифікація та послуги довіри; кіберрегулювання кризи.

Щодо факторів розвитку, то найбільший вклад втілюватимуть (рис. 7) оцінка якості регуляторів; дохід без урахування грантів; податкові надходження; найменший вклад – оплачувані та наймані працівники; платежі за використання інтелектуальної власності; ВВП на душу населення; кількість підписок на послуги мобільного зв'язку. При цьому треба враховувати знак значення показника. Якщо вага має знак «+», то зі збільшенням фактору значення кореня збільшується, якщо «–», то, навпаки, значення кореня зменшується. Наприклад, якщо платежі за використання інтелектуальної власності будуть збільшуватися, то це буде зменшувати внесок цього вкладу у значення кореня.

Значення канонічних вагів дало нам змогу визначити рівняння регресії для канонічних змінних лівої та правої множин (формула 2):

$$Y\ (1\ \text{корень}) = 0{,}0934y_1 + 0{,}2763y_2 + 0{,}2568y_3 + 0{,}1072\ y_4 - 0{,}0946y_5 + 0{,}0582y_6 + 0{,}0507y_7 + 0{,}2804y_8 + 0{,}0984y_9 + 0{,}0284y_{10} + 0{,}0716y_{11} + 0{,}1000y_{12},$$

$$X\ (1\ \text{корень}) = -0{,}0331x_1 + 0{,}0907x_2 + 0{,}0703x_3 + 0{,}0286x_4 - 0{,}4000x_5 + 0{,}3394x_6 - 0{,}2858x_7 + 0{,}5324x_8 + 0{,}2539x_9 - 0{,}1917x_{10} + 0{,}2109x_{11} + 0{,}0588x_{12} - 0{,}0334x_{13} + 0{,}5246x_{14} + 0{,}0608x_{15} - 0{,}4487x_{16} + 0{,}2051x_{17} + 0{,}0872x_{18} - 0{,}0275x_{19}. \quad (2)$$

Якщо є потреба у визначенні для кожної країни значення канонічних змінних, то необхідно підставити в

Root Variable	Factor Structure, right set		
	Root 1	Root 2	Root 3
GDP per capita	0.690718	0.287945	-0.094678
General government expenditure	0.582425	0.012476	0.040691
Life expectancy	0.560505	-0.073121	0.092636
Wage and salaried workers	0.689980	-0.055039	0.015387
Control of Corruption: Estimate	0.670031	0.287895	-0.102873
Government Effectiveness: Estimate	0.828089	0.155910	-0.005329
Political Stability and Absence of Violence/Terrorism: Estimate	0.386819	0.291094	0.076111
Regulatory Quality: Estimate	0.857579	0.086692	0.056519
Rule of Law: Estimate	0.751873	0.300340	-0.058753
Exports of goods and services	0.422173	0.302194	0.706982
GNI per capita	0.778433	0.178293	0.027060
High-technology exports	0.533411	0.270292	0.166244
Mobile cellular subscriptions	0.526399	-0.278181	0.250180
Revenue, excluding grants	0.643730	0.081836	0.122554
Statistical Capacity score	-0.408921	-0.592820	0.198385
Tax revenue	0.520408	0.027981	0.075796
Individuals using the Internet	0.775450	0.060895	0.247898
Secure Internet servers	0.396156	0.382797	-0.107892
Charges for the use of intellectual property, payments	0.334831	0.253151	0.071409

Рис. 5. Факторна структура для факторів розвитку країни (фрагмент)

Джерело: побудовано автором самостійно

отримане рівняння (2) значення факторів розвитку та складових частин національного індикатору кібербезпеки. Це дасть змогу знайти зважену суму факторів з урахуванням впливу множин одна на одну.

На наступному кроці побудовано діаграму розсіювання канонічних значень для першої пари канонічних коренів (рис. 8), в якій горизонтальна вісь – це складові частини національного індексу кібербезпеки, а вертикальна – показники соціо-економіко-політичного розвитку.

На діаграмі 8 можна побачити, що скупчення спостережень є характерним для лінійної залежності, при цьому графік не містить значних викидів. Це свідчить про те, що між складовими частинами національної кібербезпеки та факторами соціо-економіко-політичного розвитку є досить тісний зв'язок, який говорить про те, що рівень національної кібербезпеки, а в нашому випадку інформаційної безпеки, залежить від рівня розвитку країни, при цьому рівень безпеки може також впливати на розвиток країни.

Variable	Canonical Weights, left set		
	Root 1	Root 2	Root 3
1. Cyber Security Policy Development	0.093381	-0.185643	-0.532721
2. Cyber Threat Analysis and Information	0.276326	0.439113	-0.584769
3. Education and Professional Development	0.256820	-0.243435	-0.077787
4. Contribution to global cyber security	0.107176	0.440184	0.010013
5. Protection of digital services	-0.094643	0.609075	0.196664
6. Protection of essential services	0.058188	0.392554	0.564118
7. E-identification and trust services	0.050683	-0.385354	0.517350
8. Protection of personal data	0.280400	0.059237	-0.014170
9. Cyber incidents response	0.098364	-0.082615	0.004520
10. Cyber crisis management	0.028405	-0.169556	0.449290
11. Fight against cybercrime	0.071589	-0.551104	0.212369
12. Military cyber operations	0.100034	-0.036566	-0.537026

Рис. 6. Канонічні ваги для складових частин національної кібербезпеки (фрагмент)

Джерело: побудовано автором самостійно

Висновки. Виходячи з результатів проведеного дослідження, можемо прийняти гіпотезу щодо обумовленості ефективності системи інформаційної безпеки факторами соціально-економічного розвитку країни. Цю гіпотезу було підтверджено візуальним аналізом карти країн світу, розподілених за національним індексом кібербезпеки. Аналіз підтвердив, що країни, які належать до розвинутих, мають найвище значення національного індексу кібербезпеки. Найменш розвинуті країни мають найнижчі значення індексу. В результаті проведеного канонічного аналізу було визначено, що приблизно 49 % множини складових частин показника кібербезпеки пояснюються факторами соціо-економіко-політичного розвитку. Оскільки ці фактори оцінюють спроможність країни протистояти різним кіберзагрозам, то у країн із високим економічним потенціалом збільшуються можливості їм протидіяти, а також зростає фінансова спроможність для організації додаткових заходів, залучення більш сучасних технологій, кваліфікованих фахівців. Однак, з іншого боку, саме у таких країнах підвищується ризик кібератак, інформаційного тероризму та кібершахрайства, тому треба провести додаткове дослідження аналізу впливу рівня кіберзагроз на різні країни світу.

Також було визначено, що 38 % множини факторів розвитку країни пояснюються за рахунок складових частин національної кібербезпеки, тобто підвищення рівня інформаційної безпеки загалом та кібербезпеки зокрема сприятиме розвитку країни щодо соціального, економічного чи політичного розвитку. Чим вище рівень захищеності персональних даним, тим вище довіра населення до

Variable	Canonical Weights, right set		
	Root 1	Root 2	Root 3
GDP per capita	-0.033104	-0.138295	-0.614914
General government expenditure	0.090716	-0.054161	-0.008651
Life expectancy	0.070309	-0.128029	0.196566
Wage and salaried workers	0.028595	0.016751	-0.389475
Control of Corruption: Estimate	-0.399981	0.020568	-0.051804
Government Effectiveness: Estimate	0.339411	-0.387680	-0.341282
Political Stability and Absence of Violence/Terrorism: Estimate	-0.285751	0.132452	0.139113
Regulatory Quality: Estimate	0.532497	-0.646778	0.240597
Rule of Law: Estimate	0.253941	0.914662	-0.036946
Exports of goods and services	-0.191654	0.353281	1.079455
GNI per capita	0.210886	-0.734044	0.204656
High-technology exports	0.058820	0.398051	-0.099102
Mobile cellular subscriptions	-0.033339	-0.192015	0.207310
Revenue, excluding grants	0.524632	0.682581	0.044147
Statistical Capacity score	0.060800	-0.836141	0.019507
Tax revenue	-0.448721	-0.601972	-0.002488
Individuals using the Internet	0.205069	-0.022148	0.064643
Secure Internet servers	0.087222	0.364151	-0.423961
Charges for the use of intellectual property, payments	-0.027525	0.078019	0.300656

Рис. 7. Канонічні ваги для факторів розвитку країни (фрагмент)

Джерело: побудовано автором самостійно

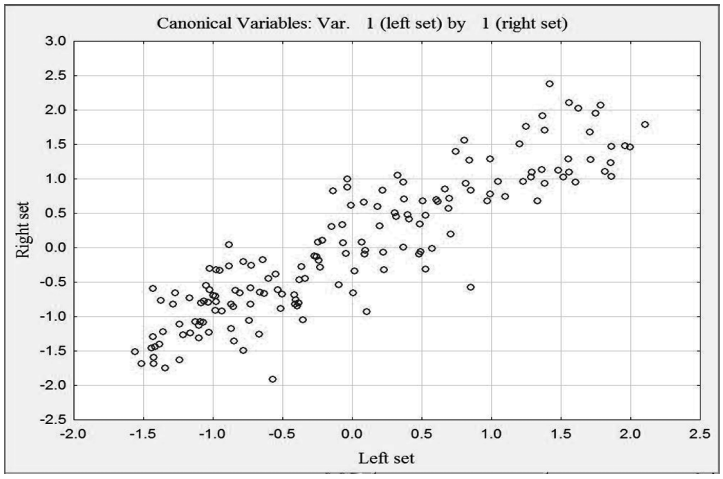

Рис. 8. Діаграма розсіювання канонічних значень

Джерело: побудовано автором самостійно

держави та різних інститутів. Якщо це фінансові дані людини, то тим вище надійність банківської системи та менше втрати від кібершахраїв.

Отримані в роботі результати сприятимуть виробленню низки стратегічних заходів саме в тих напрямах, де цей зв'язок є тіснішим. Як наслідок, це приведе до посилення інститутів безпеки, впровадження нових методів та вжиття нових заходів безпеки, що позитивно впливатиме на політичну стабільність у 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, розроблення відповідних норм законодавства, які підвищують відповідальність за кіберзлочини, впровадження потужних аналітичних систем є напрямами впливу на розвиток будь-якої країни.

Список використаних джерел:

1. 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: 10.9770/JSSI.2020.9.3(1).
2. 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. *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.
3. 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: 10.9770/jssi.2020.9.3(8).
4. Sorokivska O.A. Economic security of Ukrainian enterprises under information war. *Actual Problems of Economics*. 2015. Vol. 174. № 12. P. 198–202.
5. Shkarlet S., Lytvynov V., Dorosh M., Trunova E., Voitsekhovska M. The model of information security culture level estimation of organization. *14th International Scientific-Practical Conference, MODS 2019,* Chernihiv, Ukraine; 24 June 2019 through 26 June 2019. Advances in Intelligent Systems and Computing, 2019. Vol. 1019. P. 249–258. DOI: 10.1007/978-3-030-25741-5_25.
6. 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.
7. Rikk R. National Cyber Security Index 2018. *E-governance Academy* : веб-сайт. URL: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf (дата звернення: 20.07.2020).
8. National Cyber Security Index. *NCSI* : веб-сайт. URL: https://ncsi.ega.ee/ncsi-index (дата звернення: 20.07.2020).
9. Халафян А. STATISTICA 6. Статистический анализ данных. Москва : ООО «Бином-Пресс», 2007. 512 с.
10. World Development Indicators. *The World Bank* : веб-сайт. URL: https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on (дата звернення: 20.07.2020).

References:

1. Loshytskyi M., Kostenko O., Koropatnik I., Tereshchuk G., Karelin V. (2020) Organizational competence of NATO information security policy. *Journal of Security and Sustainability Issues*, vol. 9., no. 3, pp. 735–746. DOI: 10.9770/JSSI.2020.9.3(1).
2. Gnatyuk S., Sydorenko V., Polozhentsev A., Fesenko A., Akatayev N., Zhilkishbayeva G. (2020) Method of cybersecurity level determining for the critical information infrastructure of the state. Proceedings of the *2nd International Workshop on Control, Optimisation and Analytical Processing of Social Networks, COAPSN 2020 (Ukraine, Lviv, May 21, 2020),* CEUR Workshop Proceedings, vol. 2616, pp. 332–341.
3. Chyzhmar K., Dniprov O., Korotiuk O., Shapoval R., Sydorenko O. (2020) State information security as a challenge of information and computer technology development. *Journal of Security and Sustainability Issues,* vol. 9, no. 3, pp. 819–828. DOI: 10.9770/jssi.2020.9.3(8).
4. Sorokivska O. (2015) Economic security of ukrainian enterprises under information war. *Actual Problems of Economics,* vol. 174, no. 12, pp. 198–202.
5. Shkarlet S., Lytvynov V., Dorosh M., Trunova E., Voitsekhovska M. (2019) The model of information security culture level estimation of organization. Proceedings of the *14th International Scientific-Practical Conference, MODS 2019 (Ukraine, Chernihiv, June 24–26, 2019)*, Advances in Intelligent Systems and Computing, vol. 1019, pp. 249–258. DOI: 10.1007/978-3-030-25741-5_25.
6. 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.

7. Rikk R. National Cyber Security Index 2018. *E-governance Academy.* Available at: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf (accessed 20 July 2020).
8. National Cyber Security Index. *NCSI.* Available at: https://ncsi.ega.ee/ncsi-index (accessed 20 July 2020).
9. Halafyan A.A. (2007) *STATISTICA 6. Statisticheskiy analiz dannyih* [STATISTICA 6. Statistical data analysis]. M. : LLC "Binom-Press" (in Russian).
10. World Development Indicators. *The World Bank.* Available at: https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on (accessed 20 July 2020).

КАНОНИЧЕСКИЙ АНАЛИЗ ВЗАИМОСВЯЗИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СОЦИО-ЭКОНОМИКО-ПОЛИТИЧЕСКОГО РАЗВИТИЯ СТРАНЫ

Аннотация. Одним из драйверов современного развития страны может выступать ее информационная безопасность, поэтому в статье автором была выдвинута гипотеза о существовании взаимосвязи между информационной безопасностью страны и ее социо-экономико-политическим развитием, что доказывалось с помощью канонического анализа. Для исследования были выбраны данные национального индекса кибербезопасности и факторы социо-экономико-политического развития для 159 стран мира за 2018 год. Построена карта стран мира с указанием национального индекса кибербезопасности. Это позволило сделать предварительный вывод о справедливости выдвинутой гипотезы. Канонический анализ проводился в аналитическом пакете STATISTICA, в результате чего были определены канонические корни, факторная структура, дисперсия и избыточность, канонические веса для факторов, регрессионные уравнения. Результаты анализа подтвердили справедливость гипотезы, что факторы развития обусловливают уровень информационной безопасности и наоборот, уровень безопасности может влиять на развитие страны.

Ключевые слова: канонический анализ, корреляционный анализ, информационная безопасность, национальный индекс кибербезопасности, социо-экономико-политическое развитие, STATISTICA.

CANONICAL ANALYSIS OF RELATIONSHIP BETWEEN INFORMATION SECURITY AND SOCIO-ECONOMIC-POLITICAL DEVELOPMENT OF THE COUNTRY

Summary. One of the drivers of the country's modern development can be its information security. It can help raise the level of economic growth, reduce the risks of losing information for companies and the population, and decrease political and social tension in society. For this reason, the author has hypothesized the existence of a relationship between the information security of the country and its socio-economic and political development. To prove this, the scientist has chosen canonical analysis, which helps to investigate the relationships between two sets of factors. To study, the researcher has selected 12 components of the national cybersecurity index and 37 elements of socio-economic and political development for 159 world countries for 2018. The author has conducted a correlation analysis and chosen those indicators which have had a relationship with a correlation coefficient of more than 0.3. This procedure has reduced the number of development factors to 19. In this work, the researcher has built a map of the world countries, indicating the national cybersecurity index. The visual analysis of the chart has allowed us to make a preliminary conclusion about the validity of the author's hypothesis. At the next stage, the scientist has carried out a canonical analysis in the analytical package STATISTICA. The obtained calculations have made it possible to determine the canonical roots, factor structure, variance and redundancy, canonical weights for factors, regression equations. The analysis results have confirmed the validity of the hypothesis that development factors determine the level of information security and vice versa, the level of protection can affect the development of the country. The obtained data will make it possible to develop a range of strategic measures in those areas where this relationship is closer. To sum up, such strategies will lead to the strengthening of security institutions, the introduction of new methods of protection, which will have a positive effect on political stability in the country, social welfare of the population from cyber fraud, and a decrease in losses to the national economy from illegal use of resources.

Key words: canonical analysis, correlation analysis, information security, national cybersecurity index, socio-economic-political development, STATISTICA.