МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ЯРОВЕНКО ГАННА МИКОЛАЇВНА

УДК 330.5:330.3:004.056(043.3)

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ДРАЙВЕР РОЗВИТКУ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

Спеціальність 08.00.03 – економіка та управління
національним господарством

Автореферат
дисертації на здобуття наукового ступеня
доктора економічних наук

Суми – 2021

Дисертацією є рукопис.
Робота виконана в Сумському державному університеті Міністерства освіти і науки України.

Науковий консультант – докторка економічних наук, професорка *Кузьменко Ольга Віталіївна,* Сумський державний університет Міністерства освіти і науки України, завідувачка кафедри економічної кібернетики.

Офіційні опоненти:

докторка економічних наук, професорка *Затонацька Тетяна Георгіївна,* Київський національний університет імені Тараса Шевченка, професорка кафедри економічної кібернетики;

докторка економічних наук, професорка *Маргасова Вікторія Геннадіївна,* Національний університет «Чернігівська політехніка» Міністерства освіти і науки України, проректорка з наукової роботи;

докторка економічних наук, професорка *Онищенко Світлана Володимирівна*, Національний університет «Полтавська політехніка імені Юрія Кондратюка» Міністерства освіти і науки України, професорка кафедри фінансів, банківського бізнесу та оподаткування.

Захист відбудеться 13 травня 2021 року о 10:00 годині на засіданні спеціалізованої вченої ради Д 55.051.06 у Сумському державному університеті за адресою: 40000, м. Суми, вул. Петропавлівська, 57, зала засідань вченої ради.

З дисертацією можна ознайомитись у бібліотеці Сумського державного університету за адресою: 40007, м. Суми, вул. Римського-Корсакова, 2.

Автореферат розісланий 09 квітня 2021 року.

Учений секретар
спеціалізованої вченої ради
доктор економічних наук, доцент А. О. Бойко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми дослідження. Четверта промислова революція впродовж останнього десятиліття сприяла стрімкому розвитку новітніх інформаційних технологій та цифровізації національної економіки (НЕ). 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 (ІБ) на належному рівні перетворюється у сучасних умовах на один із найважливіших чинників захисту національного фінансово-економічного суверенітету, посилення конкурентоспроможності НЕ на світовому рівні та драйвера розвитку національного господарства.

Обґрунтування ролі та місця ІБ 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 ІБ, методології її оцінювання, визначення її місця в забезпеченні збалансованості розвитку НЕ, ефективності системи її забезпечення, розроблення механізмів її підвищення, тощо. Відсутність системного розуміння ролі ІБ як драйвера розвитку НЕ 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 ІБ 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.) та 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 НЕ 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 НЕ.

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

Поставлена мета зумовила необхідність вирішення таких завдань:

- уточнити змістовну сутність ІБ та сформувати концептуальну модель її забезпечення в системі управління НЕ;
- поглибити структуризацію наукового доробку щодо напрямів дослідження ІБ як драйвера розвитку НЕ;
- сформувати склад показників для оцінювання рівня ІБ НЕ шляхом канонічного аналізу взаємного впливу індикаторів розвитку та інформатизації НЕ;
- розробити методологію інтегрального оцінювання рівня ІБ НЕ;
- розробити методологію аналізу ефективності функціонування системи ІБ НЕ;
- дослідити залежність національних патернів забезпечення ІБ 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 ІБ в Україні;
- поглибити методологію обґрунтування пріоритетів формування державних секторальних і галузевих програм у напрямку забезпечення ІБ НЕ;
- розробити методологію визначення ролі цифрової спроможності та кібербезпеки країни щодо забезпечення збалансованості розвитку НЕ;
- 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 ІБ та здійснення регуляторних інтервенцій щодо підвищення її ефективності.

Предметом дослідження є науково-методологічні засади та методичний інструментарій реалізації державної політики забезпечення ІБ як елемента системи управління НЕ.

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 ІБ та управління НЕ.

Відповідно до визначених завдань використано такі методи дослідження: логічне узагальнення та групування, наукову абстракцію – під час визначення тенденцій розвитку НЕ у світлі формування цифрового суспільства; системний аналіз – при уточненні сутності ІБ та розробленні концепції її забезпечення в системі управління НЕ; динамічний та бібліометричний аналізи – під час дослідження наукового доробку щодо ролі та місця ІБ в економічній системі; кореляційний аналіз – під час обґрунтування впливу ІБ країни на ймовірність її використання в незаконних операціях; канонічний аналіз – під час обґрунтування взаємного впливу показників розвитку НЕ, цифрової спроможності та кібербезпеки країни; кластерний аналіз методом k-means – під час дослідження закономірностей формування в НЕ домінуючих моделей забезпечення персональної ІБ населення; метод побудови карт Кохонена – під час визначення груп країн, близьких за рівнем ІБ НЕ; метод переваг та функція Харрінгтона – Менчера – під час інтегрального оцінювання ІБ НЕ; DEA-аналіз – під час визначення порівняльної ефективності складових системи ІБ НЕ; 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 НЕ; гравітаційне моделювання – при доведенні впливу рівня ІБ на привабливість країн для легалізації кримінальних доходів; BPMN-моделювання – в процесі оптимізації бізнес-процесів забезпечення ІБ; 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 ІБ 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 ІБ з урахуванням її впливу на розвиток НЕ в цілому та її окремих секторів.

Найбільш вагомими науковими результатами дослідження є такі:

вперше:

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

– запропоновано методологію аналізу порівняльної ефективності складових системи забезпечення ІБ НЕ 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 ІБ, 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 НЕ, 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 НЕ, так і за інтегральним рівнем центра мас у моделі, а для України – окреслити напрямки реалізації державної політики для підвищення збалансованості розвитку НЕ;

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 НЕ і кібербез-

пеки, економічного, соціального й фінансового розвитку НЕ, зовнішньо–економічної діяльності, інноваційної активності, якості інформаційної інфраструктури, інституційної спроможності держави. Це дозволило сформувати перелік релевантних індикаторів інтегрального оцінювання ІБ НЕ та визначити пріоритети в реалізації державної політики її підвищення;

– методологічний базис дослідження закономірностей формування в НЕ домінуючих моделей забезпечення персональної ІБ 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 ІБ і наслідків її порушення, які залежать від рівня економічного розвитку країни та історично сформованих суспільних традицій;

– методологію обґрунтування впливу ІБ 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 НЕ та вдосконалення вітчизняної системи державного фінансового моніторингу;

– методологічні засади обґрунтування таргетів та напрямків реформування системи забезпечення ІБ 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 ІБ НЕ;

– методологію обґрунтування пріоритетів формування державних секторальних та галузевих програм у напрямку забезпечення ІБ НЕ, 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 ІБ, додержання якого є економічно доцільним. Це дозволило емпірично встановити, що у фокусі підвищеної державної уваги в разі забезпечення ІБ НЕ 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 НЕ. Це дозволило розробити концепцію забезпечення ІБ в системі управління

НЕ, що формалізує зовнішні та внутрішні загрози як передумови порушення цілісності, конфіденційності й доступності об'єктів ІБ, визначити суб'єкти, засоби і механізми контролю, обґрунтувати системно-структурні взаємозв'язки між наслідками забезпечення ІБ для розвитку НЕ в цілому та окремих її секторів;

– теоретичні основи структуризації наукового доробку щодо напрямів дослідження ІБ як драйвера розвитку НЕ, 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 ІБ;

– 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 ІБ;

– 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 ІБ НЕ; 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 ІБ; 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 ІБ – 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.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У першому розділі **«Теоретичні засади дослідження сутності та ролі інформаційної безпеки в національній економіці»** визначено тенденції розвитку НЕ у світлі формування цифрової економіки, уточнено змістовну сутність ІБ та

концептуальні засади її забезпечення в системі управління НЕ, поглиблено структуризацію наукового доробку щодо напрямів її дослідження.

Дослідження частки ІТ-галузі в структурі НЕ 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.

Результати аналізу наукових напрацювань щодо трактування поняття «інформаційна безпека» дозволили виокремити два їх напрями: 1) характеристика ІБ через її функціональне навантаження, що звужує її розуміння лише як стану, процесу або сфери діяльності, залишаючи поза увагою системний характер; 2) характеристика ІБ через її суб'єктів, що розмежовує дослідження ІБ держави, економічних агентів або індивідів, залишаючи поза увагою багаторівневість та крос-секторність наслідків її порушення. З огляду на виявлені недоліки існуючих підходів запропоновано трактувати ІБ 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 ІБ як складної багатокомпонентної та динамічної системи, що потребує комплексного дослідження з урахуванням суб'єктно-об'єктної специфіки.

Такий підхід дозволив уточнити концептуальні засади забезпечення ІБ в системі управління НЕ (рис. 1). 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 цього 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 НЕ від дій інсайдерів та кібершахраїв, з урахуванням потреби в оптимізації витрат на функціонування системи забезпечення ІБ і стабілізації економічного, політичного й соціального вимірів розвитку НЕ.

Проведене дослідження трендів наукової зацікавленості питаннями ІБ виявило, що починаючи з 1967 р. проблематиці ІБ 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. (рис. 2 а), що обумовлено стрім-

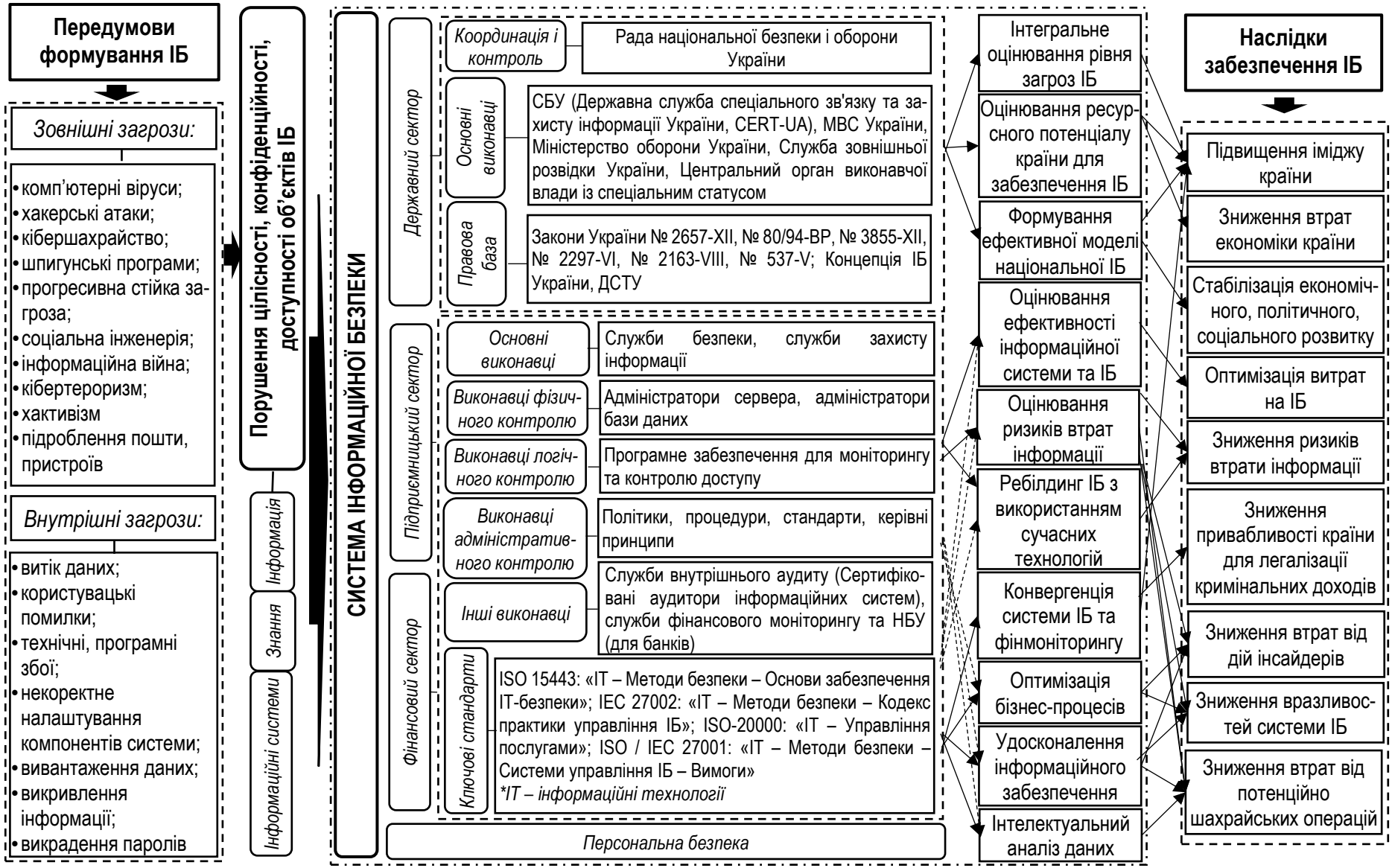
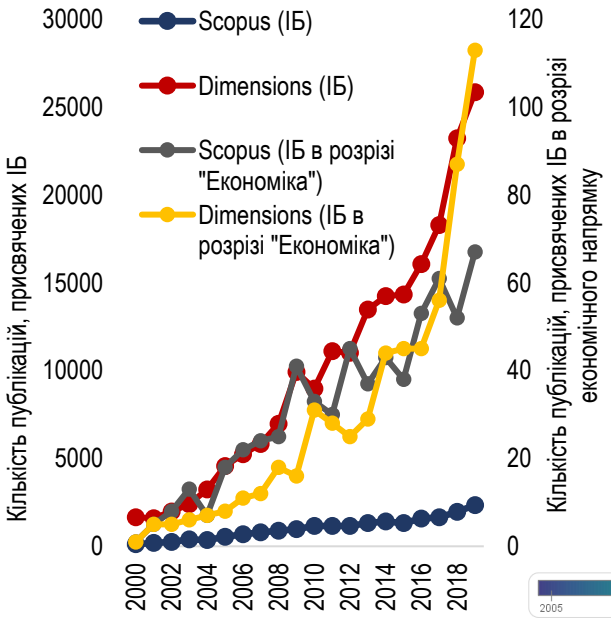
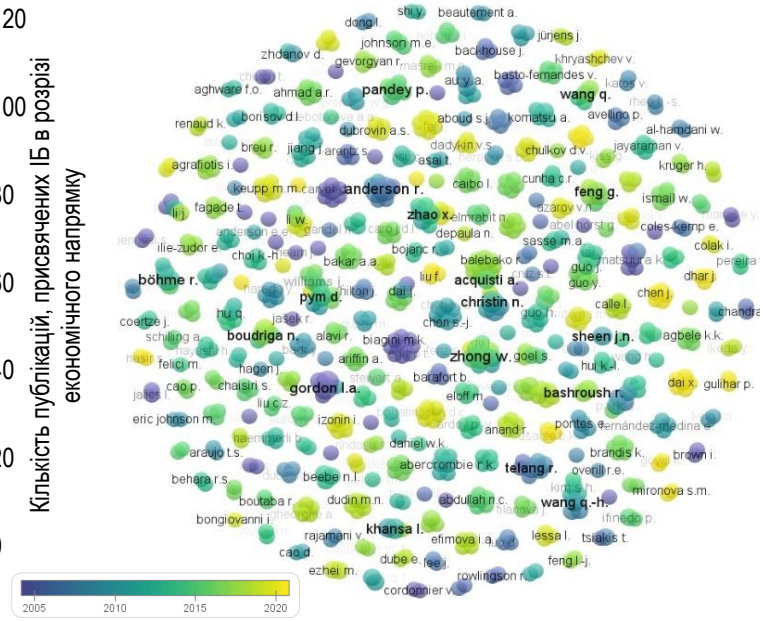


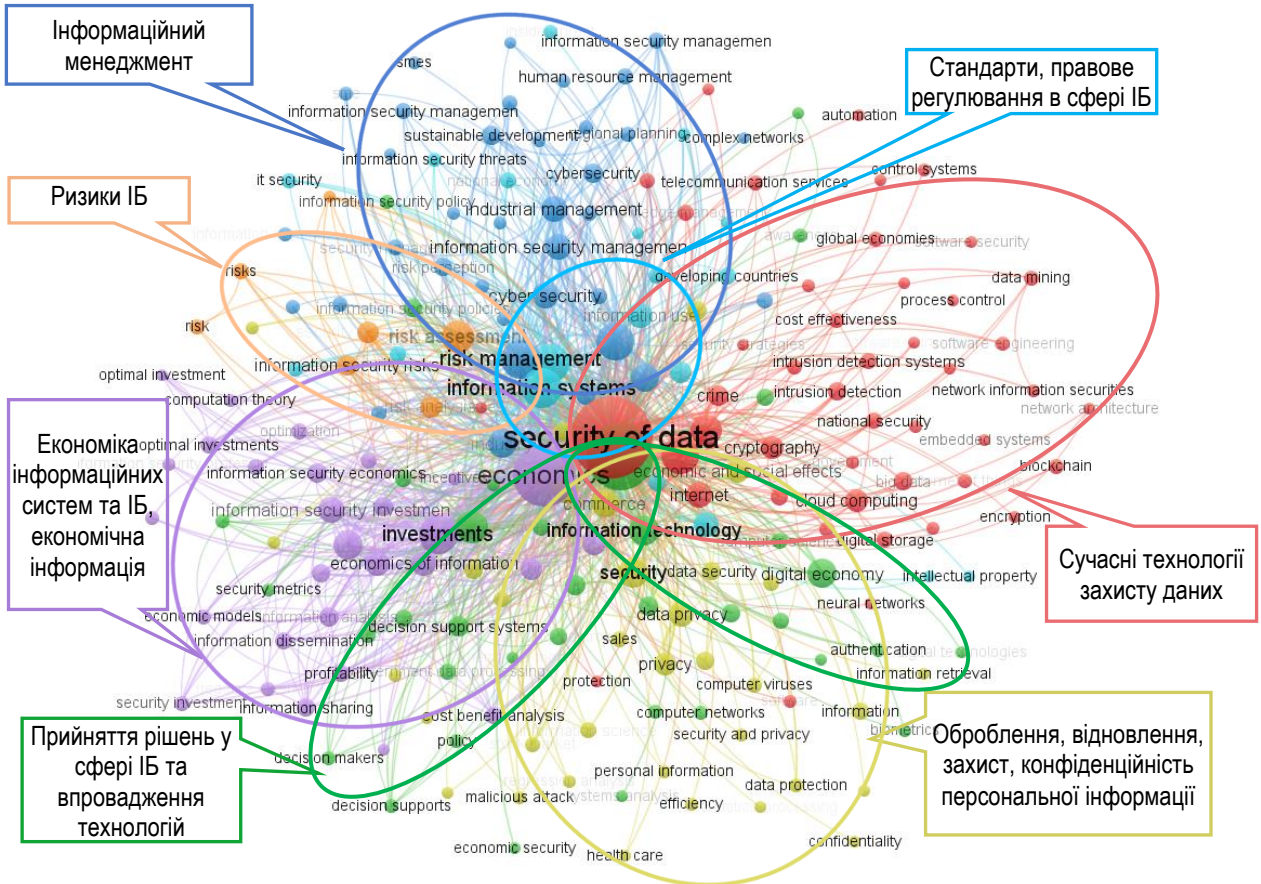
Рисунок 1 – Концептуальна модель забезпечення ІБ в системі управління НЕ



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

кою 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 ІБ у контексті економічного розвитку (рис. 2 б), виявив відсутність домінування окремих наукових шкіл за останні 10 років.

Бібліометричний аналіз ключових слів наукових публікацій, що індексуються наукометричною базою даних Scopus та присвячені проблематиці ІБ як драйвера розвитку НЕ (рис. 2 в), 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 ІБ; 4) ризики ІБ; 5) правове забезпечення ІБ; 6) інформаційний менеджмент. Одержані результати дозволили окреслити пріоритетні для науки та практики завдання, пов’язані з формуванням системи ІБ як драйвера розвитку НЕ.

У другому розділі **«Методологія оцінювання інформаційної безпеки національної економіки та ефективності системи її забезпечення»** за допомогою канонічного аналізу визначено склад індикаторів ІБ НЕ; методом переваг проведене її інтегральне оцінювання; методом кластерного аналізу та DEA-аналізу здійснене оцінювання ефективності системи забезпечення ІБ НЕ.

З метою обґрунтування індикаторів, які повинні бути враховані під час інтегрального оцінювання рівня ІБ країни, сформовано 8 груп показників: цифрової спроможності НЕ і кібербезпеки (5), економічного (9), соціального (4) та фінансового (5) розвитку НЕ, 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. Як засвідчили результати розрахунків (рис. 3 а), найбільш істотний взаємний вплив демонструють група індикаторів інституційної спроможності держави та група показників цифрової спроможності НЕ 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 ІБ країни. Розрахунок канонічних ваг засвідчив, що з цих двох груп індикаторів найбільш вагомими є «Рівень цифрового розвитку» та «Ефективність уряду» (рис. 3 б), що повинно бути враховано під час формування державної політики забезпечення ІБ НЕ.

Для інтегрального оцінювання рівня ІБ НЕ запропоновано використовувати метод переваг, згідно з яким нормалізовані значення п’яти індикаторів групи цифрової спроможності НЕ та кібербезпеки, а також п’яти індикаторів групи інституційної спроможності держави трансформуються за допомогою шкали бажаності (вибір типу кривої перетворення обумовлений характером відмінності факти-

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 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 3 – Результати канонічного аналізу для обґрунтування складу індикаторів рівня ІБ країни

чних значень відповідних показників від нормалізованих). Одержані значення узагальнюються в межах інтегрального індикатора ІБ НЕ за функцією Харрінгтона – Менчера (рис. 4). Розрахунки на даних 159 країн світу за 2018 р. засвідчили, що найвищий рівень ІБ НЕ 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 ІБ НЕ 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 %). Для України обґрунтовані таргети реалізації державної політики в напрямку підвищення ІБ загалом та в розрізі окремих її складових.

У роботі за допомогою системного поєднання методу DEA-аналізу в специфікації CCR (модель Чарнеса, Купера і Родоса оцінки загальної ефективності щодо постійності віддачі від масштабу) із використанням аналітичного пакета Frontier Analyst та кластерного аналізу, реалізованого за допомогою побудови карт Кохонена на платформі Deductor Academic, сформовані 7 кластерів країн (рис. 5 а), які є найбільш близькими за співвідношенням фактичних рівнів складових інтегрального індексу ІБ НЕ. Україна ввійшла до кластеру № 1 разом із

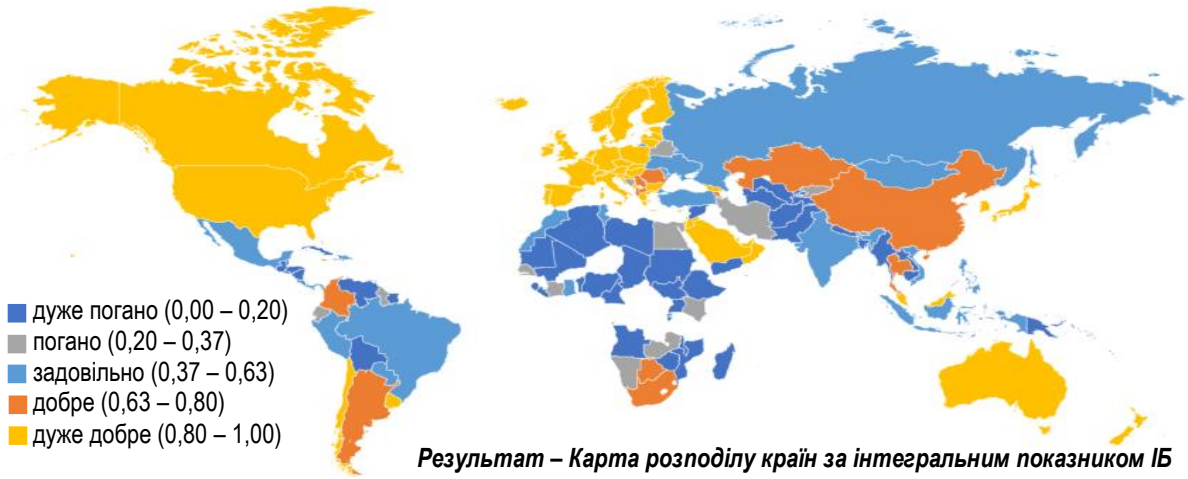
Етап 1: 1) формування бази даних для розрахунку інтегрального показника: 5 індикаторів цифрової спроможності НЕ та кібербезпеки (ЦСіКБ): індекс розвитку інформаційних і комунікаційних технологій (ІР ІКТ); індекс мережевої готовності (ІМГ); глобальний індекс кібербезпеки (ГІК); національний індекс кібербезпеки (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	***За кривою 2-го типу***: НІК. ІМГ
$d_{ij}^{\ *} = \exp(-\exp(-\left(9\left(\frac{Z_{ij}-\min\limits_i Z_{ij}}{\max\limits_i Z_{ij}-\min\limits_i Z_{ij}}\right)^{1.927}-2\right)$, 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})	$d_{ij}^{\ *} = \exp(-\exp(-\left(9\left(\frac{Z_{ij}-\min\limits_i Z_{ij}}{\max\limits_i Z_{ij}-\min\limits_i Z_{ij}}\right)^{k_{II}}-2\right)$, 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



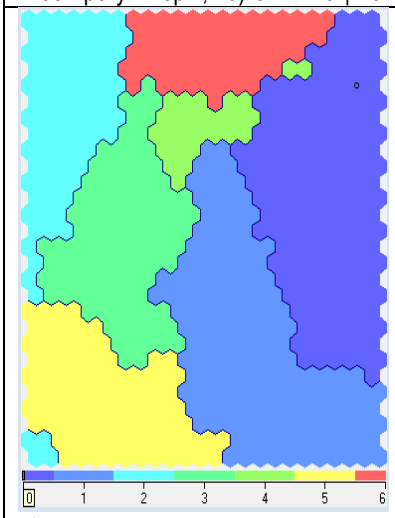
Результат – Карта розподілу країн за інтегральним показником ІБ

Рисунок 4 – Методологія формування та результати оцінювання інтегрального індексу ІБ НЕ

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 ІБ НЕ та визначити відповідні напрямки реалізації державної політики щодо збільшення рівнів цифрової та інституційної спроможності НЕ, а також кібербезпеки (рис. 5 б).

У роботі визначений максимальний рівень ІБ, якого може досягти країна за умови наявного потенціалу, а також приховані резерви для його підвищення.

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

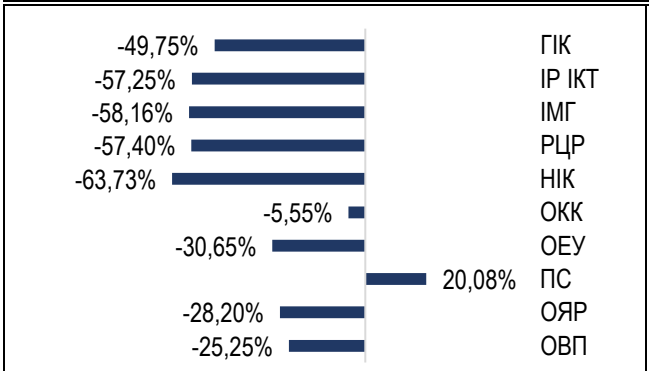
Етап 2. Визначення вагів вхідних показників за методом головних компонентів

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

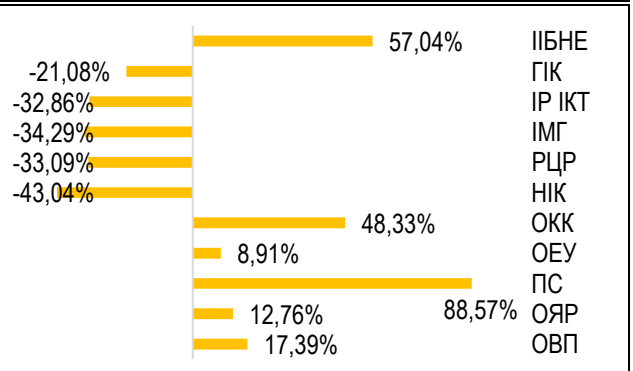
б) результати оцінювання ефективності ІБ НЕ кластерів країн

№*	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 5 – Методологія та результати аналізу ефективності системи забезпечення ІБ НЕ

Так, зокрема, поточна ефективність системи забезпечення ІБ 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 ІБ НЕ – індексу політичної стабільності та відсутності насилля / тероризму (на 20,08 %), що є абсолютно логічним в умовах військово-політичного конфлікту на Сході України (рис. 5 в).

Крім того, розрахунки засвідчили, що за умови застосування відповідних регуляторних інтервенцій інтегральний рівень ІБ 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 % (рис. 5 г). Отже, основні резерви підвищення рівня ІБ в Україні перебувають у площині підвищення якості державного регулювання НЕ.

У третьому розділі **«Причинно-наслідкові зв'язки в дослідженні впливу інформаційної безпеки на розвиток національної економіки»** досліджено вплив економічних факторів на формування національних патернів персональної ІБ, рівня кібербезпеки країни – на її привабливість для легалізації кримінальних доходів, «інформаційних бульбашок» – на функціонування глобального цифрового економічного простору.

У роботі висунуто гіпотезу, що: 1) змістовна наповненість, інтенсивність та ефективність заходів, що реалізуються органами державної влади в різних країнах щодо підвищення рівня цифрової інклюзії населення та його інформаційної грамотності, безпосередньо впливає на обсяги і типи наслідків кіберінцидентів, на які наражається населення цих країн; 2) заходи забезпечення персональної ІБ, 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 ІБ 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.

Розрахунки дозволили підтвердити цю гіпотезу: виділено 7 кластерів країн ЄС за домінуючими заходами персональної ІБ та наслідками її порушення, в яких більшість країн виявилися близькими як за рівнем ВВП на душу населення, так і за географічним розміщенням (рис. 6).

У роботі 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. (рис. 7).

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 6 – Методологія та результати кластерного аналізу країн ЄС за 2019 р. щодо зв'язку заходів персональної ІБ та наслідків кіберінцидентів

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. 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 (рис. 7 а): 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

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)

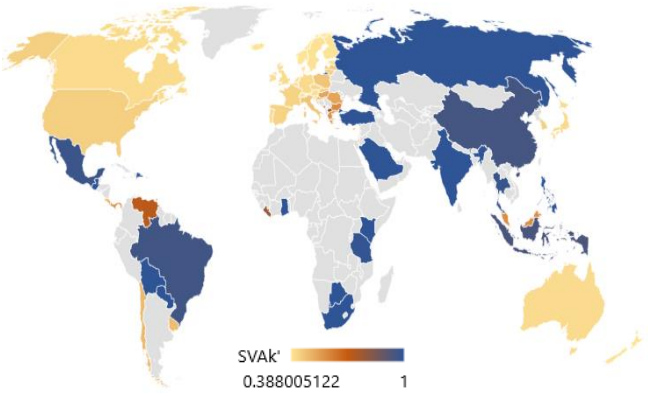
Етап 4. Визначення вагових коефіцієнтів для обраних факторів: а) проведення експертного опитування щодо важливості одного фактору стосовно до іншого з використанням методу аналізу ієрархії в частині отримання вагових коефіцієнтів: $\omega_i = \sum_{i=1}^{m} \omega_i^k / m$, де ω_i – середньоарифметичне 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 7 – Методологія та результати дослідження впливу рівня кібербезпеки країни на її привабливість для операцій із легалізації коштів

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. (рис. 7 б). Одержані результати формують наукове підґрунтя розроблення рекомендацій щодо посилення контролю за операціями, які здійснюють контрагенти визначених країн.

Одним із проявів впливу кіберінцидентів на розвиток НЕ 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 НЕ. Із застосуванням інструментарію Global Web Statistics 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 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» (рис. 8).

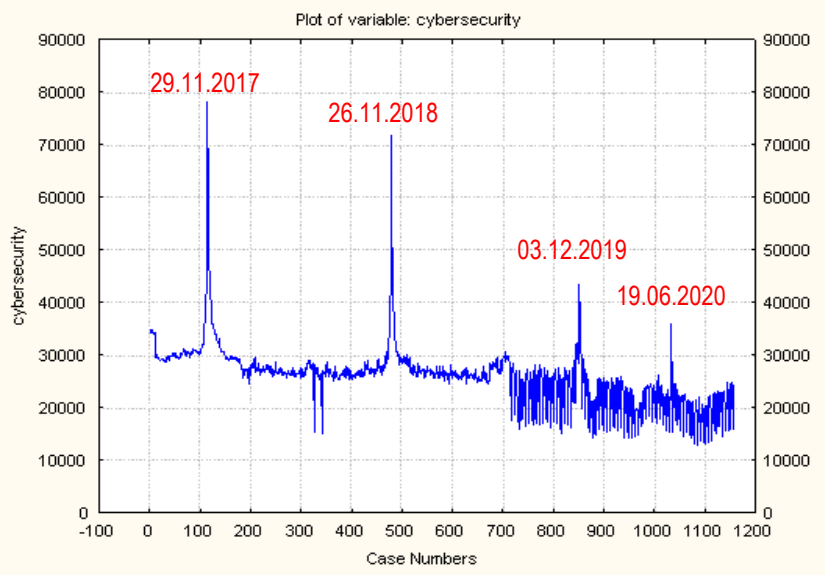


Рисунок 8 – Виявлені періоди розривів «інформаційних бульбашок» у глобальному цифровому економічному просторі з 05.08.2017 до 20.10.2020

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, Excel) визначено, що стабілізація глобального цифрового економічного простору розпочинається після десятого дня від розриву бульбашки.

У четвертому розділі **«Напрямки реалізації державної політики підвищення інформаційної безпеки національної економіки»** вдосконалено методологічні засади обґрунтування таргетів та напрямків реформування системи забезпечення ІБ в Україні; поглиблено методологію обґрунтування пріоритетів формування державних секторальних і галузевих програм у напрямку забезпечення ІБ НЕ; розроблено методологію визначення ролі цифрової спроможності та кібербезпеки країни щодо забезпечення збалансованості розвитку НЕ.

У контексті реформування вітчизняної системи ІБ НЕ важливо встановити таргетовані значення основних параметрів забезпечення кібербезпеки, на досягнення яких повинні бути спрямовані державні регуляторні інтервенції. 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 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 ІБ Естонії, тоді як в Україні лише чотири з 12 параметрів національної системи ІБ відповідають таргетованим значенням, три – на середньому рівні щодо усіх країн із вибірки, а інші п’ять – на критично низькому рівні. На рисунку 9 продемонстровано фрагмент результатів цього дослідження за методом TOPSIS.

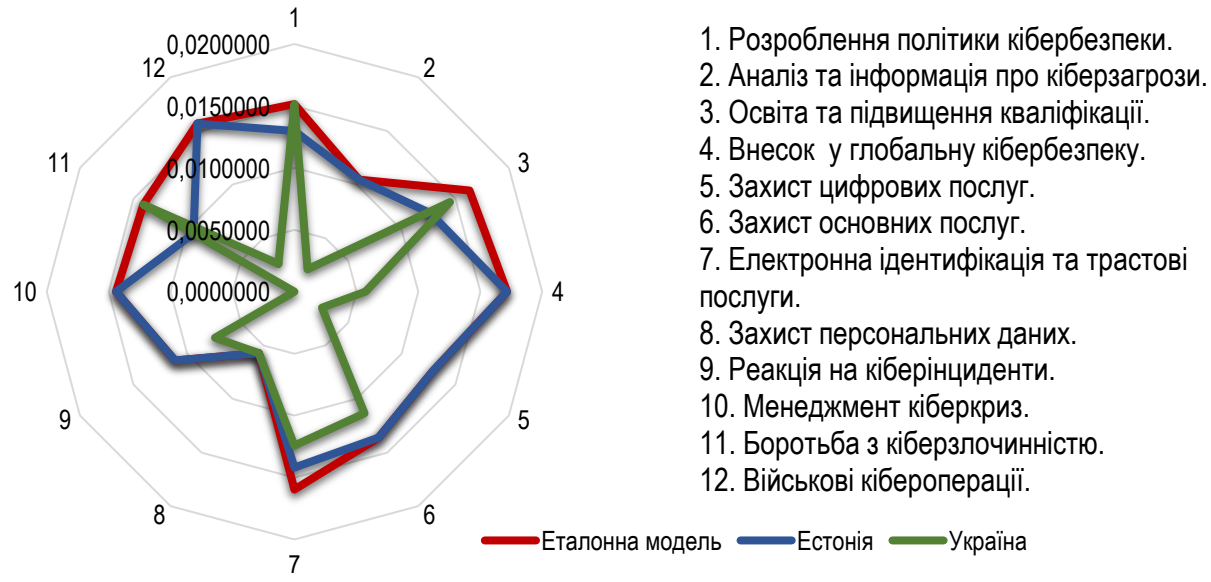


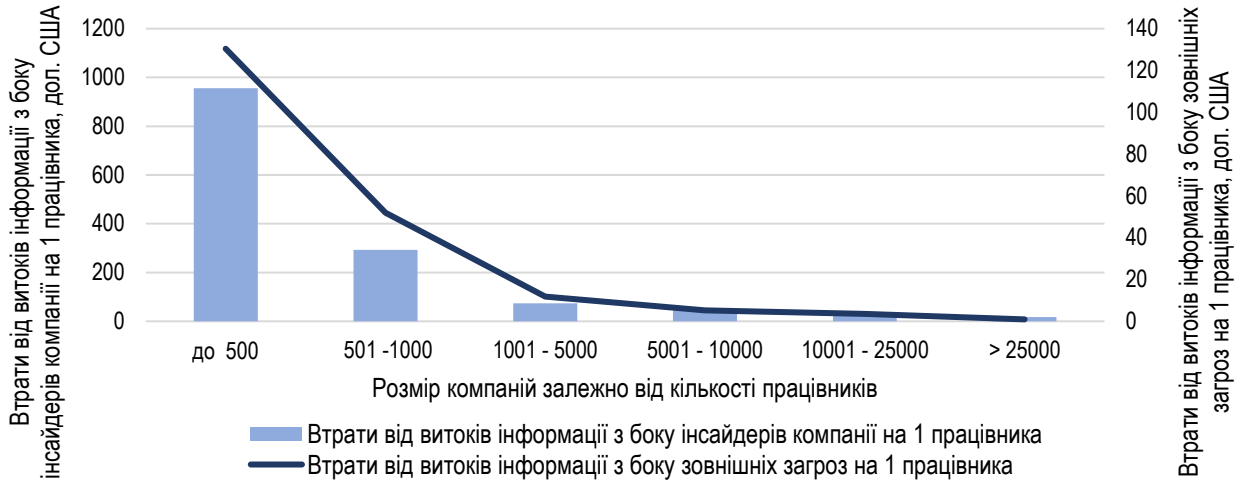
Рисунок 9 – Результати аналізу напрямків реформування національної системи ІБ в Україні (за методом TOPSIS)

На підставі результатів розрахунків обґрунтовано пропозиції щодо ребілдингу національної системи ІБ в Україні в напрямку: розвитку спеціалізованих аналітичних груп з аналізу стану ІБ, активізації участі України в розробленні Конвенції про кіберзлочинність, створення в Україні представництв міжнародних організацій із кібербезпеки, формування спеціалізованих наглядових органів у

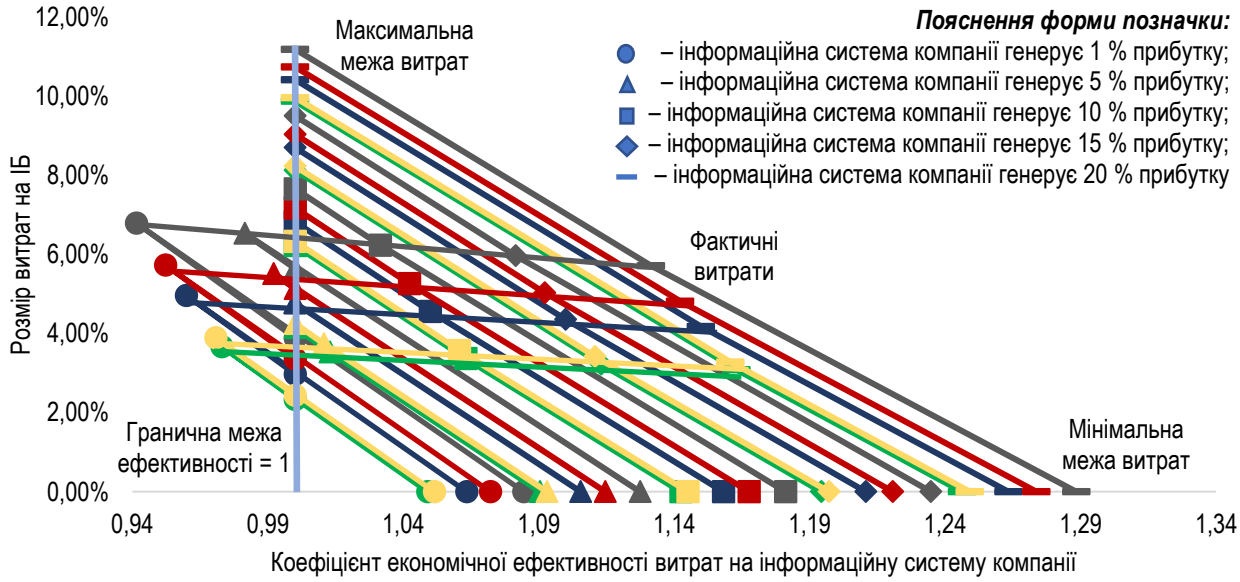
сфері ІБ, розроблення національних стандартів та стратегії ІБ НЕ, формування плану управління кіберкризовими ситуаціями на національному рівні, забезпечення участі України в міжнародних навчаннях щодо реагування на кіберкризи, розроблення заходів щодо здійснення спеціалізованих кібероперацій тощо.

У контексті формування державних програм підвищення рівня ІБ в Україні важливо розуміти, які саме суб'єкти господарювання та якої галузевої належності потребують підвищеної уваги з боку держави в цьому напрямку. З метою вирішення цього завдання 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) (рис. 10 а). Таким чином, у фокусі підвищеної державної уваги повинні перебувати питання підвищення забезпечення рівня ІБ саме цих суб'єктів; 2) на другому етапі визначено галузеву належність малих та середніх підприємств, питання забезпечення рівня ІБ яких повинна особливо ретельно контролювати держава. Розраховано граничні розміри витрат на ІБ цієї групи економічних суб'єктів (безпосередньо витрати на ІБ, на відновлення інформації внаслідок її втрат та погашення збитків) у їх відношенні до прибутків, що генерують інформаційні системи цих компаній за 2020 р. (рис. 10 б). Для компаній різної галузевої належності розраховано максимальну та мінімальну межі витрат на ІБ, забезпечення яких не загрожує втраті фінансової стійкості цих компаній, а також установлено, що найнижчий рівень забезпечення витрат на ІБ 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 ІБ для них, формування системи контролю та моніторингу рівнів їх кібербезпеки, створення центрів сертифікації й підвищення кваліфікації ІТ-аудиторів, співробітників цих компаній тощо.

У роботі досліджено місце цифрової спроможності НЕ і кібербезпеки щодо забезпечення збалансованості розвитку країни поряд з індикаторами економічного, політичного та соціального розвитку. Для цього побудовано чотириполюсну барицентричну модель за методом центра мас, згідно з якою: 1) чим ближче виявиться розрахунковий центр мас побудованого чотирикутника (його вершини – відповідні виміри розвитку НЕ) до еталонного значення, тим більшим є загальний рівень збалансованості НЕ; 2) чим ближче координата композитного індикатора для кожного виміру розвитку НЕ до 1, тим більш розвиненою є країна в цьому напрямку (рис. 11). Базою дослідження стали дані 127 країн світу за 2018 р., інструментарієм – програми MS Excel та GeoGebra. На рисунку 11 а продемонстровано результати розрахунків для п'яти найкращих країн з різних груп за рівнем економічного розвитку: для найбільш економічно розвинених країн



а) втрати компаній від кіберінцидентів на одного працівника в залежності від їх розмірів



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)

б) співвідношення розміру витрат на ІБ та коефіцієнта економічної ефективності витрат на інформаційну систему для підприємств різних галузей із кількістю до 500 осіб

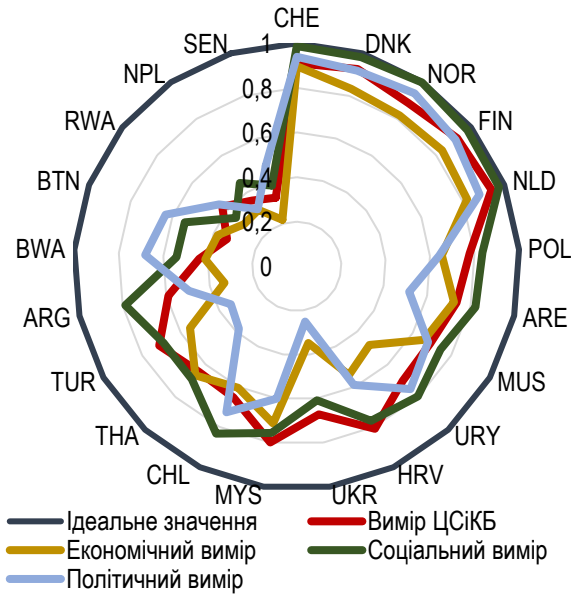
Рисунок 10 – Результати дослідження пріоритетів формування державних секторальних та галузевих програм у напрямку забезпечення ІБ НЕ

значення індикаторів для кожного виміру розвитку НЕ наближається до еталонного, тоді як для групи найменш розвинених країн цей розрив є найбільшим. Найбільш збалансованими країнами (рис. 11 б) виявилися: 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. Як бачимо, високий рівень збалансованості за всіма вимірами розвитку НЕ можуть досягати країни як із високим, так і з низьким рівнем добробуту, що дозволяє їм бути більш стійкими до внутрішніх та зовнішніх загроз.

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.

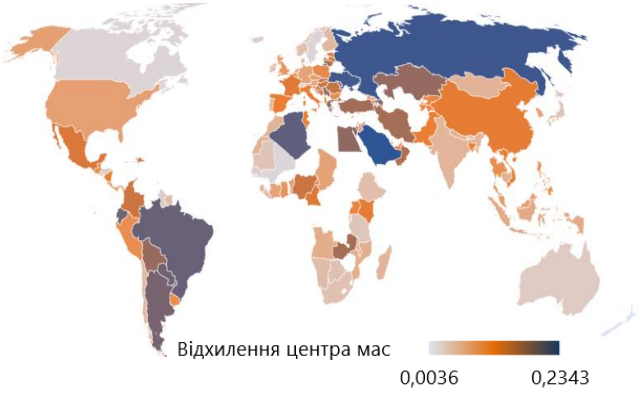
Етап 2. Нормалізація значень факторів за допомогою лінійної нормалізації

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 (відповідає центру мас країни); $(x_b; y_b)$ – координати точки B (відповідає еталонному центру мас з координатами (0;0)); 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 *(* червоний колір відповідає еталонній моделі; чорний – моделі України)*

Рисунок 11 – Методологія та результати оцінювання рівня збалансованості НЕ на основі чотириполюсної барицентричної моделі

Розрахунки для України (рис. 11 в) засвідчили, що її прогрес у напрямку забезпечення цифрової спроможності та кібербезпеки в країні є істотно більш відчутним, ніж щодо економічного, політичного та соціального розвитку, це стало основою обґрунтування напрямків відповідних регуляторних інтервенцій.

У п'ятому розділі **«Розвиток прикладного методичного інструментарію підвищення рівня інформаційної безпеки»** поглиблено методичні засади експрес-оцінювання ризиків втрати інформації, вибору найбільш ефективної системи її захисту, формування системи попередження фінансових кіберзагроз.

У контексті забезпечення ІБ важливим є оцінювання ризиків, що асоціюються з втратою інформації. 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 (рис. 12). 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).

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.

Пріоритетним завданням системи забезпечення ІБ НЕ є розроблення ефективних програмно-технологічних рішень для зменшення витоків інформації, зовнішніх, внутрішніх кіберзагроз. У роботі 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 (рис. 13). 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 ІБ, які оцінювалися за ризиком невиявлення кіберзагроз (рис. 13 а) та рівнем уразливості системи (рис. 13 б), 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

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 кіберзлочинців; *SC* – інциденти, пов'язані з некоректною роботою програмного забезпечення. Для кожної групи обрано набір факторів впливу (66 од.)

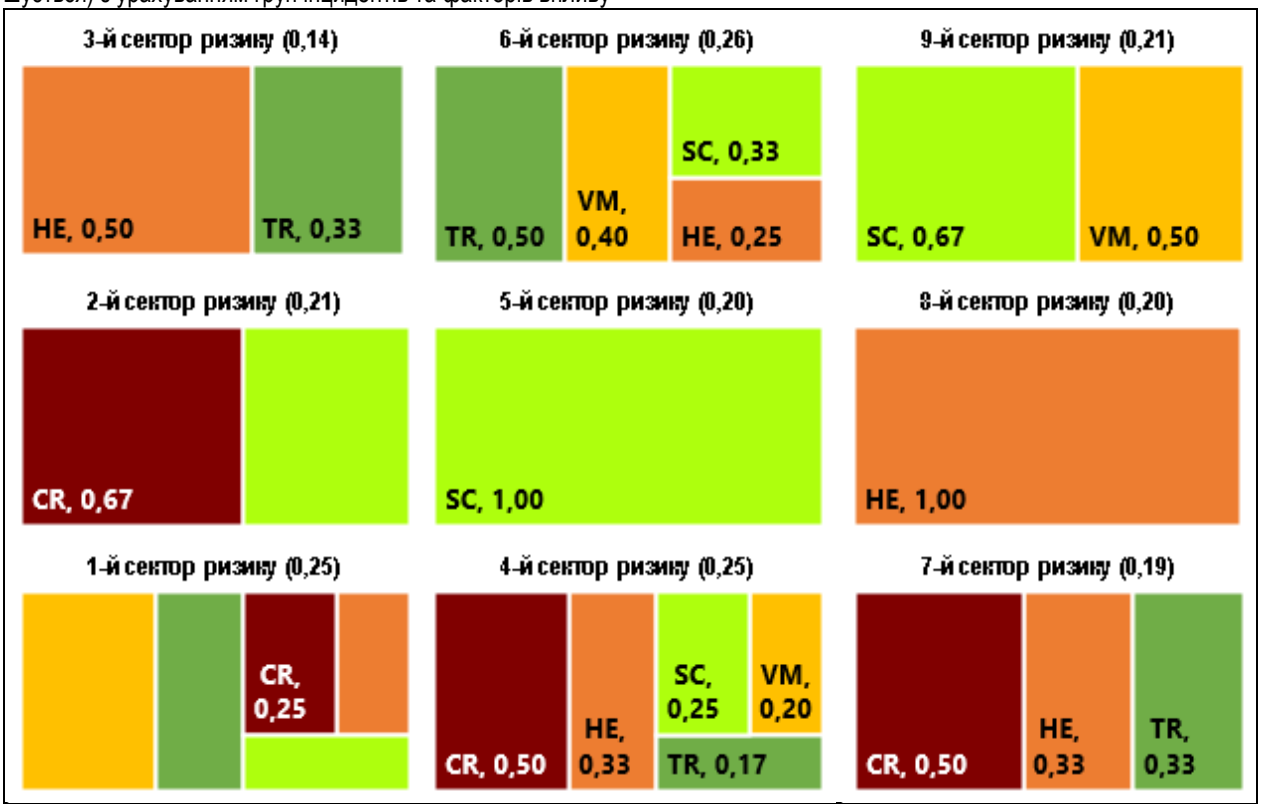
Визначення обсягів грошових втрат для кожного фактору та частоти повторення на основі фактичних даних: ведення статистики інцидентів щодо втрат, пов'язаних із відновленням даних після інциденту, та їх історичної ретроспекції

Формалізація факторів за допомогою бінарних характеристик і теорії множин, визначення загального рівня ризику за кожним із секторів, що відповідають розподілу інформації в карті ризику:

$$R_p = \sum_{i=1}^{k}\left(Z_{pi}|A_{pi} \geq 1 + \left[\frac{1}{n}\sum_{j=1}^{n} a^*_{pij}\right]|A_{pi} \geq 2\right) / \sum_{i=1}^{k}\left(Z_{pi} + \left[\frac{1}{n}\sum_{j=1}^{n} r_{pj}\right]\right),$$

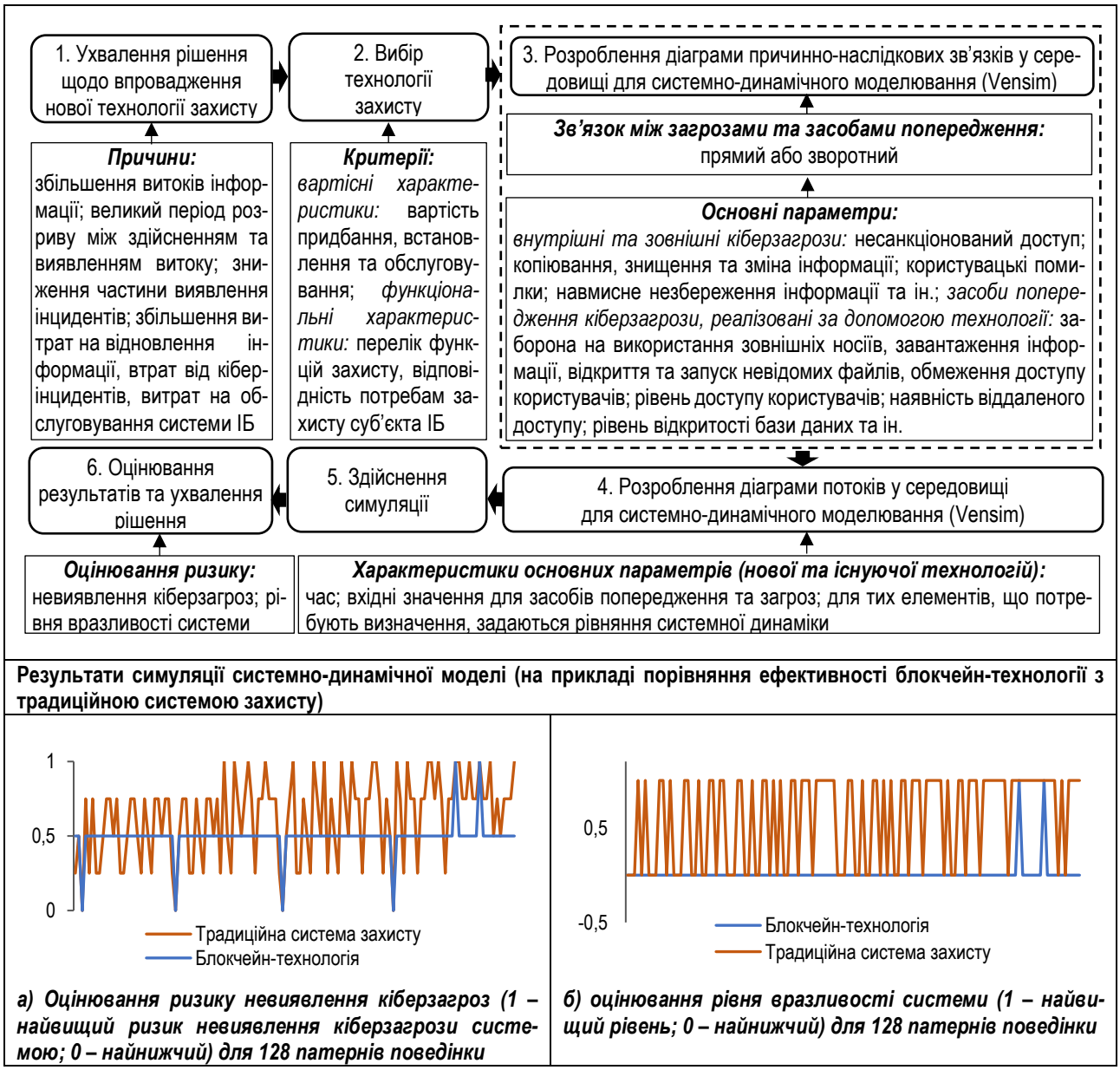
де R_p – загальний рівень ризику за кожним *p*-м сектором (9 секторів карти ризиків); Z_{pi} – базова сукупність значень інцидентів ризику (1 – якщо $A_{pi} > 0$; 0 – якщо $A_{pi} = 0$; A_{pi} – ефект від впливу факторів на інцидент ризику (0 – випадки впливу фактору на *i*-й інцидент ризику (i = 1 ÷ 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 12 – Методичні засади та результати експрес-оцінювання ризиків втрати інформації



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 13 – Методологія та результати системно-динамічного імітаційного моделювання для порівняння систем захисту інформації

відповідно), а також вона дозволяє скоротити рівень уразливості системи на 59,38 %.

Для підвищення ефективності системи забезпечення ІБ НЕ необхідно комплексно вирішувати питання захисту інформації вже на етапі попередження кіберінцидентів. Для вирішення цього завдання запропоновано трирівневу систему попередження кіберзагроз та продемонстровано ефективність її використання у фінансовому секторі НЕ (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 неконтрольо-

ваного витоку інформації або втручання кіберзлочинців. У цьому контексті запропоновано науково-методичний підхід до моделювання та оптимізації бізнес-процесів у системі забезпечення ІБ, що реалізовано шляхом побудови моделей ключових процесів інформаційного захисту в нотації BPMN 2.0 із використанням програмного забезпечення Bizagi Modeller. Запропонований 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. Запропонований підхід 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.

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.

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.

ВИСНОВКИ

У дисертації подано розроблення нових та вдосконалення існуючих методологічних підходів і методичного інструментарію формування ефективної системи ІБ з урахуванням її впливу на розвиток НЕ 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 ІБ, суб'єктно-об'єктну узгодженість її інструментів та механізмів впливу з урахуванням специфіки структури НЕ. У результаті це сприяло формуванню концепції забезпечення ІБ в системі управління НЕ, що визначає передумови формування ІБ, її наслідки, об'єкти, суб'єкти залежно від рівнів НЕ, а також інструменти та механізми її забезпечення.

2. Динамічний аналіз кількості наукових публікацій засвідчив зростання зацікавленості проблематикою ІБ лише за останні 20 років, що підтверджено 97 % обсягу публікацій за період 2000–2019 рр. порівняно з 3 % за період 1967–1999 рр. Дослідження ІБ в розрізі предметних галузей економічного напрямку виявило відсутність домінування окремих наукових шкіл та наявність 7 векторів наукового вивчення проблематики ІБ. Одержані результати дозволили виділити ключові її аспекти, що потребують поглибленого дослідження та вдосконалення для потреб НЕ.

3. Аналіз взаємовпливів між показниками цифрової спроможності НЕ і кібербезпеки та групами індикаторів інституційної спроможності держави, економічного, соціального та фінансового розвитку НЕ, 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 ІБ, а також її потенційних можливостей драйвера для НЕ країни.

4. Запропонований інтегральний індекс ІБ НЕ дозволив сформувати рейтинг країн світу, внаслідок цього було виявлено 5 груп країн, яким відповідають рівні розвитку ІБ НЕ: дуже добре, добре, задовільно, погано, дуже погано. Україна ввійшла до переліку тих країн, рівень ІБ НЕ 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 ІБ.

5. На основі проведеного кластерного аналізу і DEA-аналізу виявлено 7 кластерів країн за інтегральним рівнем їх ІБ НЕ та показниками інституційної та цифрової спроможності й кібербезпеки. У результаті визначено структурну неефективність для кожного кластеру країн, що показало недостатню забезпеченість поточного стану ІБ НЕ для країн 2-го, 4-го та 6-го кластерів, а також структурну неефективність усіх кластерів для досягнення максимального рівня ІБ НЕ. Для України забезпечення системи ІБ НЕ 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 ІБ НЕ на 57,04 %.

6. Проведене дослідження закономірностей формування в НЕ моделей забезпечення персональної ІБ населення дозволило виявити 7 кластерів країн ЄС, сформованих за домінуючими заходами персональної ІБ 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 ІБ.

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 ІБ 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 ІБ.

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. Одер-

жані результати довели існування дестабілізаційних впливів інформаційного середовища на НЕ країни, що сприятиме їх виявленню та попередженню колапсів у різних секторах НЕ.

9. Використані методи багатоатрибутного прийняття рішень дозволили виявити таргети та напрямки реформування системи забезпечення ІБ 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 кіберопераций. Це сприяло розробленню комплексу заходів державної політики забезпечення ІБ НЕ в цьому напрямку.

10. Обґрунтування пріоритетів формування державних секторальних та галузевих програм у напрямку забезпечення ІБ НЕ 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 ІБ, 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 ІБ.

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 НЕ.

12. Запропонована методика експрес-оцінювання ризиків втрат інформації та даних незалежно від суб’єкта ІБ 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 ІБ 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 ІБ дозволила визначити її ефективність за такими параметрами: середнім ризиком невиявлення кіберза-

гроз 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 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 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.).

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, Суми, 2021.

У дисертації уточнено змістовну сутність інформаційної безпеки та сформовано концептуальну модель її забезпечення в системі управління національної економіки; структуровано науковий доробок щодо напрямів дослідження інформаційної безпеки як драйвера розвитку національної економіки; сформовано склад показників для оцінювання її рівня шляхом канонічного аналізу взаємного впливу індикаторів її розвитку та інформатизації; розроблено методологію інтегрального оцінювання рівня інформаційної безпеки національної економіки та аналізу її ефективності; досліджено залежність національних патернів забезпечення інформаційної безпеки населення від рівня економічного розвитку країни та суспільних традицій; обґрунтовано вплив рівня кібербезпеки країни на її привабливість для легалізації кримінальних доходів; визначено часові характеристики впливу «інформаційних бульбашок» на функціонування глобального цифрового економічного простору; удосконалено методологічні засади обґрунтування таргетів та напрямків реформування системи забезпечення інформаційної безпеки в Україні; поглиблено методологію обґрунтування пріоритетів формування державних секторальних та галузевих програм у напрямку її забезпечення; розроблено методологію визначення ролі цифрової спроможності та кібербезпеки країни щодо забезпечення збалансованості розвитку національної економіки; поглиблено методичні засади експрес-оцінювання ризиків втрати інформації; на засадах системно-динамічного імітаційного моделювання поглиблено підхід до вибору найбільш ефективної системи захисту інформації; запропоновано трирівневу систему попередження фінансових кіберзагроз.

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

SUMMARY

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 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.

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 through constructing self-organizing maps was carried out, and the analysis of the comparative effectiveness of the components of the information security system of the national economy using the DEA analysis revealed the structural inefficiency of the sub-indices of the integral index of the 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. Gravity modeling was used to prove that the level of their information security affects the level of attractiveness of countries for money laundering. The results provided a list of countries for which Ukraine is the most attractive in terms of money laundering. This step will improve regulatory policy and promote the convergence of cybersecurity and state financial monitoring systems. The results of modeling information activities using the

Sedova-Taylor model have proven the existence of destabilizing effects of the information environment on the national economy, which will allow timely identification of signs of collapse in its various sectors.

Multiple attribute decision making was 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. 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. The methodology for constructing a four-pole barycentric model 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.

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 developed method of system dynamics modeling 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.

Підписано до друку 02.04.2021.
Формат 60×90/16. Ум. друк. арк. 2,1. Обл.-вид. арк. 1,9. Тираж 100 пр. Зам. No

Видавець і виготовлювач
Сумський державний університет,
вул. Римського–Корсакова, 2, м. Суми, 4007
Свідоцтво суб'єкта видавничої справи ДК № 3062 від 17.12.2007