DOI https://doi.org/10.32405/2522-9931-2022-22(51)-139-160
УДК 330.1:330.3:338.1:004.8:004.9:005.2:005.33

Бойко Олена Володимирівна,
доктор економічних наук, доцент,
професор кафедри маркетингу, фінансів,
банківської справи та страхування ПЗВО
«Східноєвропейський університет імені Рауфа Аблязова».
Черкаси, Україна.
https://orcid.org/0000-0003-0719-8921
lvbojko@yahoo.com

Пушак Ярослав Ярославович,
доктор економічних наук, професор,
професор кафедри соціально-поведінкових,
гуманітарних наук та економічної безпеки Львівського
державного університету внутрішніх справ.
Львів, Україна.
https://orcid.org/0000-0003-1369-8770
yaro_push@yahoo.com

Трушкіна Наталія Валеріївна,
кандидат економічних наук, старший дослідник,
докторант Науково-дослідного центру
індустріальних проблем розвитку НАН України.
Харків, Україна.
https://orcid.org/0000-0002-6741-7738
nata_tru@ukr.net

ФОРМУВАННЯ СУЧАСНОЇ ПАРАДИГМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ: ТЕОРЕТИЧНІ ЗАСАДИ

Анотація. Стрімкий перехід на цифрові технології сприяє прискоренню процесів діджиталізації розвитку екосистеми. Це обумовлено використанням великих баз даних, блокчейну, гібридних (поєднання онлайн і офлайн) форм роботи, формуванням цифрових платформ та національної інформаційної інфраструктури, активізацією електронної комерції тощо. Однак це, у свою чергу, призводить до появи загроз і ризиків інформаційної безпеки, серед яких: відсутність цілісної інформаційної політики держави, витік інформації, використання неліцензійного програмного забезпечення, втрати даних через шпигунські програми, кіберзлочинність (фішинг, формджекінг, криптоджекінг), кібератаки, кібервійни, кібертероризм. Тому у статті теоретично обґрунтовано необхідність формування якісно нової

https://doi.org/10.32405/2522-9931-2022-22(51)

парадигми інформаційної безпеки національної економіки з урахуванням сучасних глобальних викликів і загроз. На підставі методів угруповань і класифікації умовно систематизовано підходи до трактування «інформаційна безпека», які запропоновано різними науковими школами, за такими групами: стан захищеності; сфера діяльності; система гарантій; властивість функціонування; функція держави; суспільні відносини; процес управління загрозами й небезпеками. Запропоновано авторський підхід до формулювання змісту терміна «інформаційна безпека національної економіки», новизна якого полягає у тому, що це визначення базується на комплексному підході і відображає безперервний процес управління інформаційними потоками ресурсів з метою підвищення конкурентоспроможності, забезпечення збалансованого сталого розвитку національної економіки та економічної безпеки держави. Доведено, що з метою формування якісно нової парадигми інформаційної безпеки національної економіки та дієвої її реалізації доцільно розробляти організаційно-економічний механізм, суть якого полягає у сукупності принципів, інструментів, функцій, методів і засобів, спрямованих на зниження рівня кіберризиків, витрат на управління інформаційними потоками і впровадження цифрових технологій і програмного забезпечення. Побудовано структурно-логічну схему формування сучасної парадигми інформаційної безпеки національної економіки України. На підставі аналізу діючого законодавства встановлено, що на даний час не приділено належної уваги забезпеченню інформаційної безпеки у системі національної економіки України в умовах Індустрії 4.0. У зв'язку з цим пропонується внести зміни і доповнення до законів України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», «Про стимулювання розвитку цифрової економіки в Україні»; Стратегії національної безпеки України; Стратегії кібербезпеки України в частині створення належних інституційних умов для забезпечення інформаційної безпеки національної економіки у контексті впровадження технологій Індустрії 4.0. Встановлено, що доцільно розробити й схвалити Концепцію розвитку цифрової економіки та суспільства України на 2023–2027 роки, у якій визначити механізми забезпечення інформаційної безпеки держави у контексті цифрових трансформацій, а також затвердити План заходів щодо її реалізації. Пропонується розробити Стратегію інформаційної безпеки національної економіки України на період до 2035 року в умовах

https://doi.org/10.32405/2522-9931-2022-22(51)

Індустрії 4.0. Подальші напрями дослідження полягають у теоретичному обґрунтуванні та розробленні практичних рекомендацій щодо формування принципово нової концепції економічної безпеки держави як важливої складової стратегії повоєнної розбудови національної економіки України.

Ключові слова: національна економіка; інформаційна безпека; концепція; парадигма; інструментарій; механізми; цифрові технології; ризик-менеджмент; Індустрія 4.0; конкурентоспроможність; сталий розвиток.

ВСТУП / INTRODUCTION

Постановка проблеми. В останні роки спостерігається тенденція зміни парадигми інформаційної безпеки держави у напрямі цифрової трансформації економічних систем. Сучасний етап цифровізації національних економік різних країн світу в умовах Індустрії 4.0 характеризується інтеграцією широкого спектру кіберфізичних систем, великих баз даних, штучного інтелекту, блокчейну, інноваційних і фінансових технологій, інформаційних інфраструктур, цифрових платформ і сервісів тощо.

Фахівці Глобального інституту McKinsey [1] стверджують, що процес розвитку цифрової економіки за масштабами можна порівняти з промисловою революцією XVIII–XIX ст., яка сприяла радикальному перетворенню глобального світу, давши багатьом країнам поштовх до економічного зростання, змінивши саму парадигму їх сталого розвитку. Збільшення частки цифрової або інформаційної економіки та прискорення зростання ВВП за рахунок цифровізації входить до кола пріоритетних проблем глобального масштабу [2, с. 6]. Так, за розрахунками фахівців The Boston Consulting Group, обсяг цифрової економіки до 2035 р. становитиме 16 трлн дол. США.

Згідно з експертним опитуванням 130 генеральних, операційних і технічних директорів компаній-членів Європейської Бізнес Асоціації встановлено, що 47% респондентів оцінили рівень цифрового розвитку свого бізнесу як помірний, а 39% вважають, що він є високим. Однак 9% респондентів стверджують, що рівень цифрової трансформації їхніх компаній є низьким. При цьому переважна більшість (89% опитаних) вказали, що корпоративна стратегія їхньої компанії містить цілі цифрової трансформації.

Отже, цифрова трансформація, яка спостерігається у багатьох галузях національної економіки, призвела до того, що з’явилися нові виклики і ризики інформаційної та кібернетичної безпеки, яким варто приділяти особливу увагу задля підвищення конкурентоспроможності та досягнення збалансованого сталого розвитку.

https://doi.org/10.32405/2522-9931-2022-22(51)

Аналіз останніх актуальних досліджень та публікацій. Як свідчить аналіз, багато наукових джерел присвячено визначенню перспектив, напрямів і механізмів промислового розвитку в умовах смарт-спеціалізації [3], [4], [5] та Індустрії 4.0 [6], а також пошуку шляхів вирішення актуальних проблем цифрової трансформації національної економіки [2], [7]–[10].

З'ясовано, що термін «цифрова трансформація» вперше введено у науковий обіг дослідниками в кінці XX століття, коли цифрові методи управління вийшли за рамки звичайних технологій і почали суттєво змінювати формат бізнесу. Трансформація являє собою процес кардинальних перетворень національної економіки або окремих її елементів у результаті впливу зовнішніх і внутрішніх чинників.

Питання забезпечення економічної безпеки шляхом формування інноваційної інфраструктури з використанням сучасних цифрових технологій та інформаційно-комунікаційних систем розглядаються у роботах багатьох учених-економістів [11]–[18]. Однак за всієї важливості проведених досліджень окремі аспекти формування принципово нової парадигми інформаційної безпеки національної економіки з позицій глобальних трансформаційних перетворень залишаються невирішеними і потребують подальших фундаментальних і прикладних розробок.

МЕТА ТА ЗАВДАННЯ / AIM AND TASKS

Мета даного дослідження полягає у теоретичному обґрунтуванні необхідності формування якісно нової парадигми інформаційної безпеки національної економіки з урахуванням сучасних глобальних викликів і загроз.

Для досягнення поставленої мети визначено такі наукові ***завдання***: узагальнити й систематизувати існуючі наукові підходи до визначення змісту поняття «інформаційна безпека»; надати авторське трактування даної категорії у контексті підвищення конкурентоспроможності та забезпечення сталого розвитку національної економіки; запропонувати сучасну парадигму інформаційної безпеки національної економіки.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ / THE THEORETICAL BACKGROUNDS

Забезпечення збалансованого сталого розвитку національної економіки можливо досягти лише при використанні науково обґрунтованих і чітко сформованих концепцій, які мають базуватися на певній теоретичній основі (гіпотезах, теоріях, інструментарії, методах, прийомах дослідження тощо).

Концепція (від лат. *conceptio* – сприйняття, розуміння, уявлення) розглядається як: 1) система поглядів, понять про ті чи інші явища або

https://doi.org/10.32405/2522-9931-2022-22(51)

процеси, спосіб їхнього розуміння, тлумачення; 2) основна ідея теорії, головний задум; 3) ідея або план нового, оригінального розуміння [19].

У Словнику іншомовних слів концепція трактується як система поглядів на певне явище; спосіб розуміння, тлумачення якихось явищ, основоположна ідея теорії, загальний її задум;

в Академічному тлумачному словнику – як система доказів певного положення, поглядів на те чи інше явище;

в Економічній енциклопедії – як форма і засіб наукового пізнання, що є способом розуміння, пояснення, тлумачення основної ідеї, теорії; науково обґрунтоване і логічно доведене вираження основного змісту теорії, але на відміну від теорії воно ще не може бути втіленим у систему точних наукових понять; система поглядів, помислів, що визначають основний напрям, стратегію і тактику реалізації бізнесово-підприємницьких проєктів, програм (в економіці);

у Фармацевтичній енциклопедії – як система доказів, методів, прийомів дослідження, аналізу, яка базується на певній теоретичній основі; впорядкована система поглядів щодо тих чи інших явищ, фактів, проблем, що потребують розв'язання або пояснення, обґрунтування рішень, результатів досліджень, отриманих під час відповідного спостереження, аналізу.

Варто зазначити, що термін «парадигма» належить до таких спеціальних категорій, без яких сьогодні неможливо уявити будь-яку наукову публікацію. Під парадигмою (від гр. *παράδειγμα* – «приклад», «взірець») у загальному значенні розуміється теоретико-методологічна модель. Це сукупність філософських, загальнотеоретичних основ науки; система понять і уявлень, які властиві певному періодові розвитку науки, культури, цивілізації [20].

Н. Андрейчук [21] пропонує розглядати парадигму як: 1) ідеальний зразок, ідеал, прообраз, прототип, архетип, оригінал; 2) стандартний або типовий приклад, модель; 3) особливий формат наукових досліджень, який відображає ідеологію досліджень, визначає шляхи формування та упорядкування знань і програми досліджень, встановлює критерії оцінювання та інтерпретацію результатів досліджень; 4) модель мислення, узагальнений зразок концептуалізації або теоретичного підходу; 5) теорію (або модель постановки проблем), яку прийнято як зразок розв'язку дослідницької задачі; 6) концепцію, підхід, точку зору (погляд), позицію. При цьому І. Перевозова, А. Сакун [22] стверджують, що поняття «концепція» не слід ототожнювати з більш широким поняттям «парадигма», яке означає систему теоретичних, методологічних та аксіологічних настанов, прийнятих як еталонний зразок формування економічної системи.

https://doi.org/10.32405/2522-9931-2022-22(51)

Як наголошують К. Салига та О. Гуцалюк [23], функціонування корпоративних інтеграційних об'єднань цілком доречно розглядати як сукупність різного роду бізнес-процесів, у рамках будь-якої з наявних парадигм процесного підходу до організації управління. У даному дослідження поняття «парадигма» розглядається з позицій трансформаційних змін інформаційної безпеки національної економіки. Як показує аналіз спеціальної наукової літератури, на даний час не існує єдиного теоретичного підходу до визначення суті інформаційної безпеки. Це, насамперед, обумовлено неоднозначністю і багатоаспектністю даного поняття. Адже цей термін розглядається як об'єкт досліджень з позицій державного управління, економічної [24], фінансової, національної безпеки [25] на різних рівнях, інвестиційного, фінансового і стратегічного менеджменту.

В. Шульга [26] вважає за доцільне виділяти три основні аспекти визначення сутності «інформаційна безпека»: нормативно-правовий, доктринальний, енциклопедичний. Науковець стверджує, що інформаційна безпека являє собою стан інформаційної системи, у якому вона може протистояти впливу внутрішніх і зовнішніх ризиків, не ініціюючи їхнє виникнення для елементів системи й зовнішнього середовища. У. Ільницька [27] наголошує, що відсутня норма, яка б містила дефініцію поняття «інформаційна безпека», враховуючи різницю між поняттями інформаційної безпеки та безпеки інформації. Дослідницею запропоновано розглядати поняття «інформаційна безпека» як стан захищеності систем обробки та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення.

Г. Яровенко [28] виділяє два напрями до визначення інформаційної безпеки. Перший стосується підходів, які визначають інформаційну безпеку, виходячи з її властивостей функціонування, як стану, процесу та сфери діяльності. Перший підхід пов'язує інформаційну безпеку із станом захищеності, що не зовсім вірно, оскільки вона забезпечує його, використовуючи різні засоби. Тобто подібні визначення роблять акцент на мету функціонування інформаційної безпеки. Другий підхід передбачає те, що інформаційна безпека є процесом, який включає застосування різного роду програмних, технічних, правових, інформаційних та організаційних інструментів для забезпечення функціонування її основної мети. Також некоректним буде вважати інформаційну безпеку тільки процесом, тобто послідовністю виконання дій щодо захисту, оскільки вона може

https://doi.org/10.32405/2522-9931-2022-22(51)

передбачати реалізацію ряду взаємопов'язаних процесів, спрямованих на виявлення та попередження загроз. Третій підхід є досить широким, оскільки наголошує, що інформаційна безпека є мультидисциплінарною сферою. Хоча можна погодитися із тим, що вона є саме сферою діяльності, але такий підхід робить її тільки певним різновидом надання послуг. Тобто існуючі поняття тільки відображають один аспект інформаційної безпеки, пов'язаний з її функціонуванням, та не розкривають інші, які є досить важливими для розуміння її сутності. Оскільки наслідки інформаційних загроз, попередження яких є головною задачею інформаційної безпеки, є суттєвими для суспільства, то не погоджуємося із такими трактуваннями в повній мірі, оскільки вони знижують цінність інформаційної безпеки для суспільства. Другий напрям відображає підходи, які акцентують увагу на суб'єктах інформаційної безпеки, які її забезпечують, а саме держави, економічних агентів, особистості. У даному випадку акцент робиться тільки на тому, хто впроваджує її, регулює та використовує. Також дані поняття не враховують спільні риси безпеки для різних суб'єктів, які дозволяють використовувати загальні підходи та інструменти у процесі організації захисту інформації. Все це обмежує розуміння даного поняття тільки на рівні окремого суб'єкта або окремої сфери [28]. На підставі узагальнення позицій науковців щодо тлумачення феномену «інформаційна безпека» виокремлено його сутнісні характеристики, а саме: це стан захищеності інформаційного простору; стан захищеності національних інтересів України в інформаційному середовищі; захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі; суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства і держави від реальних та потенційних загроз в інформаційному просторі; невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки [29].

Виходячи з вищевикладеного можна зазначити, що здебільшого дослідники (Y. Cherdantseva, J. Hilton, С. Антонова, О. Барановський, Л. Бєсєдіна, В. Богуш, І. Боднар, Ю. Гарічев, А. Гаркуша, Я. Жарков, В. Желіховський, З. Живко, М. Зубок, У. Ільницька, Р. Калюжний, І. Керницький, Б. Кормич, В. Ліпкан, Ю. Максименко, І. Маркіна, Г. Мартинюк, А. Марущак, Т. Микитенко, В. Ортинський, І. Панарін, В. Петрик, І. Петровська, П. Рогов, В. Шульга, Г. Яровенко та інші) під поняттям «інформаційна безпека» розуміють стан, сферу діяльності, систему гарантій, властивість функціонування, здатність, функцію держави, суспільні відносини, процес управління загрозами й небезпеками тощо.

https://doi.org/10.32405/2522-9931-2022-22(51)

У наукових джерелах цей концепт, як правило, визначається як: 1) пріоритетна функція держави; 2) стан правових норм і відповідних їм інститутів безпеки; 3) сукупність засобів забезпечення інформаційного суверенітету держави; 4) стан захищеності; 5) інтегрована складова національної безпеки; 6) складова частина економічної безпеки; 7) стан інформаційної роботи суб'єктів підприємництва; 8) стан правових норм і відповідних їм інститутів безпеки; 9) законодавче формування державної інформаційної політики; 10) створення і впровадження безпечних інформаційних технологій; 11) багатоаспектна система з позицій системного підходу; 12) мультидисциплінарна сфера.

Отже, на підставі узагальнення концептуальних положень щодо даної проблематики термін «інформаційна безпека» пропонується розглядати з двох позицій, як:

- ключовий елемент економічної безпеки на рівні держави;
- важливий чинник підвищення конкурентоспроможності, інвестиційної привабливості та досягнення збалансованого сталого розвитку національної економіки.

МЕТОДИ ДОСЛІДЖЕННЯ / RESEARCH METHODS

Для досягнення поставленої мети і визначених наукових завдань використано такі загальнонаукові методи дослідження: аналізу та синтезу; порівняння та класифікації; експертного опитування; системного підходу; структурно-логічного узагальнення.

Дослідження «Рекордний оптимізм всупереч новим викликам», яке проведено у 2018 р. PwC, дозволило встановити, що одним з найактуальніших питань для бізнесу стала кібербезпека. І якщо у 2017 р. лише 62% керівників найбільших компаній світу були стурбовані з цього приводу, то у 2018 р. значення даного показника зросло до 80%. За прогнозними розрахунками Cybersecurity Ventures, збитки від кібератак через використання здирницького та шкідливого програмного забезпечення становитимуть у найближчі роки 11,5 млрд дол. США.

За даними Ponemon Institute, 75% опитаних IT-фахівців визнали, що ризик злому через третіх осіб небезпечний і зростатиме. У ході обстеження, проведеного компанією Soha Systems, доведено, що 63% усіх випадків витоку даних можуть бути прямо або опосередковано пов'язані з атаками третіх осіб. Міжнародне дослідження з проблем інформаційної безпеки (Global Information Security Survey, GISS), яке проведено консалтинговою компанією Ernst&Young, показало, що у 2021 р. 77% респондентів у світі повідомили про зростання кількості серйозних

https://doi.org/10.32405/2522-9931-2022-22(51)

кібератак (у 2020 р. – 59%). І лише 9% опитаних впевнені у тому, що існуючі в їхній компанії заходи з мінімізації кіберризиків здатні захистити її від серйозних кібератак (порівняно з 20% у 2020 р.). При цьому виявлено, що незважаючи на зростаючу загрозу кібератак, бюджет на кібербезпеку вкрай малий відносно загальних витрат на застосування інформаційно-комунікаційних технологій.

Згідно з опитуванням українських підприємств у ході Всесвітнього дослідження економічних злочинів та шахрайства, яке в 2020 р. проведено компанією PwC, виявлено, що 31% респондентів стикається з кіберзлочинами. За даними Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України у період з 7 вересня по 6 грудня 2020 р. зафіксовано понад 22 млн кіберінцидентів. Загальний рівень загроз інформаційної та кібернетичної безпеки становить 58%. Глобальне дослідження «Довіра до цифрових технологій 2021», яке проведено компанією PwC, демонструє зростання рівня ризиків кібератак на бізнес у світі приблизно на 24%. При цьому в Україні тільки 20% підприємців розглядають кібербезпеку як сучасну необхідність, готові коригувати стратегію забезпечення інформаційної безпеки у зв'язку з пандемією COVID і вкладати для її реалізації певні інвестиційні ресурси. За результатами опитування 600 топ-менеджерів великих міжнародних компаній, проведеного Deloitte у рамках дослідження «Майбутнє кіберпростору в 2021 році», виявлено, що 69% респондентів відмічають значне зростання кіберзагроз і ризиків для їхнього бізнесу з початку 2020 року. Майже 75% респондентів, які мали дохід понад 30 млрд дол. США, заявили, що витрачатимуть на кібербезпеку понад 100 млн дол. США. Global Information Security Survey показало, що виручка компаній складала у 2021 р. приблизно 11 млрд дол. США. Тоді як щорічні витрати на інформаційну безпеку становили у середньому лише 5,28 млн дол. США. Виявлено, що 56% представників компаній із недостатнім бюджетом відмічають про перегляд вимог до кібербезпеки. А 44% заявили, що вони були змушені скоротити витрати та зосередитися на своїй старій архітектурі та інформаційній системі. При цьому 39% респондентів зазначили, що витрати на кібербезпеку не враховуються належним чином у вартості стратегічних інвестицій, пов'язаних з цифровою трансформацією ланцюгів постачання. 36% опитаних вважають, що можуть зіткнутися із серйозним порушенням інформаційної безпеки, якого можна уникнути, якщо компанія збільшить обсяг інвестицій у засоби кіберзахисту. У Звіті «Погляд керівників бізнесу в Україні 2021», який підготовлено KPMG в Україні, до ключових ризиків діяльності компаній в умовах невизначеності віднесено кіберзагрози. Лише 58% організацій у

https://doi.org/10.32405/2522-9931-2022-22(51)

світі та 49% в Україні заявили, що вони добре підготовлені до кібератак. Керівництво компаній визнають важливість співпраці та адаптивного підходу до трансформацій – 54% керівників в Україні та 70% у світі відмічають, що нові партнерства матимуть вирішальне значення для зростання темпів цифрових перетворень. Як зазначено у Звіті Центру кібербезпеки Всесвітнього економічного форуму (WEF) «Глобальні перспективи кібербезпеки до 2022 року», 81% опитаних визнають цифрову трансформацію ключовим чинником підвищення кіберстійкості шляхом зміцнення політик, процесів і стандартів із залученням третіх сторін. 84% опитаних стверджують, що кіберстійкість вважається пріоритетом бізнесу в їхній організації за підтримки керівництва. Проте 68% респондентів розглядають кіберстійкість як основну частину загального управління ризиками.

Усе це підтверджує актуальність досліджень з проблем забезпечення інформаційної безпеки національної економіки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ / RESULTS OF THE RESEARCH

На сьогоднішній день правові засади розвитку системи інформаційної безпеки регулюються такими законодавчими й нормативно-правовими документами: Закон України від 21.06.2018 р. № 2469-VIII «Про національну безпеку України»; Указ Президента України від 14.09.2020 р. № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»; Указ Президента України від 26.08.2021 р. № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» тощо. Разом з тим, незважаючи на деякі позитивні законодавчі ініціативи щодо створення системи інформаційної безпеки як пріоритету забезпечення національної безпеки та сталого розвитку національної економіки України, все ж таки існують певні проблеми недостатньо ефективного нормативно-правового забезпечення у цьому напрямі. Наприклад, більшість нормативних документів не кореспондуються один з одним. У деяких з них лише йдеться про інформаційну безпеку в системі національної безпеки. Але не прописано загальних засад, належних інституційних умов і не визначено спеціальних режимів і відповідних механізмів нормативно-правового, організаційно-економічного і фінансового забезпечення функціонування системи інформаційної безпеки з позицій цифрової трансформації національної економіки. На даний момент не розроблено законопроєкт «Про інформаційну безпеку України», Стратегію інформаційної безпеки України та Концепцію інформаційної безпеки України.

https://doi.org/10.32405/2522-9931-2022-22(51)

Хоча були деякі спроби розроблення останніх двох програмних документів. Однак вони так і залишилися недоопрацьованими і незатвердженими проєктами. Тому ці питання потребують особливої уваги з боку освітян, науковців, представників державних органів влади і бізнес-середовища. І це варто робити лише при їхній спільній взаємодії.

З метою формування якісно нової парадигми інформаційної безпеки національної економіки та дієвої її реалізації доцільно розробити організаційно-економічний механізм, суть якого полягає у сукупності принципів, інструментів, функцій, методів і засобів, спрямованих на зниження рівня кіберризиків, витрат на управління інформаційними потоками і впровадження цифрових технологій і програмного забезпечення (рис. 1).

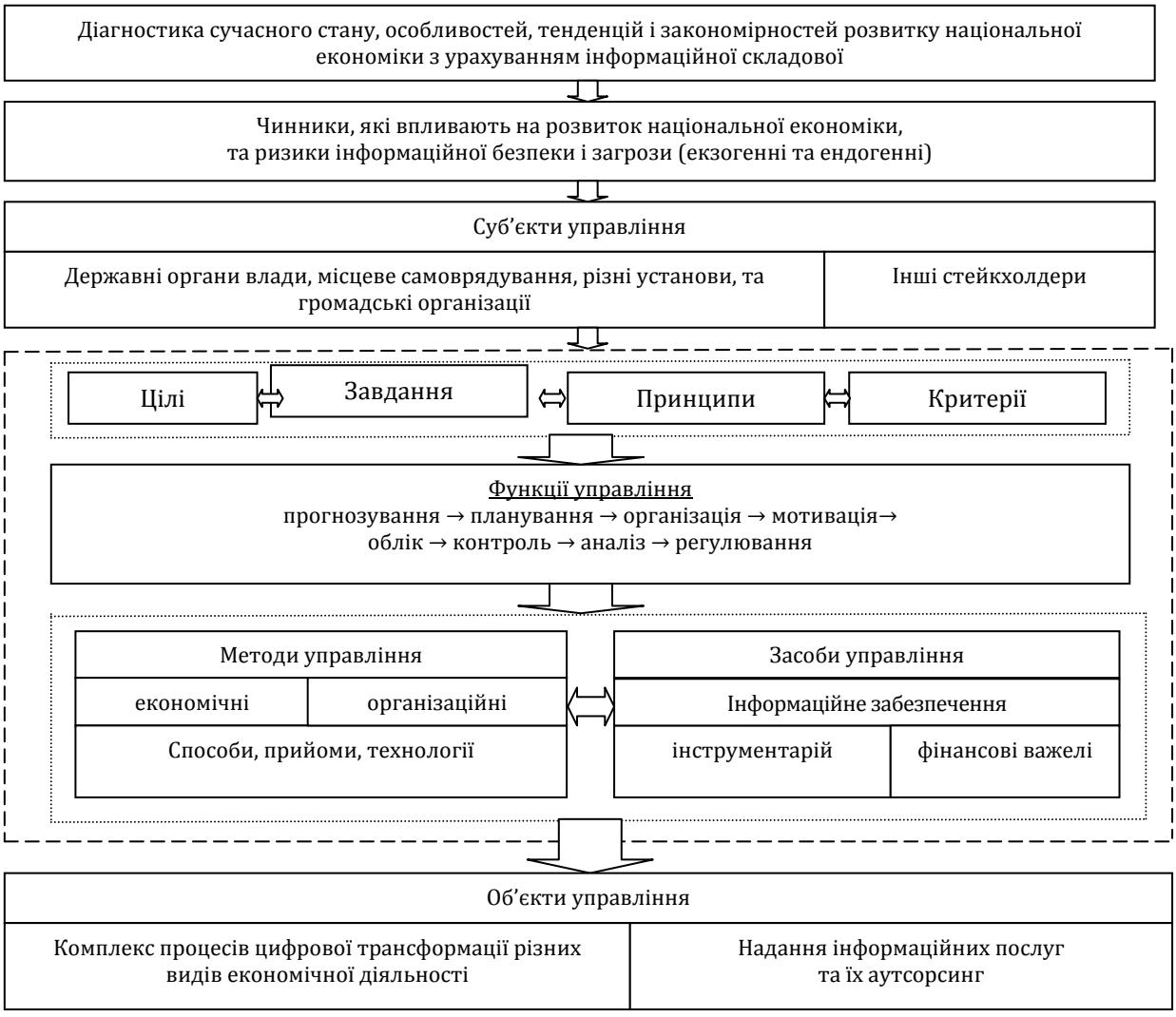

Рис. 1 Основні елементи організаційно-економічного механізму реалізації парадигми інформаційної безпеки національної економіки

Джерело: авторська розробка

https://doi.org/10.32405/2522-9931-2022-22(51)

До складових парадигми інформаційної безпеки національної економіки (рис. 2) належать ресурси; чинники впливу; цілі, принципи, функції, методи, важелі управління; цифрові технології та інформаційні системи; фінансові інструменти фінансування (краудсорсинг, краудфандинг, гранти європейських і міжнародних фінансових організацій, технічна допомога міжнародних фінансових організацій, фінансові ресурси інвестиційних фондів тощо); механізми публічно-приватного партнерства; критерії ефективності.

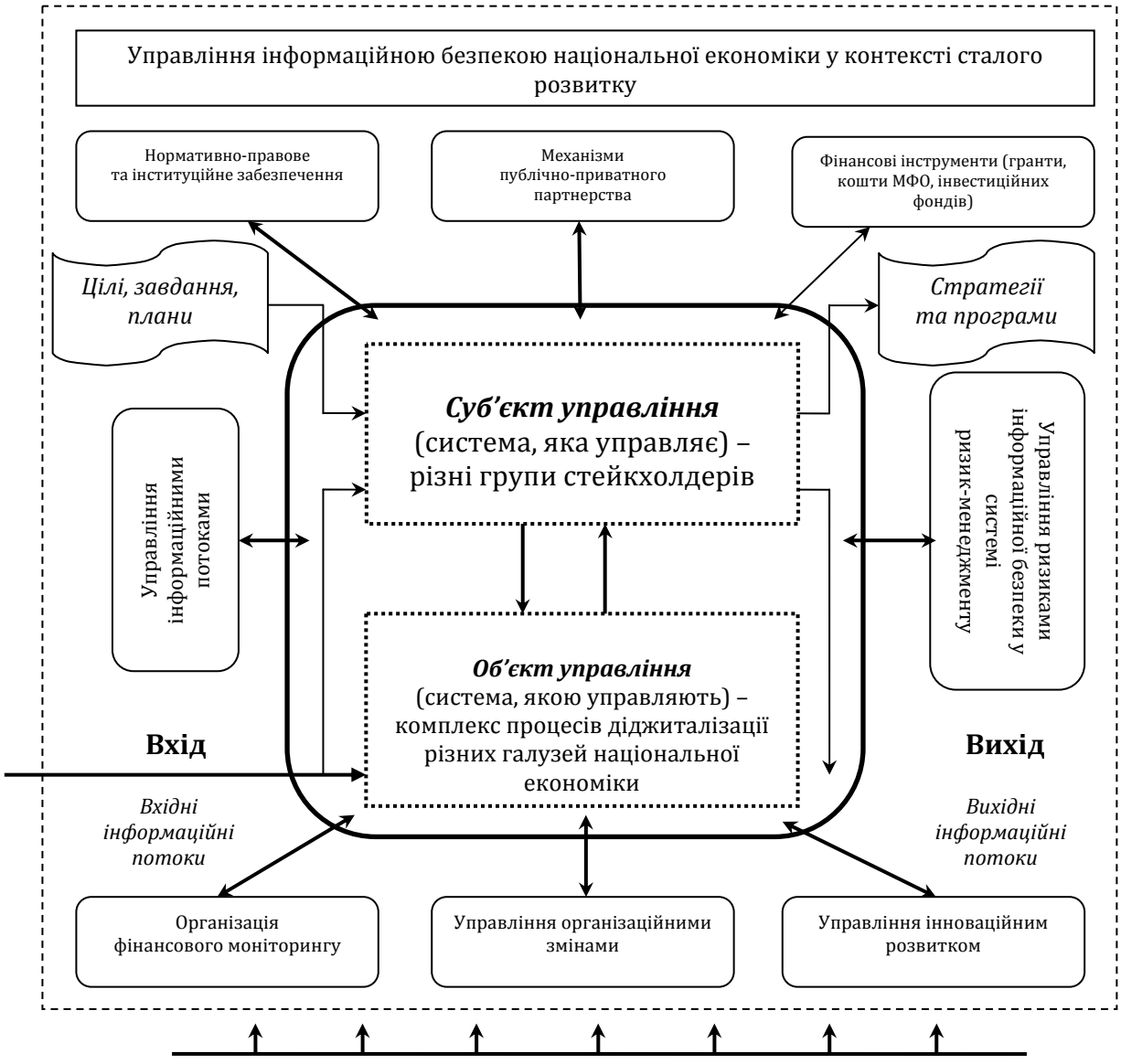

Рис. 2 Структурно-логічна схема формування сучасної парадигми інформаційної безпеки національної економіки України
Джерело: авторська розробка

https://doi.org/10.32405/2522-9931-2022-22(51)

До ключових принципів формування парадигми можна віднести системність, узгодженість, інтегрованість, надійність, комплексність, структурованість, наявність зв'язків, ієрархічність, емерджентність, складність, цілісність, синергійність (прояв синергічного ефекту), гнучкість, динамічність, адаптивність, націленість на комплексну ефективність.

Для мінімізації негативних наслідків від випадків кіберзлочинності та шахрайства необхідно приділяти увагу:

- нівелюванню ризиків інформаційної безпеки;
- удосконаленню законодавства з інформаційної безпеки держави;
- застосуванню відповідного методологічного інструментарію;
- діагностиці і здійсненню постійного фінансового моніторингу [30];
- створенню національної моделі цифрового середовища;
- формуванню інформаційної інфраструктури;
- впровадженню комплексу заходів і відповідних механізмів нормативно-правового, інституційного, фінансового, організаційно-економічного забезпечення інформаційної безпеки національної економіки;
- реалізації національної стратегії кібербезпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ / CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

Отже, виходячи з вищевикладеного, можна дійти висновку, що у законодавстві не приділяється належної уваги забезпеченню інформаційної безпеки у системі національної економіки в умовах Індустрії 4.0. Однак з точки зору перспективності й результативності Індустрію 4.0 варто вважати ключовим етапом цифрової трансформації національної економіки України та екосистем різного рівня. Тому нагальним питанням залишається визначення на законодавчому рівні термінів «Індустрія 4.0», «цифрова трансформація», «інформаційна безпека», «економічна безпека держави в умовах Індустрії 4.0».

Загальні положення про інформаційну безпеку держави необхідно включити у закони України «Про основні засади забезпечення кібербезпеки України», «Про стимулювання розвитку цифрової економіки в Україні»; Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»; Розпорядження Кабінету Міністрів України «Деякі питання цифрової трансформації» і «Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації».

На даний час доцільно внести зміни й доповнення до законів України «Про національну безпеку України», «Про основні засади забезпечення

кібербезпеки України», «Про стимулювання розвитку цифрової економіки в Україні»; Стратегії національної безпеки України; Стратегії кібербезпеки України в частині створення належних інституційних умов для забезпечення інформаційної безпеки національної економіки у контексті впровадження технологій Індустрії 4.0.

Необхідно розробити й схвалити Концепцію розвитку цифрової економіки та суспільства України на 2023–2027 роки, у якій визначити механізми забезпечення інформаційної безпеки національної економіки у контексті цифрових трансформацій, а також затвердити План заходів щодо її реалізації. Крім цього, пропонується розробити Стратегію інформаційної безпеки національної економіки України на період до 2035 року в умовах Індустрії 4.0.

Перспективи подальших досліджень. У подальших дослідженнях планується науково обґрунтувати та розробити практичні рекомендації щодо формування принципово нової концепції економічної безпеки держави як важливої складової стратегії повоєнної розбудови національної економіки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] M. Boden, C. Cagnin, V. Carabias, K. Haegeman, and T. Könnölä, «Facing the future: time for the EU to meet global challenges», *Luxembourg: Publications Office of the European Union*, 2010. [Online]. Available: https://is.gd/kczLT4 Дата звернення: Серп. 21, 2022.

[2] В. І. Ляшенко, та О. С. Вишневський, *Цифрова модернізація економіки України як можливість проривного розвитку*. Київ, Україна: Ін-т економіки промисловості НАН України, 2018.

[3] В. П. Вишневський та ін., *Смарт-промисловість в епоху цифрової економіки: перспективи, напрями і механізми розвитку*. Київ, Україна: НАН України; Ін-т екон. пром., 2018.

[4] В. П. Вишневський, та С. І. Князєв, «Як підвищити готовність промисловості України до смарт-трансформацій», *Наука та інновації*, т. 14, № 4, с. 55–69, 2018. https://doi.org/10.15407/scin14.04.055

[5] O. Amosha, O. Lyakh, M. Soldak, and D. Cherevatskyi, «Institutional determinants of implementation of the smart specialization concept: case for old industrial coal-mining regions in Ukraine», *Journal of European Economy*, vol. 17, no. 3(665), pp. 305–332, 2018. https://doi.org/10.35774/jee2018.03.305

[6] О. І. Амоша та ін., «Індустрія 4.0: напрямки залучення інвестицій з урахуванням інтересів вітчизняних виробників», *Економічний вісник*

Донбасу, № 3(57), с. 189–216, 2019. https://doi.org/10.12958/1817-3772-2019-3(57)-189-216

[7] N. Trushkina, «Development of the information economy under the conditions of global economic transformations: features, factors and prospects», *Virtual Economics*, vol. 2, no. 4, pp. 7–25, 2019. https://doi.org/10.34021/ve.2019.02.04(1)

[8] O. Zybareva, I. Kravchuk, Ya. Pushak, L. Verbivska, and O. Makeieva, «Economic and Legal Aspects of the Network Readiness of the Enterprises in Ukraine in the Context of Business Improving», *Estudios de Economia Aplicada*, vol. 39(5), pp. 1–19, 2021. https://doi.org/10.25115/eea.v39i5.4972

[9] S. Kryshtanovych, O. Prosovych, Y. Panas, N. Trushkina, and V. Omelchenko, «Features of the Socio-Economic Development of the Countries of the World under the influence of the Digital Economy and COVID-19», *International Journal of Computer Science and Network Security*, vol. 22, no. 1, pp. 9–14, 2022. https://doi.org/10.22937/IJCSNS.2022.22.2.2

[10] M. Bezpartochnyi, D. Revenko, H. Dolha, and N. Trushkina, «Model Tools for Diagnosing the Stability and Survivability of Economic Systems», in *Distributed Sensing and Intelligent Systems. Studies in Distributed Intelligence*, M. Elhoseny, X. Yuan, and Sd. Krit, Eds. Switzerland, Cham: Springer, 2022, pp. 275–288. https://doi.org/10.1007/978-3-030-64258-7_25

[11] О. М. Гуцалюк, О. І. Головіна, та В. А. Козловцева, «Формування інноваційної інфраструктури національної економіки в умовах глобалізації та інтеграції», *Інфраструктура ринку*, № 33, с. 381–487, 2019.

[12] С. Шкарлет, та І. Садчикова, «Трансформація системи фінансово-економічної безпеки підприємства в умовах цифрової економіки», *Проблеми і перспективи економіки та управління*, № 3(19), с. 264–276, 2019. https://doi.org/10.25140/2411-5215-2019-3(19)-264-276

[13] О. А. Паршина, Ю. І. Паршин, та Ю. В. Савченко, «Економічна безпека в умовах діджиталізації: сучасний стан та перспективи розвитку інформаційного суспільства», *Науковий вісник Дніпропетровського держ. ун-ту внутрішніх справ*, № 2, с. 167–174, 2019. https://doi.org/10.31733/2078-3566-2019-3-167-174

[14] О. В. Сталінська, «Система економічної безпеки підприємства в умовах розвитку ціфрової економіки», *Науковий вісник Міжнародного гуманітарного ун-ту. Серія: Економіка і менеджмент*, вип. 38, с. 80–86, 2019.

[15] В. Й. Бакай, «Забезпечення економічної безпеки підприємства на основі використання цифрових технологій», *Вісник Хмельницького нац. ун-ту*, т. 1, № 4, с. 32–35, 2020. https://doi.org/10.31891/2307-5740-2020-284-4-5

[16] Ю. Г. Нєустроєв, Т. І. Єгорова-Гудкова, та В. В. Острянко, «Аналіз впливу цифровізації економіки на систему економічної безпеки держави», *Вчені записки Університету «КРОК»*, № 4(60), с. 202–209, 2020. https://doi.org/10.31732/2663-2209-2020-60-202-209

[17] Н. В. Касьянова, Н. М. Кравчук, та Ю. Л. Коваль, «Безпека підприємства в умовах цифрової трансформації економіки», *Modern Economics*, № 20, с. 124–129, 2020. https://doi.org/10.31521/modecon.V20(2020)-20

[18] М. І. Чепелюк, *Інструментарій стратегічного управління в контексті сучасних концепцій та трендів світового економічного розвитку*. Харків, Україна: ФОП Лібуркіна Л. М., 2021.

[19] В. А. Рижко, «Концепція», *Енциклопедія Сучасної України*, І. М. Дзюба, А. І. Жуковський, М. Г. Железняк та ін., Ред. Київ, Україна: Ін-т енциклопед. дослід. НАН України, 2014. [Електронний ресурс]. Доступно: https://is.gd/hB9hpJ Дата звернення: Лип. 26, 2022.

[20] С. П. Бибик, та Г. М. Сюта, *Словник іншомовних слів: тлумачення, словотворення та слововживання*. Харків, Україна: Фоліо, 2006.

[21] Н. Андрейчук, «Парадигма як термін», *Вісник Львівської політехніки*, вип. 52(3), 2008. [Електронний ресурс]. Доступно: https://is.gd/6xfhW7 Дата звернення: Серп. 17, 2022.

[22] І. В. Перевозова, та А. Ж. Сакун, «Логістична концепція виробничо-промислового підприємства», *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*, вип. 14, ч. 2, с. 58–64, 2017.

[23] К. С. Салига, та О. М. Гуцалюк, «Ресурсно-компетентністна парадигма організації управління корпоративними інтеграційними процесами акціонерних товариств», *Бізнес Інформ*, № 10, с. 369–376, 2018.

[24] A. Kwilinski, K. Pajak, O. Halachenko, S. Vasylchak, Y. Pushak, P. Kuzior, «Marketing tools for improving enterprise performance in the context of social and economic security of the state: innovative approaches to assessment», *Marketing and Management of Innovations*, iss. 4, pp. 172–181, 2019.

[25] М. Ф. Криштанович, Я. Я. Пушак, М. І. Флейчук, та В. І. Франчук, *Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення*. Львів, Україна: Сполом, 2020.

[26] В. І. Шульга, «Сучасні підходи до трактування поняття інформаційна безпека», *Ефективна економіка*, № 4, 2015. [Електронний ресурс]. Доступно: https://is.gd/Q5KuZI Дата звернення: Серп. 24, 2022.

[27] У. Ільницька, «Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-

психологічним впливам», Вісник НУ «Львівська політехніка». Серія: *Політичні науки*, вип. 2, № 1, с. 27–32, 2016.

[28] Г. М. Яровенко, «Системний підхід до формалізації поняття «інформаційна безпека», *Причорноморські економічні студії*, вип. 34, с. 239–244, 2018.

[29] С. Є. Антонова, та Г. Ф. Мартинюк, «Інформаційна безпека», *Державне управління: удосконалення та розвиток,* № 11, 2019. [Електронний ресурс]. Доступно: https://is.gd/GbxMXm Дата звернення: Серп. 24, 2022.

[30] Я. Я. Пушак, та Н. В. Трушкіна, «Сутність поняття "фінансовий моніторинг" у контексті забезпечення національної безпеки», *Вісник економічної науки України*, № 2(41), с. 197–203, 2021. https://doi.org/10.37405/1729-7206.2021.2(41).197-203

FORMATION OF THE MODERN PARADIGM OF INFORMATION SECURITY OF THE NATIONAL ECONOMY: THEORETICAL BASIS

Olena Boiko,
Doctor of Economic Sciences, Associate Professor,
Professor of the Department of Marketing,
Finance, Banking and Insurance,
Rauf Ablyazov East European University.
Cherkasy, Ukraine.
https://orcid.org/0000-0003-0719-8921
lvbojko@yahoo.com

Yaroslav Pushak,
Doctor of Economic Sciences, Professor,
Professor of the Department of Social-behavioral Sciences,
Humanities and Economic Security,
Lviv State University of Internal Affairs.
Lviv, Ukraine.
https://orcid.org/0000-0003-1369-8770
yaro_push@yahoo.com

Nataliia Trushkina,
Ph.D. in Economics, Senior Researcher,
Doctoral Student, Research Centre of Industrial
Problems of Development of the NAS of Ukraine.
Kharkiv, Ukraine.
https://orcid.org/0000-0002-6741-7738
nata_tru@ukr.net

https://doi.org/10.32405/2522-9931-2022-22(51)

Abstract. The rapid transition to digital technologies contributes to the acceleration of the processes of digitization of the development of the ecosystem. This is due to the use of large databases, blockchain, hybrid (combination of online and offline) forms of work, the formation of digital platforms and national information infrastructure, the activation of electronic commerce, etc. However, this, in turn, leads to the appearance of information security threats and risks, including the absence of a comprehensive state information policy, information leakage, use of unlicensed software, data loss due to spyware, cybercrime (phishing, form jacking, cryptojacking), cyberattacks, cyber wars, cyber terrorism. Therefore, the article theoretically substantiates the need for the formation of a qualitatively new paradigm of information security of the national economy, taking into account modern global challenges and threats. On the basis of methods of grouping and classification, the approaches to the interpretation of "information security" proposed by various scientific schools are conditionally systematized, according to the following groups: the state of security; field of activity; guarantee system; the property of functioning; function of the state; public relations; threat and danger management process. An author's approach to formulating the meaning of the term "information security of the national economy" is proposed, the novelty of which is that this definition is based on a comprehensive approach and reflects the continuous process of managing information flows of resources with the aim of increasing competitiveness, ensuring balanced sustainable development of the national economy and economic security of the state. It has been proven that in order to form a qualitatively new paradigm of information security of the national economy and its effective implementation, it is advisable to develop an organizational and economic mechanism, the essence of which is a set of principles, tools, functions, methods and means aimed at reducing the level of cyber risks, costs of managing information flows and implementation of digital technologies and software. A structural and logical diagram of the formation of a modern paradigm of information security in the national economy of Ukraine has been built. On the basis of the analysis of the current legislation, it was established that at the moment, due attention has not been paid to ensuring information security in the system of the national economy of Ukraine under the conditions of Industry 4.0. In this regard, it is proposed to introduce changes and additions to the laws of Ukraine "On the national security of Ukraine", "On the basic principles of ensuring cyber security of Ukraine", "On stimulating

the development of the digital economy in Ukraine"; National security strategies of Ukraine; Cybersecurity strategies of Ukraine in terms of creating appropriate institutional conditions to ensure information security of the national economy in the context of the implementation of Industry 4.0 technologies. It has been established that it is expedient to develop and approve the Concept of the Development of the Digital Economy and Society of Ukraine for 2023-2027, in which to define the mechanisms for ensuring the information security of the state in the context of digital transformations, as well as to approve the Action Plan for its implementation. It is proposed to develop the Information Security Strategy for the national economy of Ukraine for the period up to 2035 under the conditions of Industry 4.0. Further directions of research consist in the theoretical substantiation and development of practical recommendations for the formation of a fundamentally new concept of economic security of the state as an important component of the strategy of the post-war development of the national economy of Ukraine.

Keywords: national economy; informational security; concept; paradigm; tools; mechanisms; digital technologies; risk management; Industry 4.0; competitiveness; sustainability.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] M. Boden, C. Cagnin, V. Carabias, K. Haegeman, and T. Könnölä, «Facing the future: time for the EU to meet global challenges», Luxembourg: Publications Office of the European Union, 2010. [Online]. Available: https://is.gd/kczLT4 Data zvernennia: Serp. 21, 2022.

[2] V. I. Liashenko, ta O. S. Vyshnevskyi, Tsyfrova modernizatsiia ekonomiky Ukrainy yak mozhlyvist proryvnoho rozvytku. Kyiv, Ukraina: In-t ekonomiky promyslovosti NAN Ukrainy, 2018.

[3] V. P. Vyshnevskyi ta in., Smart-promyslovist v epokhu tsyfrovoi ekonomiky: perspektyvy, napriamy i mekhanizmy rozvytku. Kyiv, Ukraina: NAN Ukrainy; In-t ekon. prom., 2018.

[4] V. P. Vyshnevskyi, ta S. I. Kniaziev, «Iak pidvyshchyty hotovnist promyslovosti Ukrainy do smart-transformatsii», Nauka ta innovatsii, t. 14, № 4, s. 55–69, 2018. https://doi.org/10.15407/scin14.04.055

[5] O. Amosha, O. Lyakh, M. Soldak, and D. Cherevatskyi, «Institutional determinants of implementation of the smart specialization concept: case for old industrial coal-mining regions in Ukraine», Journal of European Economy, vol. 17, no. 3(665), pp. 305–332, 2018. https://doi.org/10.35774/jee2018.03.305

[6] O. I. Amosha ta in., «Industriia 4.0: napriamky zaluchennia investytsii z urakhuvanniam interesiv vitchyznianykh vyrobnykiv», Ekonomichnyi visnyk Donbasu, № 3(57), s. 189–216, 2019. https://doi.org/10.12958/1817-3772-2019-3(57)-189-216

[7] N. Trushkina, «Development of the information economy under the conditions of global economic transformations: features, factors and prospects», Virtual Economics, vol. 2, no. 4, pp. 7–25, 2019. https://doi.org/10.34021/ve.2019.02.04(1)

[8] O. Zybareva, I. Kravchuk, Ya. Pushak, L. Verbivska, and O. Makeieva, «Economic and Legal Aspects of the Network Readiness of the Enterprises in Ukraine in the Context of Business Improving», Estudios de Economia Aplicada, vol. 39(5), pp. 1–19, 2021. https://doi.org/10.25115/eea.v39i5.4972

[9] S. Kryshtanovych, O. Prosovych, Y. Panas, N. Trushkina, and V. Omelchenko, «Features of the Socio-Economic Development of the Countries of the World under the influence of the Digital Economy and COVID-19», International Journal of Computer Science and Network Security, vol. 22, no. 1, pp. 9–14, 2022. https://doi.org/10.22937/IJCSNS.2022.22.2.2

[10] M. Bezpartochnyi, D. Revenko, H. Dolha, and N. Trushkina, «Model Tools for Diagnosing the Stability and Survivability of Economic Systems», in Distributed Sensing and Intelligent Systems. Studies in Distributed Intelligence, M. Elhoseny, X. Yuan, and Sd. Krit, Eds. Switzerland, Cham: Springer, 2022, pp. 275–288. https://doi.org/10.1007/978-3-030-64258-7_25

[11] O. M. Hutsaliuk, O. I. Holovina, ta V. A. Kozlovtseva, «Formuvannia innovatsiinoi infrastruktury natsionalnoi ekonomiky v umovakh hlobalizatsii ta intehratsii», Infrastruktura rynku, № 33, s. 381–487, 2019.

[12] S. Shkarlet, ta I. Sadchykova, «Transformatsiia systemy finansovo-ekonomichnoi bezpeky pidpryiemstva v umovakh tsyfrovoi ekonomiky», Problemy i perspektyvy ekonomiky ta upravlinnia, № 3(19), s. 264–276, 2019. https://doi.org/10.25140/2411-5215-2019-3(19)-264-276

[13] O. A. Parshyna, Yu. I. Parshyn, ta Yu. V. Savchenko, «Ekonomichna bezpeka v umovakh didzhytalizatsii: suchasnyi stan ta perspektyvy rozvytku informatsiinoho suspilstva», Naukovyi visnyk Dnipropetrovskoho derzh. un-tu vnutrishnikh sprav, № 2, s. 167–174, 2019. https://doi.org/10.31733/2078-3566-2019-3-167-174

[14] O. V. Stalinska, «Systema ekonomichnoi bezpeky pidpryiemstva v umovakh rozvytku tsifrovoi ekonomiky», Naukovyi visnyk

Mizhnarodnoho humanitarnoho un-tu. Seriia: Ekonomika i menedzhment, vyp. 38, s. 80–86, 2019.

[15] V. Y. Bakai, «Zabezpechennia ekonomichnoi bezpeky pidpryiemstva na osnovi vykorystannia tsyfrovykh tekhnolohii», Visnyk Khmelnytskoho nats. un-tu, t. 1, № 4, s. 32–35, 2020. https://doi.org/10.31891/2307-5740-2020-284-4-5

[16] Yu. H. Nieustroiev, T. I. Yehorova-Hudkova, ta V. V. Ostrianko, «Analiz vplyvu tsyfrovizatsii ekonomiky na systemu ekonomichnoi bezpeky derzhavy», Vcheni zapysky Universytetu «KROK», № 4(60), s. 202–209, 2020. https://doi.org/10.31732/2663-2209-2020-60-202-209

[17] N. V. Kasianova, N. M. Kravchuk, ta Yu. L. Koval, «Bezpeka pidpryiemstva v umovakh tsyfrovoi transformatsii ekonomiky», Modern Economics, № 20, s. 124–129, 2020. https://doi.org/10.31521/modecon.V20(2020)-20

[18] M. I. Chepeliuk, Instrumentarii stratehichnoho upravlinnia v konteksti suchasnykh kontseptsii ta trendiv svitovoho ekonomichnoho rozvytku. Kharkiv, Ukraina: FOP Liburkina L. M., 2021.

[19] V. A. Ryzhko, «Kontseptsiia», Entsyklopediia Suchasnoi Ukrainy, I. M. Dziuba, A. I. Zhukovskyi, M. H. Zhelezniak ta in., Red. Kyiv, Ukraina: In-t entsykloped. doslid. NAN Ukrainy, 2014. [Elektronnyi resurs]. Dostupno: https://is.gd/hB9hpJ Data zvernennia: Lyp. 26, 2022.

[20] S. P. Bybyk, ta H. M. Siuta, Slovnyk inshomovnykh sliv: tlumachennia, slovotvorennia ta slovovzhyvannia. Kharkiv, Ukraina: Folio, 2006.

[21] N. Andreichuk, «Paradyhma yak termin», Visnyk Lvivskoi politekhniky, vyp. 52(3), 2008. [Elektronnyi resurs]. Dostupno: https://is.gd/6xfhW7 Data zvernennia: Serp. 17, 2022.

[22] I. V. Perevozova, ta A. Zh. Sakun, «Lohistychna kontseptsiia vyrobnycho-promyslovoho pidpryiemstva», Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Mizhnarodni ekonomichni vidnosyny ta svitove hospodarstvo, vyp. 14, ch. 2, s. 58–64, 2017.

[23] K. S. Salyha, ta O. M. Hutsaliuk, «Resursno-kompetentnistna paradyhma orhanizatsii upravlinnia korporatyvnymy intehratsiinymy protsesamy aktsionernykh tovarystv», Biznes Inform, № 10, s. 369–376, 2018.

[24] A. Kwilinski, K. Pajak, O. Halachenko, S. Vasylchak, Y. Pushak, P. Kuzior, «Marketing tools for improving enterprise performance in the context of social and economic security of the state: innovative approaches to assessment», Marketing and Management of Innovations, iss. 4, pp. 172–181, 2019.

[25] M. F. Kryshtanovych, Ya. Ya. Pushak, M. I. Fleichuk, ta V. I. Franchuk, Derzhavna polityka zabezpechennia natsionalnoi bezpeky Ukrainy:

osnovni napriamky ta osoblyvosti zdiisnennia. Lviv, Ukraina: Spolom, 2020.

[26] V. I. Shulha, «Suchasni pidkhody do traktuvannia poniattia informatsiina bezpeka», Efektyvna ekonomika, № 4, 2015. [Elektronnyi resurs]. Dostupno: https://is.gd/Q5KuZI Data zvernennia: Serp. 24, 2022.

[27] U. Ilnytska, «Informatsiina bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydii nehatyvnym informatsiino-psykholohichnym vplyvam», Visnyk NU «Lvivska politekhnika». Seriia: Politychni nauky, vyp. 2, № 1, s. 27–32, 2016.

[28] H. M. Yarovenko, «Systemnyi pidkhid do formalizatsii poniattia «informatsiina bezpeka», Prychornomorski ekonomichni studii, vyp. 34, s. 239–244, 2018.

[29] S. Ye. Antonova, ta H. F. Martyniuk, «Informatsiina bezpeka», Derzhavne upravlinnia: udoskonalennia ta rozvytok, № 11, 2019. [Elektronnyi resurs]. Dostupno: https://is.gd/GbxMXm Data zvernennia: Serp. 17, 2022.

[30] Ya. Ya. Pushak, ta N. V. Trushkina, «Sutnist poniattia "finansovyi monitorynh" u konteksti zabezpechennia natsionalnoi bezpeky», Visnyk ekonomichnoi nauky Ukrainy, № 2(41), s. 197–203, 2021. https://doi.org/10.37405/1729-7206.2021.2(41).197-203

Стаття надійшла до редакції
10 жовтня 2022 року