JEL A1, M1, O3
DOI: https://doi.org/10.53920/ES-2024-2-9

Дмитро Ігорович ЧЕРНІКОВ,
здобувач третього (освітньо-наукового) рівня вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: 0009-0002-0647-5237

ОСОБЛИВОСТІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ ПІДПРИЄМСТВ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

У статті досліджено особливості формування інформаційно-аналітичного забезпечення діяльності підприємств в умовах гібридних загроз. На основі теоретичного обґрунтування було виокремлено тринадцять основних сфер, за якими доцільно здійснювати дослідження гібридних загроз у діяльності підприємств. Було виокремлено ключові аспекти інформаційно-аналітичного забезпечення розвитку підприємств в умовах гібридних загроз. Обґрунтовано доцільність розгляду інформаційно-аналітичного забезпечення діяльності підприємства як цілісну систему, яка складається з керуючої підсистеми та керованої підсистеми. Доведено, що виявлення вразливостей дозволяє керівництву приймати більш обґрунтовані та виважені управлінські рішення щодо мінімізації негативних наслідків. Встановлено, що система інформаційно-аналітичного забезпечення підприємства – це цілеспрямоване формування інформаційних потоків, які підпорядковані системі планування, оцінки, прийняття управлінських рішень і контролю за їх виконанням. Визначено, що планування відновлення діяльності підприємств після несанкціонованих впливів, втручань чи інших загроз вимагає раннього аналізу та стратегічних підходів для усунення небажаних наслідків. Обґрунтовано, що в стратегічному управлінні розвитком підприємства важливим є аналіз зовнішнього та внутрішнього середовища, яке може становити загрозу або сприяти розвитку підприємства. Обґрунтовано, що на сьогоднішній день більшість відомих методів не повною мірою враховують особливості гібридних загроз, тому необхідним є системний підхід, який дозволяє з максимальною ефективністю комбінувати існуючі методи. Доведено необхідність використання інформаційно-аналі-

тичного забезпечення, яке дозволить повніше сформувати уявлення про стан і перспективи розвитку суб'єкта.

Ключові слова: *гібридні загрози, інформаційно-аналітичне забезпечення, діяльність підприємств, розвиток.*

Dmytro CHERNIKOV,
Postgraduate student,
Kharkiv National University of Radio Electronics

FEATURES OF INFORMATION AND ANALYTICAL SUPPORT FOR THE DEVELOPMENT OF ENTERPRISES IN THE CONTEXT OF HYBRID THREATS

The article examines the peculiarities of the formation of information and analytical support for the activities of enterprises in the conditions of hybrid threats. On the basis of theoretical reasoning, thirteen main areas were singled out, in which it is advisable to carry out research on hybrid threats in the activities of enterprises. The key aspects of information and analytical support for the development of enterprises in conditions of hybrid threats were highlighted. The expediency of considering the information and analytical support of the company's activity as a complete system consisting of a control subsystem and a controlled subsystem is substantiated.

It was determined that the collection and analysis of data includes not only the analysis of financial and operational data on the company's activities, but also the monitoring of social media, the assessment of global political and economic trends. It has been proven that the identification of vulnerabilities allows the management to make more justified and balanced management decisions regarding the minimization of negative consequences. It was established that the system of information and analytical support of the enterprise is a purposeful formation of information flows that are subordinate to the system of planning, evaluation, management decision-making and control over their implementation. It was determined that planning the recovery of enterprises after unauthorized impacts, interventions or other threats requires early analysis and strategic approaches to eliminate unwanted consequences.

It is substantiated that in the strategic management of the development of the enterprise, it is important to analyze the external and internal environment, which can pose a threat or contribute to the

development of the enterprise. It is substantiated that today most of the known methods do not fully take into account the peculiarities of hybrid threats, therefore it is necessary to use a systematic approach that allows combining existing methods with maximum efficiency. The need to use information and analytical support, which will fully form an idea of the state and prospects of the subject's development, has been proven.

Keywords: *hybrid threats, information and analytical support, enterprise activity, development.*

Постановка проблеми. У сучасних реаліях підприємства в Україні функціонують в умовах високого ризику та мінливості оточуючого середовища. Суб'єкти господарювання, які знаходилися на територіях активних бойових дій, або територіях, які є під тимчасовою окупацією, вимушені були релокувати свої потужності до більш спокійних регіонів. Частина з них зазнала значних втрат та руйнацій, які не підлягають відновленню. Спрогнозувати такі наслідки складно, особливо в умовах інформаційної боротьби. Саме тому, в подальшому, в період повоєнної відбудови, необхідно враховувати можливості таких несприятливих подій, які загрожують безпеці діяльності суб'єктів господарювання. Особливо актуальними постають питання гібридних загроз, які мають широкий спектр впливу на діяльність підприємств як в зовнішньому, так і у внутрішньому оточенні. Тому визначення необхідного інформаційно-аналітичного забезпечення є важливим напрямом убезпечення безпеки та розвитку підприємств у стратегічній перспективі, що й обумовлює актуальність обраного дослідження.

Аналіз останніх досліджень та публікацій. Питанню розвитку підприємств та впливу гібридних загроз присвячено багато робіт вітчизняних вчених, серед яких можна виокремити праці Варналія З. С. [6], Геєця В. М. [7], Герасимчук З. В. [8], Гришко С. В. [1], Данилишина Б. М. [9], Ляшенко О. М. [13], Полозової Т. В. [15]. Незважаючи на значні наукові здобутки означених авторів, питання інформаційно-аналітичного забезпечення розвитку підприємств в умовах гібридних загроз потребують подальших досліджень.

Мета статті полягає у дослідженні особливостей інформаційно-аналітичного забезпечення розвитку підприємств в умовах гібридних загроз.

Виклад основного матеріалу дослідження. Для формування інформативного інформаційно-аналітичного забезпечення розвитку підприємств в умовах гібридних загроз необхідно визначитися, що саме слід розуміти під «гібридними загрозами». Аналіз теоретичних положень терміна «гібридні загрози», дозволив дійти висновку про багатоваріантність визначення терміна. Проте, на нашу думку, в напрямі дослідження підприємств, влучним є визначення гібридної загрози, як дії [1], метою якої є підрив або нанесення шкоди демократичним системам, впливаючи на прийняття рішень [2]. Дії можуть мати місце, наприклад, у політичній, економічній, військовій, цивільній або інформаційній сферах.

Слід зазначити, що розвиток гібридних загроз та ризиків посилюється найчастіше в тих сферах, які мають внутрішні структурні інституційні вразливості. До таких негативних факторів належать: корупція, тіньова економіка, рейдерство, монополізація бізнесу тощо. Наявність таких негативних факторів створює сприятливі умови для зовнішнього втручання різними суб'єктами економічного та державного управління. Для України і є характерними такі фактори несприятливого середовища, що негативно впливає на її розвиток та конкурентоспроможність. Так, за даними індексу сприйняття корупції в 2021 році Україна посідала 122 місце зі 180, у 2022 році посідала 116 місце з 180 країн, у 2023 році держава покращила свої позиції опинившись на 104 місці зі 180 країн. Лідерами рейтингу у 2023 році є Данія (90 балів), найгірший показник у Сомалі (180 місце зі 180) [11].

У більшості досліджень, які присвячені питанню гібридних загроз, було виокремлено тринадцять сфер, на які націлені такі ризики, а саме: економічна, політична, правова, інфраструктурна, соціальна, військова, культурна, дипломатична, інформаційна, кібернетична, публічного управління, комунікаційна та розвідувальна [3]. У зв'язку з розвитком нових цифрових технологій гібридні загрози не ідентифікуються звичайними моніторинговими системами, які працюють лише в одному домені. Потрібні нові підходи до економічного аналізу (моніторингу), який би охоплював основні домени гібридних загроз, що чинять вплив на економічні явища та процеси й включають дослідження за такими сферами (табл. 1).

Таблиця 1. Основні сфери дослідження гібридних загроз

Сфера моніторингу	Основні положення
Економічна	використання економічного інструментарію для досягнення цілей зовнішньої політики на основі застосування засобів економічної безпеки є одним з пріоритетних джерел державного впливу та влади.
Політична	формування пріоритетності влади на певній території на основі використання різних форм політичного впливу.
Правова	сукупність правових норм, чинників, правил, інститутів, які можуть бути використані для досягнення правових або неправових наслідків в гібридних загрозах.
Інфраструктурна	використовується для погіршення умов життя населення на певній території, для отримання бажаного ефекту в прийнятті певних рішень. Такий ефект дуже наочно використовується в Україні, оскільки більшість атак здійснюється саме на об'єкти критичної інфраструктури (які забезпечують життєдіяльність суспільства), з метою виснаження економічних, соціальних та виробничих сфер.
Соціальна	використання чинників, які можуть розколоти суспільство, призвести до збільшення рівня безробіття населення, що впливає на соціальну напруженість.
Військова	знищення цілісності та суверенітету держави. Зниження рівня обороноздатності країни є одним з ефективних напрямів тиску та посилення впливу зовнішніх факторів, що може служити підґрунтям для майбутніх військових операцій.
Культурна	використання державної культурної експансії для підтримки ворожих цілей (такі гібридні атаки можуть бути як зовнішніми, так і внутрішніми).
Дипломатична	управління політикою міжнародних відносин, які формує держава в своїй діяльності. У деяких аспектах міжнародної політики виправдовується війна, як елемент оборонних заходів проти спровокованої агресії з боку інших держав.
Інформаційна	використання у власних цілях інформації, яка здатна розділити групи впливу та стратегічні альянси. Найчастіше інформаційний простір використовують для протистояння політичних та економічних сил, націлених на суспільство з метою зміни їх уяви про реальний стан речей.

Закінчення таблиці 1

Сфера моніторингу	Основні положення
Кібернетична	розповсюдження терористичних актів, шпигунства, пропаганди, кіберзлочинності.
Публічне управління	недосконалість судової та правової сфери спричиняє розвиток корупції, бюрократії в державі, що негативно позначається на всіх сферах не тільки на національному рівні, але й в геополітичному просторі.
Космічна	використання навігації, зв'язку, науки та дослідження, які під впливом розвитку науково-технічного прогресу можуть впливати на сферу зв'язку більшості країн. На сьогодні активно розвивається космічна галузь, засоби штучного інтелекту, які можна використовувати для управління, збору та обробки даних для застосування в небезпечних цілях.
Розвідувальна	використання важливої стратегічної інформації проти держави, при її потраплянні до рук агресора. Загалом, розвідка націлена на збір, обробку та аналіз інформації, яка передається політикам, державним службовцям для прийняття стратегічних рішень щодо розвитку та захисту держави.

Джерело: узагальнено автором на основі [5]

Всі означені сфери першочергово впливають на макрорівень діяльності держави, проте підприємство функціонує в межах держави та в умовах впливу політичної, економічної, військової та інших сфер [4]. Тому такі елементи гібридних загроз також можна досліджувати на рівні окремого підприємства або регіону.

Оскільки підприємство функціонує в глобальному вимірі на яке впливає як зовнішнє, так і внутрішнє середовище, саме гібридність загроз для їх визначення та оцінки є досить складним явищем через їх багатомірність [17]. Для вивчення ймовірності впливу таких загроз важливим є формування інформаційно-аналітичного забезпечення розвитку підприємств, що включає поєднання різних інструментів та методів розпізнавання, аналізу та прогнозування ризиків. До основних аспектів формування аналітичного забезпечення стратегічного розвитку підприємств в умовах гібридних загроз належать такі (рис. 1).

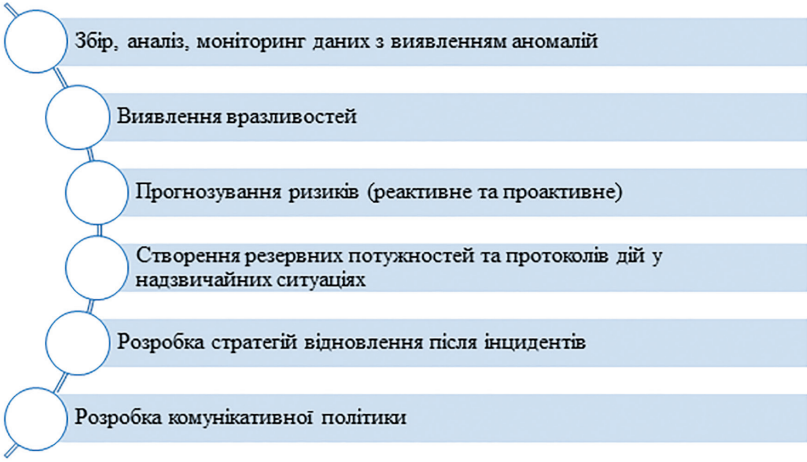

Рис. 1. Ключові аспекти інформаційно-аналітичного забезпечення розвитку підприємств в умовах гібридних загроз

Джерело: сформовано автором

Збір та аналіз даних містить не тільки аналіз фінансових та операційних даних щодо діяльності підприємства, але й моніторинг соціальних медіа, оцінку глобальних політичних та економічних тенденцій. Така аналітика націлена на виявлення потенційних загроз та можливостей. Аналітичні інструментарії використовуються для виявлення слабких сторін в діяльності організації, що можуть вказувати на кібератаки або різні внутрішні зловживання.

Виявлення вразливостей дозволяє керівництву більш обґрунтовано та виважено приймати управлінські рішення щодо мінімізації негативних наслідків. Аналіз трендів дозволяє підприємству прогнозувати можливі ризики та загрози з подальшим розробленням відповідних заходів щодо їх мінімізації або усунення. Результати моніторингу допомагають виявити вже відомі атаки для реактивного захисту, а пошук аномалій – «невідомі - невідомі» вразливості та незвичайну активність, зокрема й у мережі, що дозволяє проактивно реагувати та захищати систему [10].

Система інформаційно-аналітичного забезпечення підприємства являє собою цілеспрямоване формування інформаційних потоків, які підпорядковані системі планування, оцінки, прийнят-

тю управлінських рішень та контролю за їх виконанням. Інформаційно-аналітичне забезпечення діяльності підприємства доцільно розглядати як цілісну систему, яка складається з керуючої підсистеми та керованої підсистеми (рис. 2). На вході в систему акумулюються різни види ресурсів (інформаційних, фінансових, трудових, матеріальних), які під впливом керуючої системи проходять різні стадії управління. Так, керуюча підсистема містить елементи планування, організацію, мотивацію та контроль. Функції системи управління містять планування вхідних ресурсів, їх організацію для ефективної роботи підприємства, мотивацію здійснювати необхідні дії та контроль за їх виконанням.

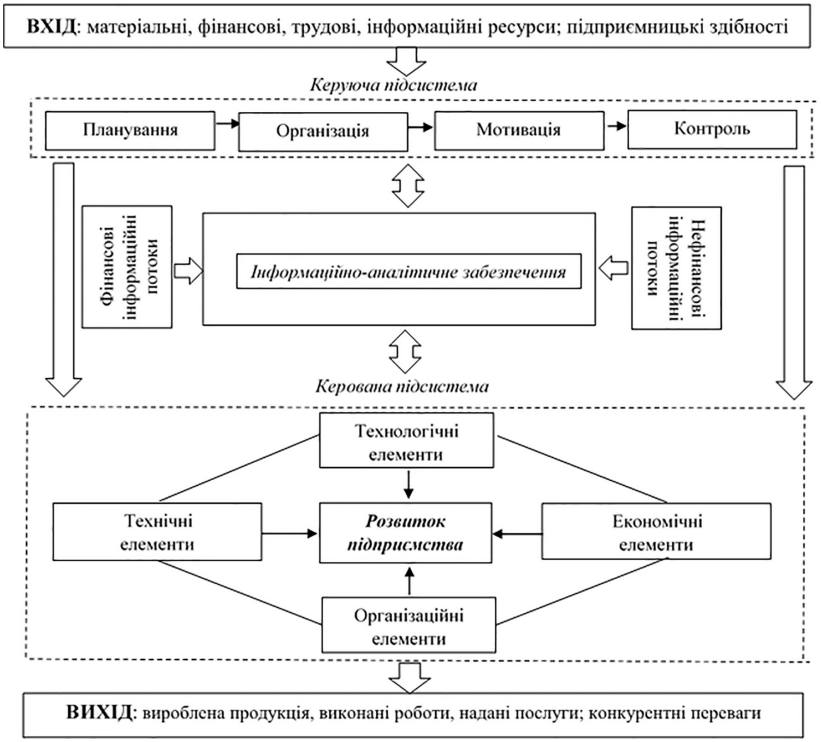

Рис. 2. Система інформаційно-аналітичного забезпечення діяльності підприємств

Джерело: сформовано автором на основі [12; 14; 16]

Керуюча підсистема на основі своїх функцій формує інформаційно-аналітичний базис діяльності підприємства. Інформаційно-аналітичний базис містить фінансові та нефінансові інформаційні потоки, які формують основу діяльності підприємства, містить, зокрема, й протидію гібридним загрозам.

Керована підсистема – об'єкт управління, який, в свою чергу, становить єдність технічних, технологічних, організаційних, економічних елементів і зв'язків між ними [17]. На виході системи підприємство отримує результат у вигляді готової продукції, послуг, конкурентних переваг.

Планування відновлення діяльності підприємств після несанкціонованих впливів, втручань або інших загроз потребує завчасного аналізу та стратегічних підходів щодо усунення небажаних наслідків. На сьогодні доцільним є використання на підприємствах засобів штучного інтелекту та автоматизованих аналітичних систем, що дозволяє виявляти патерни й тренди, які складно виявити реактивними моніторинговими системами, що може бути ефективним інструментом протидії складним гібридним загрозам.

У стратегічному управлінні розвитком підприємства важливим є аналіз зовнішнього та внутрішнього середовища, яке може становити загрозу або сприяти розвитку підприємства. Для оцінки інформаційно-аналітичного забезпечення стратегічного управління підприємством використовується ряд методик, які мають включати як кількісні, так і якісні методи [8]. Проте, на сьогодні, більшість відомих методів не враховує в повному обсязі особливостей гібридних загроз, тому необхідним є використання системного підходу, який дозволяє комбінувати існуючі методи з максимальною ефективністю.

Для реалізації стратегічних ініціатив щодо забезпечення розвитку підприємств в умовах гібридних загроз доцільно дотримуватися певних аспектів здійснення діяльності, а саме:

- структуризації аналітичної та інформаційної складової діяльності підприємства;
- використання методичного забезпечення, яке враховує особливості оцінки гібридних загроз;
- для захисту інформації на підприємстві необхідно використовувати систему резервного копіювання даних, що дасть можливість підприємству за короткі терміни відно-

вити свою роботу у випадку настання несприятливих подій кібератак;

- у стратегічному плануванні підприємству важливо приділяти увагу розробці заходів протидії ризикам, які містять напрями їх усунення або мінімізації з урахуванням захисту та повноти інформаційно-аналітичного забезпечення;
- для успішного управління ризиками та протидії гібридним загрозам на підприємстві необхідно приділяти увагу навчанню персоналу щодо ідентифікації таких загроз та методів їх уникнення;
- для використання сучасних технологій підприємствам доцільно налагоджувати співпрацю з різними міжнародними партнерами для обміну досвідом в питаннях протидії гібридним загрозам та захисту інформації.

Висновки. Умови сьогодення, які характеризуються ризиками та гібридними загрозами, потребують від підприємств виважених підходів щодо формування інформаційно-аналітичного забезпечення своєї діяльності, оскільки, в подальшому, на основі таких даних формується стратегія розвитку суб'єкта господарювання. Функціонування підприємств в умовах гібридних загроз вимагає системного підходу, який передбачає поєднання традиційних стратегій управління та інноваційних підходів до питань захисту бізнесу. Необхідно використовувати інформаційно-аналітичне забезпечення, яке в повному обсязі сформує уявлення про стан та перспективи розвитку суб'єкта. Особливо гостро постають проблеми формування інформаційно-аналітичного забезпечення діяльності підприємств в умовах високої мінливості та невизначеності оточуючого середовища, що негативно впливає на можливість стратегічного управління суб'єктами господарювання. Точність, інформативність та достовірність даних щодо діяльності підприємств допомагає керівникам більш об'єктивно враховувати існуючі ризики та загрози, що впливає, в подальшому, на адаптивну спроможність підприємства протидіяти гібридним загрозам. В умовах сьогодення, для підприємств України важливо оцінювати своє інформаційно-аналітичне забезпечення протидії загрозам з урахуванням зміни оточуючого середовища, що дозволить в майбутньому визначити недоліки в інформаційно-аналітичному забезпеченні.

ЛІТЕРАТУРА

1. Hybrid Threats Glossary / Глосарій з гібридних загроз Deliverable 5.5 «WARN environment» Результат 5.5 «WARN-середовище» «Academic Response to Hybrid Threats» Erasmus+ Capacity Building Project WARN 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP URL: https://openarchive.nure.ua/server/api/core/bitstreams/8ea23436-adf5-4127-8b1b-2d251b4ea81e/content.

2. NATO. Capstone Concept for the Military Contribution to Countering Hybrid Threats. Brussels: NATO Military Committee. 2020. 18 p. https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf.

3. Nemeth, William, J. Future War and Chechnya: A Case for Hybrid Warfare. Monterey: Naval Postgraduate School. URL: https://core.ac.uk/download/pdf/36699567.pdf.

4. O'Rourke, Ronald. A Shift in the International Security Environment: Potential Implications for Defense. Issues for Congress. URL: https://www.everycrsreport.com/files/20181024_R43838_fd72c9a2f744419b3ff915ddc881ed7ce74caddf.pdf.

5. PATRICK, CULLEN, et al. The landscape of Hybrid Threats: A Conceptual Model (Public Version). 2021.

6. Варналій З.С., Буркальцева Д.Д., Саєнко О.С. Економічна безпека України: проблеми та пріоритети зміцнення : моногр. Київ : Знання України, 2011. 299 с.

7. Геєць В. М. Економіка України: ключові проблеми і перспективи. *Економіка і прогнозування*. 2016. № 1. 722 с.

8. Герасимчук З. В. Абрамова І. О. Механізм забезпечення соціально-економічної безпеки регіонів держави. *Intellectual economics: investment aspect*. 2016. С. 14 – 23.

9. Данилишин Б., Малій О. Онищенко С. Соціально-економічна безпека: сучасний підхід до забезпечення соціально-економічного розвитку регіонів. *Економіка і регіон*. 2019. С. 62 – 73.

10. Івченко Ю. А. Теоретичні засади забезпечення потенціалу економічної безпеки підприємства в умовах гібридних загроз та постконфліктної трансформації. *Вісник Східноукраїнського національного університету імені Володимира Даля*. № 1 (257). 2020. С. 32 – 39.

11. Індекс сприйняття корупції. Transparency international Ulraine. URL: https://cpi.ti-ukraine.org/.

12. Котлер Ф, Армстронг Г. Основи маркетингу. *Науковий світ*. 2022. 880 с.

13. Ляшенко О. М. Ресурсно-захисний підхід до стратегування економічної безпеки підприємства. *Вчені записки Університету «КРОК»*. 2021. С. 132 – 143.

14. Пирожков С. І., Майборода О. М., Хамітов Н. В., Головаха Є. І., Дембіцький С. С., Смолій В. А. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь. *Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України*. Київ. 2022. 552 с.

15. Полозова Т. В, Ал-Касеасбех Ахмад Закарія Саламех Особливості формування обліково-аналітичної інформації в системі забезпечення економічної безпеки підприємства. 2020. ХНУРЕ.

16. Сменковський А. Ю. Економічні інструменти протидії гібридній агресії. Київ : НІСД. 2020. 69 с.

17. Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці: Матеріали IV Міжнародної науково-практичної конференції (м. Київ, 22 листопада 2023 року). Київ: ДУІТ, ХНУРЕ, МНТУ. 2023. 821 с.

REFERENCES

1. Hybrid Threats Glossary URL: https://openarchive.nure.ua/server/api/core/bitstreams/8ea23436-adf5-4127-8b1b-2d251b4ea81e/content.

2. NATO. (2020). Capstone Concept for the Military Contribution to Countering Hybrid Threats. Brussels: NATO Military Committee. 18 p. https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf.

3. Nemeth, William, J. Future War and Chechnya: A Case for Hybrid Warfare. Monterey: Naval Postgraduate School. URL: https://core.ac.uk/download/pdf/36699567.pdf.

4. O'Rourke, Ronald. A Shift in the International Security Environment: Potential Implications for Defense. Issues for Congress. URL: https://www.everycrsreport.com/files/20181024_R43838_fd72c9a2f744419b3ff915ddc881ed7ce74caddf.pdf.

5. PATRICK, CULLEN, et al. The landscape of Hybrid Threats: A Conceptual Model (Public Version). 2021.

6. Varnalii Z.S., Burkaltseva D.D., Sayenko O.S. (2011). Economicna bezpeka Ukraini problem I prioriteti zmicnenya [Economic security of Ukraine: problems and priorities of strengthening]. *Knowledge of Ukraine*. 299 p.

7. Geets V. M. (2016). Economika Ukraini kluchovi problem I perspektivi [Economy of Ukraine: key problems and prospects]. *Economics and forecasting*. No 1. 722 p.

8. Gerasimchuk Z. V. Abramova I. O. (2016). Mehanizm zabezpecheniya socialno-economicnoi bezpeki regioniv dergavi [The mechanism of ensuring socio-economic security of the regions of the state]. *Intellectual economics: investment aspect*. Pp. 14 – 23.

9. Danylyshyn B., Malii O. Onyshchenko S. (2019). Socialno-economicna bezpeka suchasnii pidhid do zabezpecniya socialno-economicnogo rozvitku regioniv [Socio-economic security: a modern approach to ensuring the socio-economic development of regions]. *Economy and region*. Pp. 62 – 73.

10. Ivchenko Yu. A. (2020). Teoretucnha zasadi zabezpecneniya potencialy economicnoi bezoeki pidpriemstva v umovah hibridnih zagroz ta postkonfliktnoi transformacii [Theoretical principles of ensuring the potential of economic security of the enterprise in conditions of hybrid threats and post-conflict transformation]. *Bulletin of the Eastern Ukrainian National University named after Volodymyr Dal*. No. 1 (257).Pp. 32 – 39.

11. Index of perception of corruption. Transparency international Ulrain. URL: https://cpi.ti-ukraine.org/.

12. Kotler F, Armstrong G. (2022). Osnovi marketing [Basics of marketing]. *Scientific world*. 880 p.

13. Lyashenko O. M. (2021). Resursno-zahianii pidhid do strateguvaniya economicnoi bezpeki pidpriemstva [Resource-protective approach to strategizing economic security of the enterprise]. *Scientific notes of the KROK University*. Pp. 132 – 143.

14. Pirozhkov S. I., Maiboroda O. M., Khamitov N. V., Holovakha E. I., Dembitskyi S. S., Smoliy V. A. (2022). Nacionalna stiikist Ukraini strategiai vidpovidi na vikliki ta viperedgeniua gibridnih zagroz nationalna dopovid [National resilience of Ukraine: a strategy for responding to challenges and anticipating hybrid threats: national report]. *Institute of Political and Ethnonational Studies named after I. F. Kuras NAS of Ukraine*. Kyiv. 552 p.

15. Polozova T.V., Al-Kaseasbeh Ahmad Zakaria Salameh. (2020). Osoblivosti formuvaniya oblikovo-analiticnoi infiormacii v sisteme zabezpecheniya economicnoi bezpeki pidpriemstva [Peculiarities of the formation of accounting and analytical information in the system of ensuring the economic security of the enterprise]. KHNURE.

16. Smenkovsky A. Yu. (2020). Ekonomicni instrumenti protidii gibridnii agresii [Economic tools for countering hybrid aggression]. Kyiv: NISD. 69 p.

17. Upravlenie I administruvanie v umovah protidii gibridnim zagrozam nationalnii bezpeci (2023). [Management and administration in the conditions of countering hybrid threats to national security: Materials of the 4th International Scientific and Practical Conference] (Kyiv, November 22, 2023). Kyiv: DUIT, Khnure, MNTU. 821 p.

СТАТТЯ НАДІЙШЛА ДО РЕДАКЦІЇ 24.04.2024