УДК 316.776:004.58:658.012+334.7(477) DOI: *https://doi.org/10.37405/1729-7206.2023.1(44).45-49*

Катерина Сергіївна Озарко
канд. екон. наук
ORCID 0000-0002-1452-0686
e-mail: kateryna.ozarko@gmail.com,

Сергій Богданович Копитко
канд. екон. наук
ORCID 0000-0001-7353-0422
e-mail: KopytkoSB@gmail.com,

Державний університет інтелектуальних технологій і зв'язку, м. Одеса

ОСОБЛИВОСТІ ФУНКЦІОНАЛЬНОГО ПІДХОДУ ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ ЗА КРИЗОВИХ УМОВ

Постановка проблеми. За сучасних високодинамічних умов розвитку комп'ютерних, інформаційних та комунікаційних технологій, активізування використання глобальної мережі Інтернет підприємствами, організаціями, людьми тощо захист інформації, інформаційна безпека посідає все вагоміше місце в системі економічної безпеки підприємств. Адже постійно виникають загрози кібервтручання, дестабілізуючих впливів на певні об'єкти підприємств із використанням високотехнологічних можливостей інформаційного, комунікаційного, кіберпросторів [3]. Безперервно структурні підрозділи підприємства, що займаються забезпеченням необхідного рівня інформаційної безпеки, стикаються зі спробами несанкціонованих доступів до інформаційних масивів.

Передумовами для досягнення інформаційної безпеки підприємства виступає формування та реалізування сучасних, інноваційних методологій, систем щодо управління нею, особливо це стосується кризових умов господарювання.

Аналізування останніх досліджень і публікацій. Проблематиці управління інформаційною безпекою підприємств та організацій, держави є присвячені наукові здобутки таких фахівців як Т. Андрухів [15], О. Атамас [1], О. Безпарточна [18, с. 8-19], О. Безчасний [19, с. 282-295], А. Білоус [2, с. 51-55], В. Бурячок [3], В. Вітлінський [4-5], Г. Великоіваненко [4], М. Ворохоб [14, с. 98-112], В. Гаркуша [6, с. 85-90], Н. Георгіаді [13], О. Гладка [11, с. 69-74], Н. Грабар [7], І. Доровська [19, с. 282-295], А. Завербний [8, с. 110-113; 9, с. 13-19], І. Карпович [11, с. 69-74], Р. Корчомний [14, с. 98-112], Н. Коршун [14, с. 98-112], І. Котерлін [12, с. 150-155], О. Кузьмін [13], І. Літвінчук [14, с. 98-112], Т. Майстер [1], Ю. Наконечна [11, с. 69-74], С. Наконечний [5], К. Озарко [15], Я. Пушак [8, с. 110-113;18, с. 8-19; 19, с. 282-295], М. Репін [2, с. 51-55], В. Толубко [10], Н. Трушкіна [18, с. 8-19], В. Хобта [19, с. 282-295], А. Чередниченко [16, с. 335-338], О. Шандрівська [17, с. 94-105], Н. Шинкаренко [17, с. 94-105] та багатьох інших.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на детальне дослідження процесів управління інформаційним забезпеченням, інформаційною безпекою підприємства недостатньо висвітленою залишається проблематика управління інформаційною безпекою на засадах функціонального підходу, функціональна послідовність формування системи управління інформаційною безпекою підприємств.

Формулювання цілей статті (постановка завдання). Цілі статті полягають у дослідженні проблематики застосування функціонального підходу при формуванні системи управління інформаційною безпекою підприємств за кризових умов.

Виклад основного матеріалу дослідження. Активний розвиток новітніх інформаційних, комунікаційних технологій, загальне комп'ютеризування привели до того, що інформаційна безпека стала ключовою характеристикою інформаційних систем підприємств. Адже за умов, що інформаційно-комунікаційні технології володіють глобальним характером, саме інформаційна безпека стає невід'ємною частиною всієї системи економічної безпеки підприємств.

Комплексність актуальних загроз безпеці підприємств саме в інформаційній сфері вимагає від менеджмерів формування дієвої системи управління інформаційною безпекою, що базуватиметься на інноваційних підходах при формуванні систем захисту інформаційного простору за глобалізаційних, інтеграційних умов, особливо при кризових явищах.

Інформаційну небезпеку для підприємств формують інформаційні загрози, які поширюються інформаційним простором, комунікаціями тощо. Від рівня ефективності сформованої системи управління інформаційною безпекою будь-якого підприємства залежатиме його економічна безпека. Адже інформаційні ризики, як і будь-які інші їх види, становлять потенційну загрозу збитковості підприємства.

Формування комплексної системи управління інформаційною безпекою доцільно здійснювати на всеохоплюючих засадах функціонального підходу. Оскільки лишень функціональний підхід [13] (базування на ключових управлінських функціях) сприятиме досягненню комплексності системи управління інформаційною безпекою підприємств (див. рисунок).

Лишень чітке дотримання послідовності виконання ключових управлінських функцій [13] сприятиме досягненню очікуваного результату (збалансо-

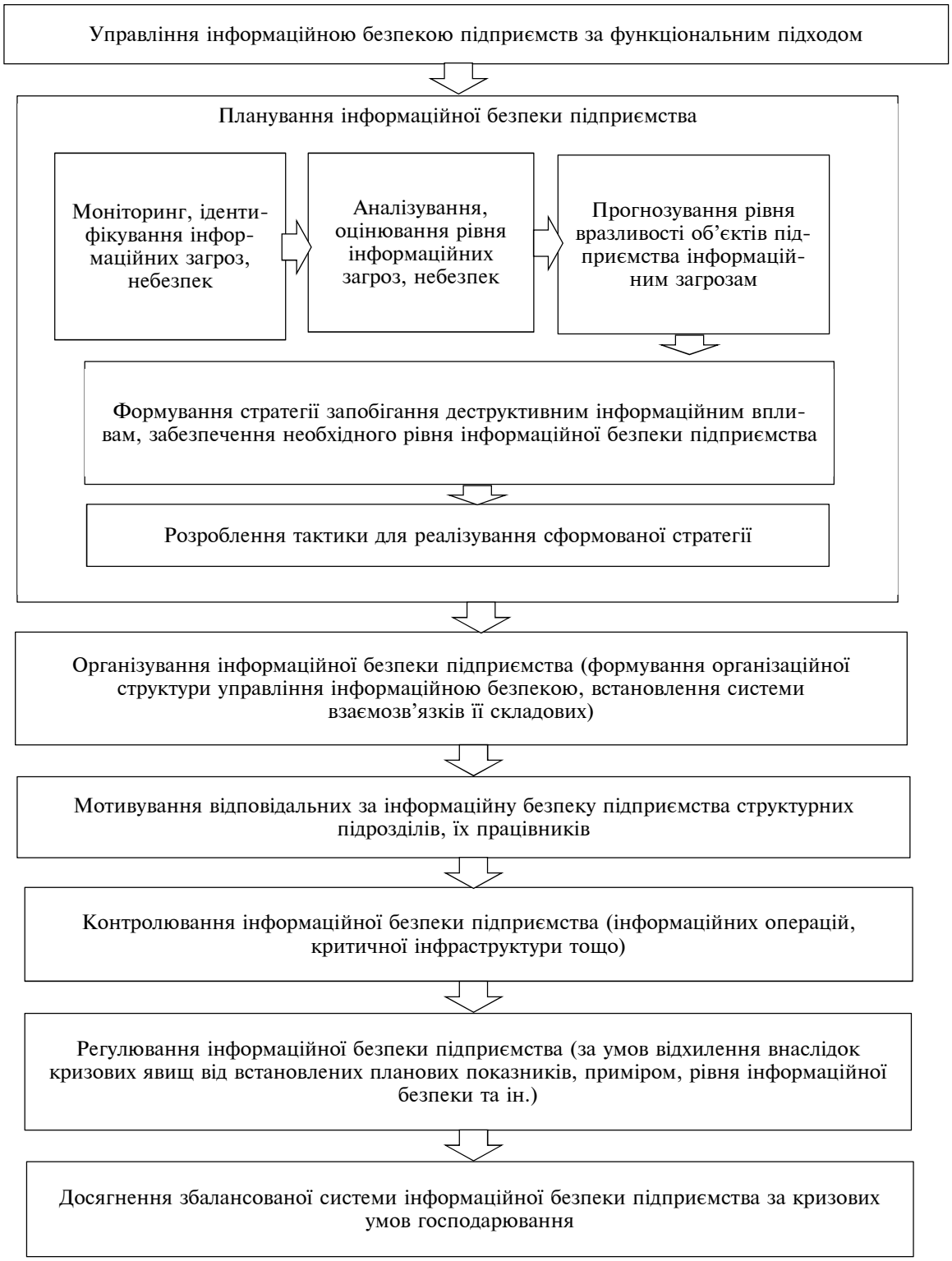

Рисунок. Концептуальна модель управління інформаційною безпекою підприємства за кризових умов на засадах функціонального підходу

Примітка: побудовано на основі [6, с. 88; 12-13;16, с. 97].

вана система інформаційної безпеки підприємства за кризових умов господарювання).

Передусім потрібно чітку спланувати процеси управління інформаційною безпекою підприємства (див. рисунок) [13].

Лишень розроблена чітка стратегія та формування тактики для її подальшого реалізування, забезпечення гнучкості розробленої стратегії, враховуючи динамічність внутрішнього, зовнішнього середовищ (і загроз та перспективи, які виникатимуть в процесі

управління) сприятимуть ефективному функціональному управлінні інформаційною безпекою підприємства.

Встановлені орієнтири спонукатимуть всі задіяні в системі управління підрозділи дотримуватися єдиної стратегії (функція організування інформаційної безпеки). Задля стимулювання вказаного процесу потрібно вміло розробити мотивуючі заходи (функція мотивування всіх фахівців, залучених в процеси управління інформаційною безпекою (див. рисунок) [13].

Процес ефективного управління інформаційною безпекою сприятиме забезпеченню прийняття, реалізування ефективних управлінських рішень на підприємстві.

Система управління інформаційною безпекою підприємств, що формується на засадах функціонального підходу повинна забезпечувати надійний рівень захисту інформації, комунікацій підприємства. Це досягатиметься передусім завдяки безперервного моніторингу інформаційного середовища (загроз, небезпек, викликів тощо), постійному контролюванню інформаційно-комунікаційної діяльності підприємства, прогнозуванню інформаційної безпеки (зокрема ризиків, які на неї чинитимуть вплив) [4-6] тощо.

Запропонований для використання функціональний підхід при формуванні системи управління інформаційною безпекою підприємства дозволятиме отримувати керівництву науково-обгрунтовані управлінські рішення, спрямовані на зменшення потенційних наслідків від реалізування загроз, зниження ймовірності виникнення їх у майбутніх періодах.

Дослідження існуючих методів управління інформаційною безпекою підприємств дає можливість пропонувати новітні підходи до управління ризиками інформаційної безпеки [4-5], оцінювати загрози (їх рівень, ймовірність впливу, настання тощо), загальний стан інформаційної безпеки підприємства (галузі). Це дозволятиме системі менеджменту підприємства попереджувати виникнення можливих збитків при настанні загроз в інформаційній сфері [17, с. 97-98].

Результатом формування та застосування систему управління інформаційною безпекою підприємства на засадах функціонального підходу є формування комплексної, збалансованої, дієвої та гнучкої системи інформаційної безпеки, яка враховуватиме всі особливості застосування заходів для захищеності підприємства від негативних інформаційних, комунікаційних впливів, захисту інформаційних масивів (даних), інформаційних та інтелектуальних прав, забезпечуватиме відкритий доступ до інформаційних ресурсів працівників [17, с. 97-98].

Будуючи систему управління інформаційною безпекою підприємства саме на засадах функціонального підходу можна досягти високого рівня її самовдосконалення, гармонійного розвитку тощо.

Висновки з дослідження і перспективи подальших розвідок у цьому напрямі. Отже, формування системи управління інформаційною безпекою підприємств за кризових умов, що формується на засадах -функціонального підходу повинна забезпечувати надійний рівень захисту інформації, комунікацій підприємства. Досягатиметься це завдяки безперервного моніторингу інформаційного середовища (загроз, небезпек, викликів тощо), постійному контролюванню (за необхідності регулюванню) інформаційно-комунікаційної діяльності підприємства, прогнозуванню інформаційної безпеки (зокрема ризиків, які на неї чинитимуть вплив) тощо. Запропонований для використання функціональний підхід при формуванні систем управління інформаційною безпекою підприємств дозволить їх керівництву формувати і реалізовувати науково-обгрунтовані управлінські рішення, спрямовані на зменшення потенційних наслідків від реалізування загроз, зниження ймовірності виникнення їх у майбутніх періодах. Застосування концептуальної моделі управління інформаційною безпекою підприємства за кризових умов на засадах функціонального підходу сприятиме підвищенню рівня інформаційної та економічної безпеки. Перспективи подальших досліджень полягатимуть у дослідженні існуючих методів, підходів до управління інформаційною безпекою підприємств а також деталізування кожної із часткових функцій управління.

Список використаних джерел

1. Атамас О. П., Майстер Т. М. Удосконалення системи управління інформаційною складовою фінансово-економічної безпеки підприємства. *Проблеми сучасних трансформацій. Серія: економіка та управління*. 2023. № 8. URL: https://reicst.com.ua/pmt/article/view/2023-8-04-02. DOI: https://doi.org/10.54929/2786-5738-2023-8-04-02.

2. Білоус А. Я., Репін М. В. Мінімізація ризиків на підприємстві шляхом впровадження системи екологічного менеджменту. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки*. 2020. Т. 31(70). № 1. С. 51−55. DOI https://doi.org/10.32838/2663-5941/2020.1-1/09.

3. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ: НАУ, 2013. 432 с.

4. Вітлінський В. В., Великоіваненко Г. І. Ризикологія в економіці та підприємництві: монографія. Київ: КНЕУ, 2004. 480 с.

5. Вітлінський В. В., Наконечний С. І. Ризик у менеджменті. Київ: ТОВ "Борисфен-М", 1996. 336 с.

6. Гаркуша В. О. Методичний підхід до оцінки ризиків інформаційної безпеки підприємства. *Приазовський економічний вісник*. 2020. Вип. 2(19). С. 85-90. DOI: https://doi.org/10.32840/2522-4263/2020-2-15.

7. Грабар Н. С. Інформаційна безпека в умовах становлення глобального інформаційного суспільства. *Державне управління: удосконалення та розвиток*. 2019. № 7. URL: http://www.dy.nayka.com.ua/?op=1&z=1461. DOI: https://doi.org/10.32702/2307-2156-2019.7.21.

8. Завербний А. С., Пушак Я. Я. Проблеми та потенційні можливості розвитку ІТ-сфери в Україні за умов активізування процесів інтегрування до міжнародного ринку: управлінський аспект. *Вісник економічної науки*. 2022. №1(42). С. 110-113. DOI: https://doi.org/10.37405/1729-7206.2022.1(42).110-113.

9. Завербний А. С. Комунікаційні стратегії: проблеми та перспективи формування і реалізування за умов євроінтегрування. *Innovation and Sustainability*. 2022. № 1. С. 13-19. DOI: https://doi.org/10.31649/ins.2022.1.13.19.

10. Інформаційна безпека держави у контексті протидії інформаційним війнам / заг. ред. В. Толубка. Київ: НАОУ, 2004. 177 с.

11. Карпович І. М., Гладка О. М., Наконечна Ю. А. Аналіз ризиків безпеки інформаційної сис-

теми ІТ-підприємства. *Вчені записки ТНУ імені В. І. Вернадського. Серія: технічні науки*. 2020. Т. 31 (70). № 5. С. 69-74. DOI https://doi.org/10.32838/2663-5941/2020.5/12.

12. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 1. С. 150-155.
DOI: https://doi.org/10.32782/392257.

13. Кузьмін О. Є., Георгіаді Н. Г. Формування і використання інформаційної системи управління економічним розвитком підприємства: монографія. Львів: Львівська політехніка, 2006. 368 с.

14. Літвінчук І. С., Корчомний Р. О., Коршун Н. В., Ворохоб М. В. Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». *Кібербезпека: освіта, наука, техніка*. 2020. № 2(10). С. 98-112. DOI: https://doi.org/10.28925/2663-4023.2020.10.98112.

15. Озарко К. С., Андрухів Т. В. Особливості формування оптимальних організаційних структур управління ІТ-бізнесом як елемент його інформаційної безпеки. *Економіка та суспільство*. 2022. 43. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1709. DOI: https://doi.org/10.32782/2524-0072/2022-43-21.

16. Чередниченко А. О. Методи забезпечення захисту підприємств від економічного шпигунства. *Вісник економіки транспорту і промисловості*. 2013. № 42. С. 335-338.

17. Шандрівська О. Є., Шинкаренко Н. В. Прикладна оцінка ризиків у системі забезпечення безпеки соціально-економічних процесів у кіберпросторі. *Вісник Національного університету "Львівська політехніка". Серія "Проблеми економіки та управління"*. 2020. № 2(8). С. 94-105. DOI:https://doi.org/10.23939/semi2020.02.094.

18. Bezpartochna O., Pushak Ya., Trushkina N. Current issues of information security management during the state of martial. *Current issues of security management during martial law*: scientific monograph. Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, 2022. P. 8-19.

19. Bezchasnyi O., Khobta V., Pushak Ya., Kotkalova-Litvin I., Dorovska I. Modeling of control stability of communication channels in development management conditions. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2018. Т. 4, №27. С. 282-295.

References

1. Atamas, O. P., Maister, T. M. (2023). Udoskonalennia systemy upravlinnia informatsiinoiu skladovoiu finansovo-ekonomichnoi bezpeky pidpryiemstva [Improving the management system of the information component of the financial and economic security of the enterprise]. *Problemy suchasnykh transformatsii. Seriia: ekonomika ta upravlinnia – Problems of modern transformations. Series: Economics and Management*, 8. Retrieved from https://reicst.com.ua/ pmt/ article/view/2023-8-04-02 [in Ukrainian].

2. Bilous, A. Ya., Repin, M. V. (2020). Minimizatsiia ryzykiv na pidpryiemstvi shliakhom vprovadzhennia systemy ekolo-hichnoho menedzhmentu [Minimizing risks at the enterprise by implementing an environmental management system]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Tekhnichni nauky – Scientific notes of TNU named after V. I. Vernadskyi. Series: Technical sciences*, Vol. 31(70), no. 1, pp. 51–55. DOI https://doi.org/10.32838/2663-5941/2020.1-1/09 [in Ukrainian].

3. Buriachok, V. L. (2013). Osnovy formuvannia derzhavnoi systemy kibernetychnoi bezpeky [Fundamentals of Formation of the State System of Cyber Security]. Kyiv, NAU. 432 p. [in Ukrainian].

4. Vitlinskyi, V. V., Velykoivanenko, H. I. (2004). Ryzykolohiia v ekonomitsi ta pidpryiemnytstvi [Riskology in Economics and Entrepreneurship: a monograph]. Kyiv, KNEU. 480 p. [in Ukrainian].

5. Vitlinskyi, V. V., Nakonechnyi, S. I. (1996). Ryzyk u menedzhmenti [Risk in management]. Kyiv, TOV "Borysfen-M". 336 p. [in Ukrainian].

6. Harkusha, V. O. (2020). Metodychnyi pidkhid do otsinky ryzykiv informatsiinoi bezpeky pidpryiemstva [A methodological approach to assessing enterprise information security risks]. *Pryazovskyi ekonomichnyi visnyk – Pryazovsky Economic Bulletin*, Issue 2(19), pp. 85-90. DOI: https://doi.org/10.32840/2522-4263/2020-2-15 [in Ukrainian].

7. Hrabar, N. S. (2019). Informatsiina bezpeka v umovakh stanovlennia hlobalnoho informatsiinoho suspilstva [Information security in the context of the global information society]. *Derzhavne upravlinia: udoskonalennia ta rozvytok – Public administration: improvement and development*, 7. Retrieved from http://www.dy.nayka.com.ua/?op=1&z=1461. DOI: https://doi.org/10.32702/2307-2156-2019.7.21 [in Ukrainian].

8. Zaverbnyj, A. S., Pushak, Ya. Ya. (2022). Problemy ta potentsiini mozhlyvosti rozvytku IT-sfery v Ukraini za umov aktyvizuvannia protsesiv intehruvannia do mizhnarodnoho rynku: upravlinskyi aspekt [Problems and potential opportunities for the development of the IT sphere in Ukraine under the conditions of intensifying the processes of integration into the international market: a managerial aspect]. *Visnyk ekonomichnoi nauky Ukrainy,* 1(42), pp. 110-113 DOI: https://doi.org/10.37405/1729-7206.2022.1(42).110-113 [in Ukrainian].

9. Zaverbnyj, A. S. (2022). Komunikatsiini stratehii: problemy ta perspektyvy formuvannia i realizuvannia za umov yevrointehruvannia [Communication strategies: problems and prospects of formation and implementation in the context of European integration]. *Innovation and Sustainability*, 1, pp. 13-19. DOI: https://doi.org/10.31649/ins.2022.1.13.19 [in Ukrainian].

10. Tolubko, V. (Ed.). (2004). Informatsiina bezpeka derzhavy u konteksti protydii informatsiinym viinam [Information security of the state in the context of counteracting information wars]. Kyiv, NAOU [in Ukrainian].

11. Karpovych, I. M., Hladka, O. M., Nakonechna, Yu. A. (2020). Analiz ryzykiv bezpeky informatsiinoi systemy IT-pidpryiemstva [Security risk analysis of the IT enterprise information system]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: tekhnichni nauky – Academic notes of TNU named after V. I. Vernadskyi. Series: technical sciences*, Vol. 31 (70), no. 5, pp. 69-74. DOI https://doi.org/10.32838/2663-5941/2020.5/12 [in Ukrainian].

12. Koterlin, I. B. (2022). Informatsiina bezpeka v umovakh voiennoho stanu u aspekti zabezpechennia

informatsiinykh prav ta svobod [Information security in martial law in terms of ensuring information rights and freedoms]. *Aktualni problemy vitchyznianoi yurysprudentsii – Actual problems of domestic jurisprudence*, 1, pp. 150-155. DOI: https://doi.org/10.32782/392257 [in Ukrainian].

13. Kuzmin, O. Ye., Heorhiadi, N. H. (2006). Formuvannia i vykorystannia informatsiinoi systemy upravlinnia ekonomichnym rozvytkom pidpryiemstva [Formation and use of information management system of economic development of the enterprise]. Lviv, Lvivska politekhnika [in Ukrainian].

14. Litvinchuk, I. S., Korchomnyi, R. O., Korshun, N. V., Vorokhob, M. V. (2020). Pidkhid do otsiniuvannia ryzykiv informatsiinoi bezpeky dlia avtomatyzovanoi systemy klasu «1» [An approach to assessing information security risks for a class 1 automated system]. *Kiberbezpeka: osvita, nauka, tekhnika – Cyber security: education, science, technology*, 2(10), pp. 98-112. DOI: https://doi.org/10.28925/2663-4023.2020.10.98112 [in Ukrainian].

15. Ozarko, K. S., Andrukhiv, T. V. (2022). Osoblyvosti formuvannia optymalnykh orhanizatsiinykh struktur upravlinnia IT-biznesom yak element yoho informatsiinoi bezpeky [Features of the formation of optimal organizational dtructures of IT-business management as an element of its information security]. *Ekonomika ta suspilstvo – Economy and society*, 43. Retrieved from https://economyandsociety.in.ua/ index.php/journal/article/view/1709. DOI: https://doi.org/10.32782/2524-0072/2022-43-21 [in Ukrainian].

16. Cherednychenko, A. O. (2013). Metody zabezpechennia zakhystu pidpryiemstv vid ekonomichnoho shpyhunstva [Methods of protecting enterprises from economic espionage]. *Visnyk ekonomiky transportu i promyslovosti – Herald of the economy of transport and industry*, 42, pp. 335-338 [in Ukrainian].

17. Shandrivska, O. Ye., Shynkarenko, N. V. (2020). Prykladna otsinka ryzykiv u systemi zabezpechennia bezpeky sotsialno-ekonomichnykh protsesiv u kiberprostori [Applied risk assessment in the system of ensuring the security of socio-economic processes in cyberspace]. *Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia "Problemy ekonomiky ta upravlinnia" – Bulletin of the Lviv Polytechnic National University. Series "Problems of economics and management"*, 2(8), pp. 94-105. DOI: https://doi.org/10.23939/ semi2020.02.094 [in Ukrainian].

18. Bezpartochna, O., Pushak, Ya., Trushkina, N. (2022). Current issues of information security management during the state of martial. *Current issues of security management during martial law*: scientific monograph. (pp. 8-19). Košice, Vysoká škola bezpečnostného manažérstva v Košiciach.

19. Bezchasnyi, O., Khobta, V., Pushak, Ya., Kotkalova-Litvin, I., Dorovska, I. (2018). Modeling of control stability of communication channels in development management conditions. *Finansovo-kredytna diialnist: problemy teorii ta praktyky – Financial and credit activity: problems of theory and practice*, Vol. 4, no. 27, pp. 282-295.

Стаття надійшла до редакції 31.05.2023

Формат цитування:

Озарко К. С., Копитко С. Б. Особливості функціонального підходу до управління інформаційною безпекою підприємств за кризових умов. *Вісник економічної науки України*. 2023. № 1 (44). С. 45-49. *DOI: https://doi.org/10.37405/1729-7206.2023.1(44).45-49*

Ozarko, K. S., Kopytko, S. B. (2023). Peculiarities of the Functional Approach to the Management of Information Security of Enterprises in Crisis Conditions. *Visnyk ekonomichnoi nauky Ukrainy*, 1 (44), pp. 45-49. *DOI: https://doi.org/10.37405/1729-7206.2023.1(44).45-49*