

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

Онищенко С. В., доктор економічних наук, професор, професор кафедри фінансів, банківського бізнесу та оподаткування, Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава, Україна

e-mail: s07onyshchenko@gmail.com

ORCID: 0000-0002-6173-4361

Білько С. С., здобувач третього (наукового) рівня вищої освіти, Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава, Україна

e-mail: stanislav_bilko@ukr.net

ORCID: 0000-0003-0259-4482

***Анотація.** Стаття присвячена обґрунтуванню концептуальних засад інформаційної безпеки національної економіки та систематизації загроз інформаційній безпеці України як базису для розроблення превентивних заходів їх запобігання та мінімізації деструктивного впливу. Відмічено відсутність єдиного підходу до трактування поняття «інформаційна безпека». Запропоновано досліджувати інформаційну безпеку з двох аспектів: як самостійний елемент національної безпеки країни та як інтегровану складову економічної безпеки. Обґрунтовано, що детермінантою формування інформаційної безпеки є загрози та їх деструктивні впливи на національну економіку та національну безпеку країни в цілому. Систематизовано та удосконалено багаторівневу класифікацію загроз інформаційній безпеці національної економіки з метою подальшого формування напрямів запобігання, протидії, мінімізації негативного впливу загроз.*

***Ключові слова:** пзагрози, інформаційна безпека національної економіки, національні інтереси, систематизація, класифікація.*

THREATS TO THE INFORMATION SECURITY OF THE NATIONAL ECONOMY

Onyshchenko Svitlana, Doctor of Economics, Professor, Professor of the Department of Finance, Banking and Taxation, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

e-mail: s07onyshchenko@gmail.com

ORCID: 0000-0002-6173-4361

Bilko Stanislav, applicant of the third (scientific) level of higher education, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

e-mail: stanislav_bilko@ukr.net

ORCID: 0000-0003-0259-4482

***Abstract.** The article is devoted to the substantiation of the conceptual foundations of information security of the national economy and systematization of threats to information security of Ukraine as a basis for the development of preventive measures to prevent and minimize their destructive impact. The lack of a single approach to the interpretation of the concept of "information security" is noted. It is proposed to study information security from two aspects: as an independent element of national security and as an integrated component of economic security. It is substantiated that the determinant of information security formation is threats and their destructive impact on the national economy and national security of the country as a whole. The multilevel classification of threats to the information security of the national economy has been systematized and improved in order to further form directions for prevention, countermeasures, and minimization of the negative impact of threats.*

***Keywords:** threats, information security of the national economy, national interests, systematization, classification.*

JEL Classification: B410; E600; H110; H560.

Постановка проблеми. Процеси глобалізації та цифровізації спричинили виникнення нових ризиків і загроз функціонуванню національних економік та виявили критичні проблеми в інформаційній сфері. Інформаційні війни, інформаційний тероризм, масштабні кібератаки – ці деструктивні феномени заповнили сучасний світ. Лише за умови формування безпекоорієнтованого інформаційного середовища можливо забезпечити захист економічних інтересів, стійкість національної економіки та зміцнення національної безпеки в цілому. Водночас забезпечення інформаційної безпеки національної економіки має ґрунтуватися на своєчасній ідентифікації реальних і потенційних загроз, що є базисом їх стримування, протидії та мінімізації негативного впливу. Цим пояснюється необхідність

систематизації загроз інформаційній безпеці.

Аналіз останніх досліджень і публікацій. Проблема забезпечення інформаційної безпеки, в тому числі у контексті підтримки національної безпеки країни, широко актуалізується у працях зарубіжних та вітчизняних науковців. Наукові дослідження присвячені обґрунтуванню концептуальних засад та механізму забезпечення інформаційної безпеки [1–3], розробленню напрямів упередження й мінімізації загроз [4–6], правового забезпечення та управління кібербезпекою й інформаційною безпекою в цілому як на національному, так і на міжнародному рівні [7–9].

Відокремлення невирішених раніше частин загальної проблеми. ПВодночас в умовах військової агресії російської федерації, зростання викликів у інформаційному та кіберпросторі питання ідентифікації нових загроз інформаційній безпеці національної економіки та напрямів їх мінімізації потребує подальшого дослідження.

Метою дослідження є обґрунтування концептуальних засад інформаційної безпеки національної економіки та систематизація загроз інформаційній безпеці України.

Основний матеріал. Концептуальні положення інформаційної безпеки закріплені у Стратегії інформаційної безпеки, відповідно до якої інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [10].

Водночас у дослідженнях науковців-економістів поняття «інформаційна безпека» розглядається з позиції захисту національних економічних інтересів та національної економіки. Важливість та необхідність забезпечення інформаційної безпеки обґрунтовується співвідношенням витрат на впровадження й експлуатацію систем інформаційної безпеки і фінансових втрат у випадку реалізації загроз. Роль інформаційної безпеки визначається здатністю засобів та методів інформаційної безпеки, як важливої компоненти економічної безпеки на всіх рівнях, протистояти загрозам економічної цілісності держави.

Враховуючи вищезазначене, інформаційну безпеку правомірно розглядати з двох аспектів: як самостійний елемент національної безпеки країни та як інтегровану складову економічної безпеки [11, 12].

Інформаційна безпека в умовах воєнного стану, безумовно, є основною детермінантою забезпечення стабільного функціонування національної економіки України. Необхідність формування інформаційної безпеки зумовлюється наявністю загроз та їх деструктивними наслідками. З метою своєчасного виявлення, унеможливлення реалізації, мінімізації негативного впливу загроз інформаційній безпеці необхідним є їх оперативна ідентифікація.

Систематизацію загроз інформаційній безпеці національної економіки доцільно здійснювати з урахуванням чинного законодавства.

Стратегією національної безпеки України (введена в дію Указом Президента України від 14 вересня 2020 року № 392/2020) у переліку поточних та прогнозованих загроз національній безпеці і національним економічним інтересам визначено стрімкий розвиток інформаційних технологій, що сприяє поширенню таких явищ як злочинність у кіберпросторі, деструктивна пропаганда в інформаційному середовищі; відсутність цілісної інформаційної політики держави; слабкість системи стратегічних комунікацій; несанкціоновані втручання кіберхарактеру у функціонування об'єктів критичної інфраструктури [13]. Стратегією інформаційної безпеки (введена в дію Указом Президента України від 28 грудня 2021 року № 685/2021) визначається поняття «інформаційна загроза» як потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні [10]. Цим законодавчим актом загрози інформаційній безпеці розмежовуються за рівнем реалізації на глобальні та національні. У Стратегії кібербезпеки України (введена в дію Указом Президента України від 26 серпня 2021 року № 447/2021) виокремлено такі види загроз, як гібридна агресія (кібервійна), кібертероризм, кіберзлочинність, кібершпиунство

[14].

Систематизація загроз інформаційній безпеці згідно з чинним законодавством представлена на рисунку 1.

Аналізуючи Стратегію національної безпеки України, правомірно відмітити, що описані загрози можна розділити на дві групи: зовнішні та внутрішні. Проте варто зауважити, що зазначений перелік загроз не може вважатися вичерпним та константним. В умовах посилення процесів глобалізації та цифровізації, загострення військових конфліктів в Україні і світі загрози трансформуються та модифікуються. У зв'язку з динамічними умовами функціонування національної економіки та світової економічної системи в цілому постійно змінюється і величина впливу внутрішніх та зовнішніх загроз інформаційній безпеці. Оскільки можливості мінімізації внутрішніх загроз є значно вищими, а створюються вони виключно органами державної влади та суспільством, то пріоритетним завданням є побудова стійкої національної інформаційної інфраструктури.

Згідно зі Стратегією інформаційної безпеки виокремлено глобальні та національні загрози інформаційній безпеці України, які впливають на інтереси особи, суспільства та держави. Водночас у Стратегії не враховано інтереси економічних суб'єктів (фізичних осіб – підприємців, домогосподарств, підприємств). Хоча саме ця категорія несе найбільші фінансові втрати у випадку реалізації загроз інформаційній безпеці, що безпосередньо впливає на національну економіку України.

У Стратегії кібербезпеки хоч і наводиться найкоротший перелік загроз, але водночас враховується їх деструктивний вплив на національну економіку України та світову економіку в цілому. Виокремлені кібервійна, кібертероризм, кібершпигунство, кіберзлочинність також потребують деталізації. Зокрема, у рамках кіберзлочинності можна виділяти реалізацію таких загроз як інсайдерські атаки, фішинг, цільові кібератаки та DDoS-атаки.

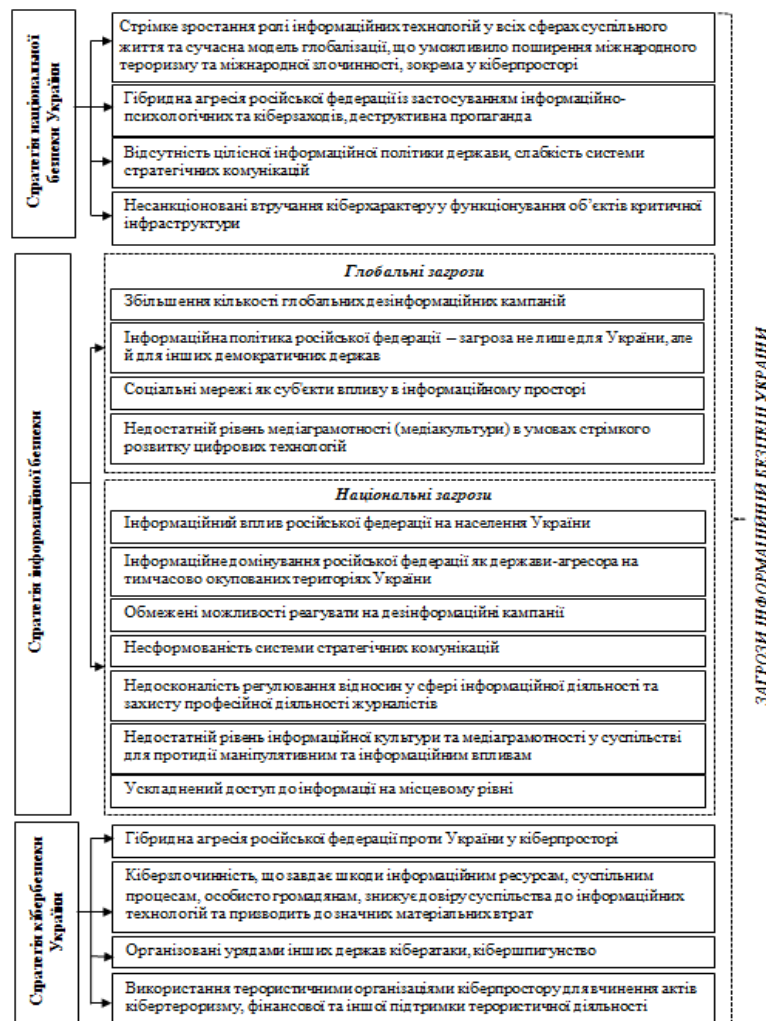


Рис. 1. Систематизація загроз інформаційній безпеці України

Джерело: складено авторами за матеріалами [10, 13, 14]

Аналіз доктринальних, енциклопедичних та наукових джерел дозволив розширити класифікацію загроз інформаційній безпеці національної економіки. Зокрема, за джерелами походження правомірно виділити комунікативні загрози та технологічні загрози. До першої групи належать дезінформаційні кампанії, деструктивний інформаційний вплив на громадян через соціальні мережі, обмеження свободи слова тощо. Друга група загроз інформаційній безпеці передбачає заподіяння шкоди національній економіці та національній безпеці України через несанкціоноване втручання у діяльність інформаційних систем [15, 16].

За спрямуванням загроз інформаційній безпеці науковці виокремлюють: загрози порушення конфіденційності (неправомірний доступ до інформації, «витік» інформації з обмеженим доступом, неправомірне використання якої спричинить значні втрати власника, в тому числі фінансові); загрози порушення цілісності (неправомірна зміна даних, модифікація інформації, що зберігається в інформаційній системі), загрози порушення доступності (реалізація яких унеможливує чи ускладнює доступ до інформаційних ресурсів) [17, 18].

В аспекті формування та забезпечення інформаційної безпеки національної економіки найбільшої вагомості набуває класифікація загроз на реальні та потенційні. У випадку реальної загрози дестабілізація об'єкту впливу є неминучою та не обмежена часом і простором. Реалізація потенційних загроз можлива за певних умов інформаційного середовища, наявності вразливості інформаційної системи, низького чи недостатнього рівня захищеності інформаційних ресурсів та ін.

З урахуванням філософської концепції загальної об'єктивної зумовленості явищ і процесів, за ступенем детермінізму можна виділити: випадкові загрози, які можуть бути реалізовані або можуть не відбутися (наприклад, загроза DDoS-атаки на суб'єкт господарювання); закономірні загрози, які характеризуються стійким, повторюваним характером та зумовлені об'єктивними умовами розвитку цифровізації та посилення напруги на світовій арені (кібератаки хакерських угруповань на офіційні сайти державних органів влади) [19, 20].

Класифікацію загроз інформаційній безпеці доцільно також доповнити розподілом за об'єктами, тобто на що безпосередньо спрямовані дестабілізуючі дії: макрорівень (держава), мезорівень (регіон, галузь), мікрорівень (підприємство), нанорівень (особа, домогосподарство, суб'єкт господарювання). Такий розподіл дасть можливість визначити важелі та інструменти побудови ефективної системи захисту інформаційних ресурсів та підвищення інформаційної безпеки на усіх зазначених рівнях.

Систематизована та удосконалена багаторівнева класифікація загроз інформаційній безпеці національної економіки дозволяє ідентифікувати загрози та вживати превентивних заходів. Водночас вона є умовною, оскільки в умовах стрімкого цифрового розвитку загрози швидко модифікуються та трансформуються.

Доцільність використання удосконаленої класифікації при дослідженні загроз інформаційній безпеці підтверджується тим, що виокремлення реальних та потенційних загроз, авторський розподіл загроз за об'єктами є базисом для формування напрямів запобігання, протидії, мінімізації негативного впливу від їх реалізації. Крім того, систематизація загроз за наведеними ознаками у нормативно-правових актах дозволить підвищити їх регуляторний вплив та сформувати безпекоорієнтоване інформаційне середовище в Україні.

Висновки. На основі проведеного дослідження правомірно зробити наступні висновки.

1. В умовах поглиблення процесів глобалізації та цифровізації, які спричинили появу нових ризиків і загроз функціонуванню національних економік та виявили критичні проблеми в інформаційній сфері, зміцнення інформаційної безпеки є необхідною умовою захисту національних економічних інтересів.

2. Детермінантою формування інформаційної безпеки є загрози та їх деструктивні впливи на національну економіку та національну безпеку країни в цілому. Потреба підтримки національної економіки в умовах воєнного стану передбачає необхідність забезпечення її функціонування на засадах інформаційної захищеності. З метою своєчасного виявлення, унеможливлення реалізації, мінімізації негативного впливу загроз інформаційній безпеці необхідним є їх оперативна ідентифікація.

3. Проведений аналіз чинного законодавства у сфері інформаційної безпеки підтвердив відсутність ґрунтовної систематизації загроз. Удосконалена багаторівнева класифікація загроз інформаційній безпеці національної економіки може стати базисом для формування напрямів запобігання, протидії, мінімізації негативного впливу від їх реалізації.

Список літератури

1. Яровенко Г. М. Канонічний аналіз взаємозв'язку інформаційної безпеки та соціо-економіко-політичного розвитку країни. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. 2020. № 31. С. 160–167.
2. Барановський О. І. Філософія безпеки: монографія: у 2 т. Т. 1: Основи економічної і фінансової безпеки економічних агентів. Київ: УБС НБУ, 2014. 831 с.
3. Varnalii Z., Onyshchenko S., Maslii O., Filonych O. Prerequisites for Shadowing and Corruption in the Construction Business of Ukraine. In: Onyshchenko V., Mammadova G., Sivitska S., Gasimov A. (eds) Proceedings of the 3rd International Conference on Building Innovations. ICBI 2020. Lecture Notes in Civil Engineering. Springer, Cham. 2020. Volume 181, 793–808.
4. Литвиненко О. Інформаційна складова в сучасній гібридній війні проти України: виклики та загрози. Українознавчий альманах. 2017. Випуск 19. С. 171–174.
5. Yarovenko H. Evaluating the threat to national information security. Problems and Perspectives in Management. 2020. Vol. 18, Issue 3. P. 195–210.
6. Glushko A. D., Yanko A. S. Optimal reservation of data in the system of residual classes in the direction of ensuring information security of the national economy. Economics and Region. 2019. No. 4 (75). P. 20–28. [https://doi.org/10.26906/eip.2019.4\(75\).1814](https://doi.org/10.26906/eip.2019.4(75).1814)
7. Kaewkamol Pitakdumrongkit. What causes changes in international governance details?: An economic security perspective. Review of International Political Economy. 2020. Volume 29, Issue 2, P. 399–424. <https://doi.org/10.1080/09692290.2020.1819371>
8. Harlan Koff. Reconciling Competing Globalizations through Regionalisms? Environmental Security in the Framework of Expanding Security Norms and Narrowing Security Policies. Globalization. 2016. Volume 13, Issue 6. P. 664–682. <https://doi.org/10.1080/14747731.2015.1133044>
9. Slayton R. Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties. Science, Technology, & Human Values. 2021. 46(1). P. 81–111. <https://doi.org/10.1177/0162243919901159>
10. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення 06.12.2022).
11. Onyshchenko S., Yanko A., Hlushko A., Sivitska S. Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. International Journal of Management. 2020. 11(12). P. 1709–1726. <https://doi.org/10.34218/IJM.11.12.2020.157>
12. Онищенко С. В., Глушко А. Д. Концептуальні засади інформаційної безпеки національної економіки в умовах діджиталізації. Соціальна економіка. ХНУ, 2020. Вип. 59. С. 14–24.
13. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037> (дата звернення 06.12.2022).
14. Стратегії кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: <https://www.president.gov.ua/documents/4472021-40013> (дата звернення 06.12.2022).
15. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України : дисертація ... д-ра юрид. наук : 12.00.07. ДВНЗ «Ужгородський національний університет», Ужгород, 2019. 487 с.
16. Onyshchenko S., Hlushko A., Maslii O. Threats to information security of Ukraine in the conditions of digitalization. The world of science and innovation. Proceedings of the 12th International scientific and practical conference (July 1-3, 2021). Cognum Publishing House. London, United Kingdom. 2021. Pp. 69-73. (374 p.)
17. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с.
18. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навчальний довідник. Київ, ООО «Д.В.К.» 2004. 508 с.
19. Шемчук В. В. Загрози інформаційній безпеці: проблеми визначення та подолання. Експерт: парадигми юридичних наук і державного управління. 2020. № 1(7). С. 285–296. [https://doi.org/10.32689/2617-9660-2020-1\(7\)-285-296](https://doi.org/10.32689/2617-9660-2020-1(7)-285-296)

20. Онищенко С. В., Глушко А. Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. Економіка і регіон. 2022. № 1 (84). С. 13–20.

References

1. Horiachyj Yu. & Andrijchenko Zh. (2018). The essence of the concept of «financial risk» of I. Yarovenko, G. M. (2020). Canonical analysis of the relationship between information security and socio-economic and political development of the country. *Naukovyy visnyk Uzhhorodskoho natsionalnoho universytetu. Seriya: Mizhnarodni ekonomichni vidnosyny ta svitove hospodarstvo*, 31, 160–167. [In Ukrainian].
2. Baranovsky, O. I. (2014). *Filosofia bezpeky: monohrafiya*. K.: UB NBU. [In Ukrainian].
3. Varnalii, Z., Onyshchenko, S., Maslii, O., Filonych, O. (2020). Prerequisites for Shadowing and Corruption in the Construction Business of Ukraine. In: Onyshchenko V., Mammadova G., Sivitska S., Gasimov A. (eds) *Proceedings of the 3rd International Conference on Building Innovations. ICBI 2020. Lecture Notes in Civil Engineering*. Springer, Cham. Volume 181, 793–808.
4. Lytvynenko, O. (2017) Information component in the modern hybrid war against Ukraine: challenges and threats. *Ukrayinoznavchyy al'manakh*. 19, 171–174. [In Ukrainian].
5. Yarovenko, H. (2020). Evaluating the threat to national information security. *Problems and Perspectives in Management*. 18, 3, 195–210
6. Glushko, A. D., Yanko, A. S. (2019). Optimal reservation of data in the system of residual classes in the direction of ensuring information security of the national economy. *Economics and Region*. 4 (75), 20–28. DOI: [https://doi.org/10.26906/eip.2019.4\(75\).1814](https://doi.org/10.26906/eip.2019.4(75).1814)
7. Kaewkamol, Pitakdumrongkit (2020). What causes changes in international governance details?: An economic security perspective. *Review of International Political Economy*, 29, 2, 399–424. DOI: <https://doi.org/10.1080/09692290.2020.1819371>
8. Harlan, Koff (2016). Reconciling Competing Globalizations through Regionalisms? *Environmental Security in the Framework of Expanding Security Norms and Narrowing Security Policies*. *Globalization*, 13, 6, 664–682. DOI: <https://doi.org/10.1080/14747731.2015.1133044>
9. Slayton, R. (2021). Governing Uncertainty or Uncertain Governance? *Information Security and the Challenge of Cutting Ties*. *Science, Technology, & Human Values*, 46(1), 81–111. DOI: <https://doi.org/10.1177/0162243919901159>
10. Information security strategy: Decree of the President of Ukraine of December 28, 2021 No. 685/2021. Retrieved from <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (accessed December, 6, 2022). [In Ukrainian].
11. Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S. (2020). Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. *International Journal of Management*, 11(12), 1709–1726. DOI: <https://doi.org/10.34218/IJM.11.12.2020.157>
12. Onyshchenko, S., Hlushko, A. (2020). Kontseptualni zasady informatsiinoi bezpeky natsionalnoi ekonomiky v umovakh didzhytalizatsii [Conceptual principles of information security of the national economy in conditions of digitalization]. *Social economy: Science. profession. view*. Kh.: KhNU, 59, 14–24. DOI: <https://doi.org/10.26565/2524-2547-2020-59-02> [In Ukrainian].
13. National Security Strategy of Ukraine: Decree of the President of Ukraine of 14 September 2020 No. 392/2020. Retrieved from <https://www.president.gov.ua/documents/3922020-35037> (accessed December, 6, 2022). [In Ukrainian].
14. Cybersecurity strategies of Ukraine: Decree of the President of Ukraine of August 26, 2021 No. 447/2021. Retrieved from <https://www.president.gov.ua/documents/4472021-40013> (accessed December, 6, 2022). [In Ukrainian].
15. Tkachuk, T. Y. Legal support of information security in the context of European integration of Ukraine: dissertation ... Doctor of Law: 12.00.07. Uzhhorod National University, Uzhhorod, 2019. 487 c. [In Ukrainian].
16. Onyshchenko, S., Hlushko, A., Maslii, O. (2021). Threats to information security of Ukraine in the conditions of digitalization. *The world of science and innovation. Proceedings of the 12th International scientific and practical conference (July 1–3, 2021)*. Cognum Publishing House. London, United Kingdom, 69–73.
17. Lipkan, V. A., Maksymenko, Y. E., Zhelihovskyi, V. M. (2006). *Information security of Ukraine in the context of European integration: Study guide*. KYIV: KNT. [In Ukrainian].
18. Bogush V. M., Kryvutsa, V. G., Kudin, A. M. (2004). *Information security: Terminological*

training guide. Kyiv, LLC "D.V.K.". [In Ukrainian].

19. Shemchuk, V. V. (2020). Threats to information security: problems of definition and overcoming. *Ekspert: paradyhmy yurydychnykh nauk i derzhavnoho upravlinnya*, 1(7), 285–296. DOI: [https://doi.org/10.32689/2617-9660-2020-1\(7\)-285-296](https://doi.org/10.32689/2617-9660-2020-1(7)-285-296) [In Ukrainian].

20. Onyshchenko, S. V., Glushko, A. D. (2022). Analytical dimension of cybersecurity of Ukraine in the context of growing challenges and threats. *Ekonomika i rehion*, 1 (84), 13–20. [In Ukrainian].

Стаття надійшла до редакції 19.12.2022

Прийнята до публікації 23.12.2022