DOI: *https://doi.org/10.37405/1729-7206.2025.1(48).187-192*

УДК 005.8:338.246.8:351.862

Катерина Сергіївна Озарко
канд. екон. наук, доц.
ORCID 0000-0002-1452-0686
e-mail: kateryna.ozarko@gmail.com,
Державний університет інтелектуальних технологій і зв'язку, м. Одеса

Юрій Володимирович Опотяк
канд. техн. наук, доц.
ORCID 0000-0001-9889-4177
e-mail: yurii.v.opotiak@lpnu.ua
Національний університет «Львівська політехніка»,

Тарас Васильович Андрухів
канд. техн. наук
директор Львівської філії АТ "Укртелеком"
ORCID 0000-0001-7597-2435
e-mail: tandrukhiv@ukrtelecom.ua,
Державний університет інтелектуальних технологій і зв'язку, м. Одеса

ПРОБЛЕМИ І ПОТЕНЦІЙНІ МОЖЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БІЗНЕСУ В УМОВАХ ВОЄННОГО СТАНУ

Постановка проблеми. Тривалі воєнні дії на території України (починаючи із 2014 р.) спричинили масштабні виклики для національного бізнесу. Зокрема це стосується сфери інформаційної безпеки. Збільшення кібератак із боку агресора, спроби несанкціонованого доступу до корпоративних даних, порушення комунікаційної інфраструктури, ризики втрати критичних інформаційних ресурсів вимагають від вітчизняних підприємств оперативного реагування, підсилення рівня цифрового захисту. За вказаних умов саме інформаційна безпека перетворюється зі технічного аспекту діяльності на один із ключових факторів/чинників забезпечення стабільності, конкурентоспроможності, навіть простого виживання бізнесу.

Надійна система захисту стає основою для безперервності, систематичності бізнес-процесів, збереження репутації, захисту комерційної, персональної інформації тощо. У період війни, окрім вищезазначеного, значно зростає роль інформаційного середовища в управлінні ризиками, прийнятті стратегічних управлінських рішень, забезпеченні взаємодії із державними органами, партнерами (зокрема міжнародними), клієнтами тощо. Відповідно, відсутність належного рівня інформаційної безпеки може призводити до серйозних фінансових, правових, іміджевих та інших втрат.

Тому дослідження питань забезпечення інформаційної безпеки бізнесу за умов воєнного стану надзвичайно актуальне, має практичне значення для моніторингу, аналізу, оцінювання ризиковості та розроблення ефективних підходів щодо запобігання і протидії загрозам у цифровому середовищі.

Метою статті є дослідження проблем, потенційних можливостей забезпечення інформаційної безпеки бізнесу в умовах воєнного стану.

Аналіз останніх досліджень та публікацій. Проблематика забезпечення інформаційної безпеки бізнесу знайшла відображення у працях таких вчених як: В. Бакай [1, с. 32-35], О. Безперточна [21, с. 8-19], С. Білько [2, с. 58-77], В. Васильців [3], І. Деха [4, с. 151-159], В. Дубницький [4, с. 151-159], А. Завербний [6, с. 110-113], В. Захарченко [7, с. 63-66], Н. Леоненко [9], І. Новаківський [12], С. Онешко [7, с. 63-66], О. Панченко [16, с. 32-38], Л. Панченко [16, с. 32-38], О. Поступна [9], Я. Пушак [6, с. 110-113; 21, с. 8-19; 22, с. 26-31], В. Сусіденко [18], О. Сусіденко [18], Н. Трушкіна [21, с. 8-19; 22, с. 26-31] та ін.

Зазначені проблеми значно підсилилися у воєнний період. Дослідження за умов воєнного стану провели наступні науковці: Л. Браілко [17, с. 121-127], А. Завербний [5, с. 13-21], І. Котрелін [8, с. 150-155], Л. Мазуренко [10], О. Назаренко [11, с. 64-71], С. Обрембальський [20, с. 1-11], К. Озарко [11, с. 64-71], Д. Смотрич [17, с. 121-127], В. Топалов [19, с. 157-161], Л. Чистоклетов [20, с. 1-11] та ін.

Виклад основного матеріалу дослідження. За умов воєнного стану, спричиненого масштабним вторгненням росії в Україну, питання інформаційної безпеки бізнесу набули особливої актуальності. Бізнес-структури стали не тільки економічною опорою для країни, але й важливим елементом цифрового фронту. Відповідно, уразливість інформаційних систем може призводити до збоїв у логістиці, фінансах, управлінні персоналом тощо. Це загрожуватиме як окремо взятим

підприємствам, так і національній економіці у цілому. Забезпечення необхідного рівня інформаційної безпеки бізнесу України стало однією із умов його стабільного, гармонійного функціонування та ефективного розвитку. А за умов динамічної цифровізації, глобального інтегрування бізнесу ефективне управління інформаційною безпекою підприємств потребує формування та реалізації системного підходу. Вказаний підхід повинен включати розроблення і реалізацію політик безпеки, запровадження інноваційних технологій захисту всіх видів даних (інформації), постійне здійснення моніторингу загроз, навчання персоналу тощо. Особлива ж увага має бути присвячена адаптуванню національних підприємств до сучасних стандартів кіберзахисту, які відповідають чинним міжнародним вимогам [18, с. 157-159]. У зв'язку із геополітичною нестабільністю, зростанням кількості кібератак (рис. 1), зокрема й на критичну інфраструктуру нашої країни, вітчизняний бізнес стикається із підвищеною ризиковістю економічних втрат, порушенням конфіденційності даних, репутаційними ризиками тощо [13; 15; 19, с. 157-159]. Це потребуватиме формування системного підходу до управління інформаційними ризиками, інтегруванні сучасних засобів захисту, побудові культури кібербезпеки у всіх рівнях управління [19, с. 158-159].

Кількість кіберзлочинів, спрямованих саме на вітчизняний бізнес постійно зростає (рис. 1). Це засвідчує посилення активності кіберзловмисників та зростання вразливості корпоративного сектору. Підвищення рівня кіберзагроз обумовлюється недостатньо розвиненими, недостатньо дієвими системами кіберзахисту, недотриманням засад інформаційної безпеки працівниками, відсутністю резервних стратегій для реагування на інциденти. Відповідно, це може призводити до економічних втрат для бізнесу, підривати довіру споживачів, знижувати репутацію суб'єктів господарювання та ускладнювати підприємницьку діяльність [19, с. 158].

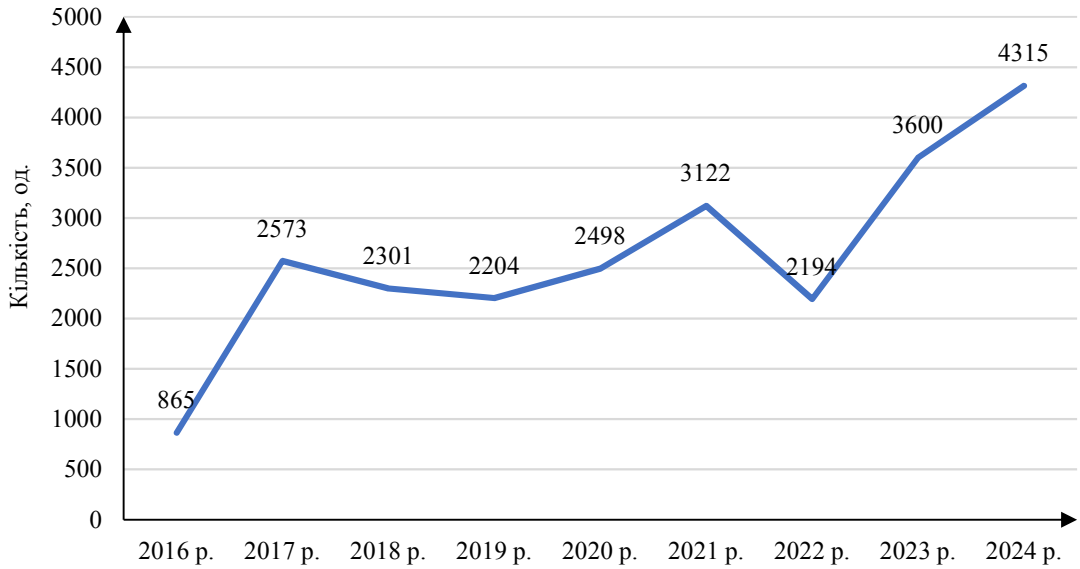

Рис. 1. Динаміка кіберзлочинів в Україні за період 2016-2024 рр. [15]

Аналізування складних і комплексних сучасних умов господарювання дозволило виявити наступні основні проблеми забезпечення інформаційної безпеки вітчизняного бізнесу:

– постійне нарощування кіберзагроз (Період воєнного стану охарактеризувався значним приростом кількості кібератак, їх рівнем складності (див. рис. 1). Найчастішими випадками були наступні: фішинг, DDoS-атаки, шкідливе програмне забезпечення, злам хмарних сервісів);

– недостатній рівень кібергігієни персоналу вітчизняних бізнес-структур (багато співробітників вітчизняних організацій, працюючи у віддаленому режимі, перебуваючи у зонах активних бойових дій, ускладнили систему контролювання за дотриманням правил безпеки під час роботи із інформацією. Це підвищило рівень ризиковості несанкціонованого доступу до внутрішніх систем);

– обмеженість фінансових ресурсів вітчизняних бізнес-структур (за умов кризи бізнес переважно зорієнтований на збереження операційної діяльності, тому інвестування до сфери інформаційної безпеки відходить на другий план. Відсутність коштів для оновлення програмного забезпечення, ліцензії, апаратні засоби створюють так звані критичні «дірки» в економічній безпеці вітчизняного бізнесу);

– відсутність чіткої інформаційної політики (багато вітчизняних підприємств, організацій не володіють формалізованими політиками інформаційної безпеки, не реалізують систематичні аудити, не формують планів для реагування на інциденти. Відповідно це призводить до хаотичних, неузгоджених та малоефективних дій у разі кібератаки) тощо.

У зв'язку зі зазначеними проблемами вітчизняний ринок кібербезпеки зріс вчетверо (рис. 2) протягом 2016-2024 рр. А згідно прогнозів, надалі зростатиме (вдвічі до 2029 р.) [13-15].

Також через високий рівень ймовірності пошкоджень сервісів та систем через російське вторгнення, український бізнес почав переносити IT-інфраструктури до хмарних сервісів (рис. 3) [14-15]. Відповідно, за повномасштабного вторгнення вітчизняний ринок хмарної безпеки (рис. 3) виріс втричі (до 1,7 млн доларів США) [15].

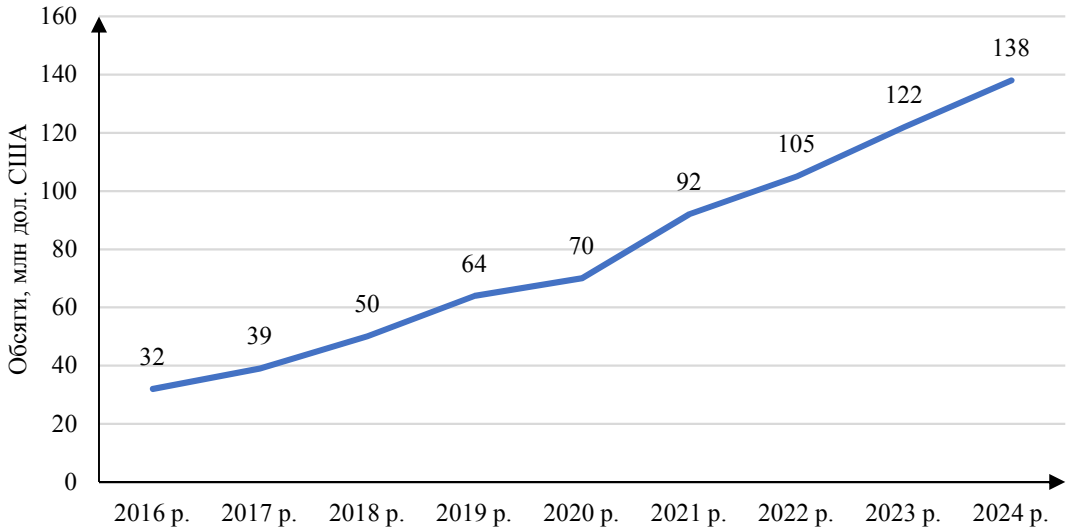

Рис. 2. Динаміка обсягів українського ринку кібербезпеки за період 2016-2024 рр. [13-15]

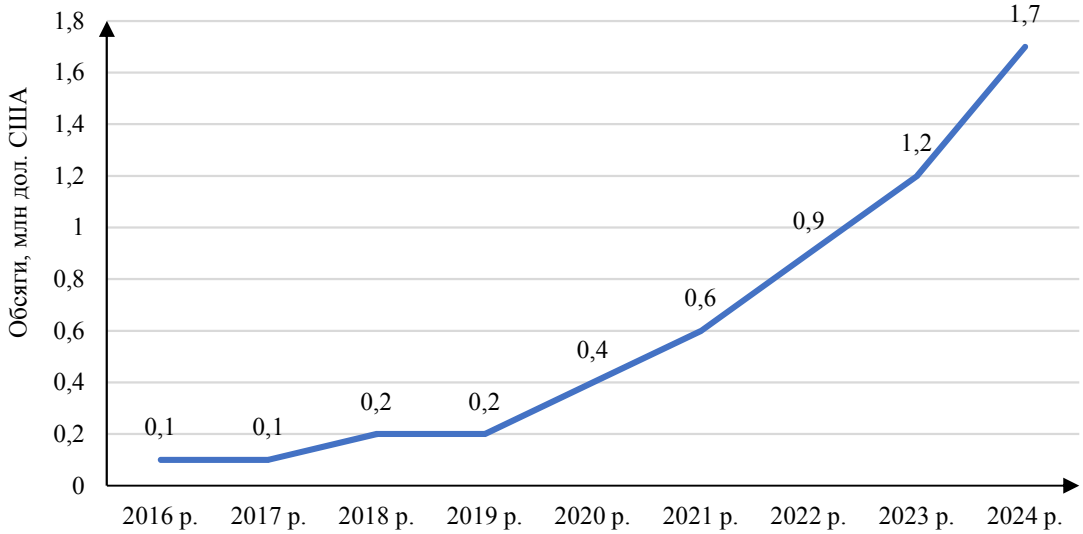

Рис. 3. Динаміка обсягів ринку хмарної безпеки в Україні за період 2016-2024 рр. [13; 15]

Причому ця динаміка (рис. 3) не враховує істотні обсяги вирішення проблем хмарної безпеки, які надаються вітчизняним державним органам безоплатно (в рамках міжнародної технічної допомоги) [15].

Задля зниження рівня інформаційної небезпеки вітчизняним підприємствам доцільно систематично проводити внутрішній аудит інформаційної безпеки; розробляти, затверджувати (за потреби реалізовувати) плани реагування на кіберінциденти; використовувати безпечні канали зв'язку, шифрування, VPN тощо; систематично оновлювати програмні забезпечення, антивірусні рішення; проводити навчання інформаційної безпеки для персоналу на постійній основі; залучати зовнішніх експертів для перевірки вразливостей.

Що стосується потенційних можливостей і напрямків зміцнення і розвитку інформаційної безпеки вітчизняних організацій, доцільно систематизувати їх наступним чином.

Формування і реалізація державної підтримки та здійснення системного нормативно-правового регулювання інформаційної безпеки бізнесу в умовах воєнного стану та післявоєнного відновлення української економіки. Слід зазначити, що уряд України активізував свою діяльність саме у сфері кібербезпеки (Національний координаційний центр кібербезпеки, CERT-UA, впровадження вимог до критичної інфраструктури). Вітчизняний бізнес зможе користуватися можливістю інтегрування із державними інструментами моніторингу, раннього сповіщення про атаки тощо.

Застосування хмарних рішень (динаміка відображена на рис. 3) із вбудованим захистом. Адже багато міжнародних хмарних платформ (Microsoft, AWS, Google тощо) надають українському бізнесу пільгові (деколи безкоштовні) пакети для доступу до безпечних сервісів із розширеним захистом. Саме це дозволятиме мінімізувати власні витрати із одночасним підвищенням рівня надійності інфраструктури.

Систематичне підвищення рівня інформаційної обізнаності працівників вітчизняних організацій. Навчання із кібергігієни, реагування на фішингові атаки, запровадження дворівневої авторизації, політик шифрування сприятиме значному зниженню інформаційних ризиків українського підприємництва. У період

воєнного стану це можливо реалізувати онлайн (за допомогою безкоштовних курсів, вебінарів, воркшопів тощо від провідних фахівців).

Реалізація міжнародного кооперування, сертифікування. Вітчизняні компанії можуть отримувати міжнародні сертифікати (ISO/IEC 27001, NIST, тощо), які крім того, що підвищуватимуть рівень їх інформаційної безпеки, ще й зміцнюватимуть репутацію їх бізнесу на глобальному ринку, полегшуючи вихід на експортні ринки за умов рецесії тощо.

Загальні висновки. Інформаційна безпека вітчизняного бізнесу за умов воєнного стану є не лише суто технічною проблемою. Сьогодні це стало стратегічним компонентом національної стійкості і безпечності. Попри серйозні виклики, вітчизняний бізнес має доступ до нових можливостей. Це стосується державної підтримки, використання міжнародної допомоги, технологічних інновацій. Реалізація цілеспрямованих дій у сфері розвитку та зміцнення інформаційної безпеки дозволить вітчизняному бізнесу не тільки уникнути втрат, але й стати підґрунтям для стабільного його розвитку у поствоєнний період.

Список використаних джерел

1. Бакай В. Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету*. 2020. № 4. Т. 1. С. 32-35. DOI: https://www.doi.org/10.31891/2307-5740-2020-284-4-5.

2. Білько С. Інформаційна та економічна безпека: оцінювання рівня та взаємозв'язку. *Науковий вісник Полісся*. 2022. Вип. 1 (24). С. 58-77. DOI: https://doi.org/10.25140/2410-9576-2022-1(24)-58-77.

3. Васильців В. Г. Організаційно-економічний механізм зміцнення економічної безпеки сектору інформаційних технологій: автореф. дис. ... канд. екон. наук. Київ: Національний інститут стратегічних досліджень, 2018.

4. Дубницький В. І., Деха І. О. Формування інформаційного та цифрового простору – необхідна умова цифрової трансформації економіки. *Вісник економічної науки України*. 2023. № 2 (45). С. 151-159. DOI: https://doi.org/10.37405/1729-7206.2023.2(45).151-159.

5. Завербний А. С. Особливості формування системи управління кібербезпекою підприємств у воєнний період: теоретико-прикладний аспект. *Innovation and Sustainability*. 2024. No. 1. С. 13-21. DOI: https://doi.org/10.31649/ins.2024.1.13.21.

6. 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 України*. 2022. №1(42). С. 110-113. DOI: https://doi.org/10.37405/1729- 7206.2022.1(42).110-113.

7. Захарченко В. І., Онешко С. В. Прийняття узгодженого рішення в організаційно-технологічній системі при створенні комплексного інформаційно-аналітичного забезпечення стратегії розвитку. *Вісник економічної науки України*. 2023. № 2 (45). С. 63-66.

8. Котрелін 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.

9. Леоненко Н. А., Поступна О. В. Інформаційна безпека України: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Вісник Національного університету цивільного захисту України. Серія: Державне управління*. 2022. № 2 (17). DOI: https://doi.org/10.52363/2414-5866-2022-2-14.

10. Мазуренко Л. І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету ім. В. Н. Каразіна. Серія "Питання політології"*. 2022. Вип. 42. DOI: https://doi.org/10.26565/2220-8089-2022-42-08.

11. Назаренко О. А., Озарко К. С. Виклики та стратегічні пріоритети публічного управління України в умовах війни. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Публічне управління та адміністрування*. 2022. Том 33 (72). № 4. С. 64-71. DOI: https://doi.org/10.32782/TNU-2663-6468/2022.4/11.

12. Новаківський І. І. Система управління підприємства в інформаційному суспільстві: автореф. дис... д-ра екон. наук. Львів: Національний університет «Львівська політехніка», 2017.

13. Огляд ринку кібербезпеки в Україні. DataDriven Research & Consulting, 2025. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf.

14. Державна служба статистики України. URL: https://www.ukrstat.gov.ua/.

15. Офіційний сайт Департаменту кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/.

16. Панченко О. А., Панченко Л. В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. *Правова інформатика*. 2015. № 2(46). С. 32-38.

17. Смотрич Д. В., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету*, 2023. Вип. 77, Ч. 2. С. 121-127. DOI: https://doi.org/10.24144/2307-3322.2023.77.2.20.

18. Сусіденко В., Сусіденко О. Комплексне забезпечення інформаційної безпеки як передумова інноваційного розвитку готельно-ресторанного бізнесу. *Економіка та суспільство*. 2025. Вип. 74. DOI: https://doi.org/10.32782/2524-0072/2025-74-96.

19. Топалов В. Забезпечення інформаційної безпеки бізнесу України в умовах сучасних загроз. *Цифрова економіка та економічна безпека*. 2024. Вип. 6 (15). С. 157-161. DOI: https://doi.org/10.32782/dees.15-24.

20. Чистоклетов Л., Обрембальський С. Особливості забезпечення інформаційної безпеки в умовах російсько-української війни. *Академічні візії*. 2024. Вип. 31. С. 1-11.
DOI: https://doi.org/10.5281/zenodo.11381101.

21. 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*: monograph. Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, 2022. P. 8-19.

22. Pushak Ya., Trushkina N. Formation on national education system for training personnel in the field of snformation security management. *International Scientific Conference Characteristics and trends of socio-economic development at the macro- and micro-levels*: Conference

Proceedings (May 5-6, 2023. Kielce, Poland). Riga, Latvia: "Baltija Publishing". P. 26-31.

References

1. Bakay, V. Y. (2020). Zabezpechennia ekonomichnoi bezpeky pidpryiemstva na osnovi vykorystannia tsyfrovykh tekhnolohii [Ensuring Economic Security of the Enterprise Based on the Use of Digital Technologies]. *Visnyk Khmelnytskoho natsionalnoho universytetu – Bulletin of Khmelnitsky National University*, 4, vol. 1, pp. 32-35. DOI: https://www.doi.org/10.31891/2307-5740-2020-284-4-5 [in Ukrainian].

2. Bilko, S. (2022). Informatsiina ta ekonomichna bezpeka: otsiniuvannia rivnia ta vzaiemozviazku. [Information and economic security: assessing the level and relationship]. *Naukovyi visnyk Polissia – Scientific Bulletin of Polissia,* vol. 1 (24), pp. 58-77. DOI: https://doi.org/10.25140/2410-9576-2022-1(24)-58-77 [in Ukrainian].

3. Vasyltsiv, V. H. (2018). Orhanizatsiino-ekonomichnyi mekhanizm zmitsnennia ekonomichnoi bezpeky sektoru informatsiinykh tekhnolohii [Organizational and economic mechanism of strengthening the economic security of the information technology sector]. *Extended abstract of candidate's thesis.* Kyiv [in Ukrainian].

4. Dubnytskyi, V. I., Dekha, I. O. (2023). Formuvannia informatsiinoho ta tsyfrovoho prostoru – neobkhidna umova tsyfrovoi transformatsii ekonomiky [Formation of information and digital space - a necessary condition for digital transformation of the economy]. *Visnyk ekonomichnoi nauky Ukrainy*, vol. 2 (45). pp. 151-159. DOI: https://doi.org/10.37405/1729-7206.2023.2(45). 151-159 [in Ukrainian].

5. Zaverbnyi, A. S. (2024). Osoblyvosti formuvannia systemy upravlinnia kiberbezpekoiu pidpryiemstv u voiennyi period: teoretyko-prykladnyi aspekt [Features of the formation of the cybersecurity management system of enterprises in wartime: theoretical and applied aspect]. *Innovation and Sustainability*, vol. 1, pp. 13-21. DOI: https://doi.org/10.31649/ins.2024.1.13.21 [in Ukrainian].

6. Zaverbnyi, A. S., Pushak, Ya. Ya. (2022). Problemy ta potentsiini mozhlyvosti rozvytku IT-sfery v Ukraini za umov aktyvizuvannia protsesiv intehruvannia do mizhnarodno-ho 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].

7. Zakharchenko, V. I., Oneshko, S. V. (2023). Pryiniattia uzghodzhenoho rishennia v orhanizatsiino-tekhnolohichnii systemi pry stvorenni kompleksnoho informatsiino-analitychnoho zabezpechennia stratehii rozvytku [Making a coordinated decision in the organizational and technological system when creating a comprehensive information and analytical support for the development strategy]. *Visnyk ekonomichnoi nauky Ukrainy*, vol. 2 (45), pp. 63-66. DOI: https://doi.org/10.37405/ 1729-7206.2023.2(45).63-66 [in Ukrainian].

8. Kotrelin, I. B. (2022). Informatsiina bezpeka v umovakh voiennoho stanu u aspekti zabezpechennia informatsiinykh prav ta svobod [Information security under martial law in the aspect of ensuring information rights and freedoms]. *Aktualni problemy vitchyznianoi yurysprudentsii*, vol. 1. pp. 150-155. DOI: https://doi.org/10.32782/392257 [in Ukrainian].

9. Leonenko, N., Postupna, O. (2022) Informatsiina bezpeka Ukrainy: mekhanizmy, suchasni vyklyky ta zahrozy v umovakh informatsiinoho hlobalizmu [Information security of Ukraine: mechanisms, modern challenges and threats in the conditions of information globalism]. *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Seria: Derzhavne upravlinnia – Bulletin of National University of Civil Defense of Ukraine. State Management series*, vol. 2 (17). DOI: https://doi.org/10.52363/2414-5866-2022-2-14

10. Mazurenko, L. I. (2022). Informatsiina bezpeka v umovakh rosiisko-ukrainskoi viiny: vyklyky ta zahrozy [Information security in the context of the russian-ukrainian war: challenges and threats]. *Visnyk Kharkivskoho natsionalnoho universytetu im. V.N. Karazina. Seriia "Pytannia politolohii" – The Journal of V.N. Karazin Kharkiv National University. Issues of Political Science,* 42. DOI: https://doi.org/10.26565/2220-8089-2022-42-08 [in Ukrainian].

11. Nazarenko, O. A., Ozarko, K. S. (2022). Vyklyky ta stratehichni priorytety publichnoho upravlinnia Ukrainy v umovakh viiny [Challenges and strategic priorities of public administration of Ukraine in wartime]. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia*, Vol. 33 (72). no. 4, pp. 64-71. DOI: https://doi.org/10.32782/TNU-2663-6468/2022.4/11 [in Ukrainian].

12. Novakivskyi, I. I. (2017). Systema upravlinnia pidpryiemstva v informatsiinomu suspilstvi [Enterprise management system in the information society]. *Extended abstract of Doctor's thesis.* Lviv, Lvivska politekhnika [in Ukrainian].

13. Ohliad rynku kiberbezpeky v Ukraini [Overview of the cybersecurity market in Ukraine]. (2025). *DataDriven Research & Consulting.* Retrieved from https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf [in Ukrainian].

14. Derzhavna sluzhba statystyky Ukrainy [State Statistics Service of Ukraine]. (n.d.). *ukrstat.gov.ua.* Retrieved from http://www.ukrstat.gov.ua [in Ukrainian].

15. Ofitsiinyi sait Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy [Official website of the Cyber Police Department of the National Police of Ukraine]. Retrieved from https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/ [in Ukrainian].

16. Panchenko, O. A., Panchenko, L. V. (2015). Informatsiina bezpeka ta informatsiina kultura v suchasnomu informatsiinomu suspilstvi [Information security and information culture in the modern information society]. *Pravova informatyka,* vol. 2(46). pp. 32-38 [in Ukrainian].

17. Smotrych, D. V., Brailko, L. (2023). Informatsiina bezpeka v umovakh voiennoho stanu [Information security under martial law]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu – Uzhhorod National University Herald. Series: Law,* vol. 77, part 2. pp. 121-127. DOI: https://doi.org/10.24144/2307-3322.2023.77.2.20 [in Ukrainian].

18. Susidenko, V., Susidenko, O. (2025). Kompleksne zabezpechennia informatsiinoi bezpeky yak peredumova innovatsiinoho rozvytku hotelno-restorannoho biznesu [Comprehensive information security as a prerequisite for the innovative development of the hotel and restaurant

business]. *Ekonomika ta suspilstvo – Economy and society,* 74. DOI: https://doi.org/10.32782/2524-0072/2025-74-96 [in Ukrainian].

19. Topalov, V. (2024). Zabezpechennia informatsiinoi bezpeky biznesu Ukrainy v umovakh suchasnykh zahroz [Ensuring the information security of Ukrainian business in the context of modern threats]. *Tsyfrova ekonomika ta ekonomichna bezpeka – Digital Economy and Economic Security*, vol. 6 (15), pp. 157-161. DOI: https://doi.org/10.32782/dees.15-24 [in Ukrainian].

20. Chystokletov, L., Obrembalskyi, S. (2024). Osoblyvosti zabezpechennia informatsiinoi bezpeky v umovakh rosiisko-ukrainskoi viiny [eatures of information security in the context of the russian-ukrainian war]. *Akademichni vizii – Academic Visions,* vol. 31, pp. 1-11. DOI: https://doi.org/10.5281/zenodo.11381101 [in Ukrainian].

21. 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*: monograph. (pp. 8-19). Košice, Vysoká škola bezpečnostného manažérstva v Košiciach.

22. Pushak, Ya., Trushkina, N. (2023). Formation on national education system for training personnel in the field of snformation security management. *International Scientific Conference Characteristics and trends of socio-economic development at the macro- and micro-levels*: Conference Proceedings (May 5-6, 2023. Kielce, Poland). (pp. 26-31). Riga, Latvia, "Baltija Publishing".

Стаття надійшла до редакції 26.05.2025
Рецензовано: 16.06.2025

Формат цитування:

Озарко К. С., Опотяк Ю. В., Андрухів Т. В. Проблеми і потенційні можливості забезпечення інформаційної безпеки бізнесу в умовах воєнного стану. *Вісник економічної науки України.* 2025. № 1 (48). С. 187-192. *DOI: https://doi.org/10.37405/1729-7206.2025.1(48).187-192*

Ozarko, K. S., Opotyak, Yu. V., Andrukhiv, T. V. (2025). Problems and Potential Opportunities for Ensuring Business Information Security under Martial Law. *Visnyk ekonomichnoi nauky Ukrainy*, 1 (48), pp. 187-192. *DOI: https://doi.org/10.37405/1729-7206.2025.1(48).187-192*