Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292. Ефективна економіка. 2025. № 7.

DOI: http://doi.org/10.32702/2307-2105.2025.7.3

УДК 338.4

В. А. Кулик,

д. е. н., професор, професор кафедри менеджменту і логістики,

Національний університет

«Полтавська політехніка імені Юрія Кондратюка»

ORCID ID: https://orcid.org/0000-0002-3271-7845

ЦИФРОВІ ЗАГРОЗИ У БІЗНЕС-СЕРЕДОВИЩІ У КОНТЕКСТІ ЦІЛЕЙ СТАЛОГО РОЗВИТКУ

V. Kulyk,

Doctor of Economic Sciences, Professor, Professor of the Department of Management and Logistics, National University "Yuri Kondratyuk Poltava Polytechnic"

DIGITAL THREATS IN THE BUSINESS ENVIRONMENT IN THE CONTEXT OF THE SUSTAINABLE DEVELOPMENT GOALS

У статті досліджено виклики цифрової трансформації для вітчизняних підприємств у контексті реалізації Цілей сталого розвитку, зокрема, для підприємств електронного бізнесу. З урахуванням зростання кіберзагроз, автор дослідження аналізує управлінські підходи та практики, що дозволяють підвищити кіберстійкість та забезпечити фінансову й операційну сталість підприємств електронного бізнесу. Методологічну основу становлять огляд

сучасних наукових підходів до управління цифровими ризиками, а також результати опитування представників українського бізнес-середовища. Результати дослідження свідчать про підвищену увагу керівників підприємств електронного бізнесу до превентивних заходів кіберзахисту та організаційного реагування на інциденти. Автор дослідження обґрунтовує, що інтеграція цифрової безпеки у стратегічне планування у контексті досягнення Цілей сталого розвитку сприяє інституційній зрілості організацій та відкриває потенціал для впровадження інновацій. У висновках зазначено, що стійке стратегічне управління з урахуванням цифрових ризиків та шляхів досягнення Цілей сталого розвитку є ключовими чинниками, що впливають на конкурентоспроможність підприємств електронного бізнесу. У висновках зазначено, що стійке стратегічне управління з урахуванням цифрових ризиків та шляхів досягнення Цілей сталого розвитку є ключовими чинниками, що впливають на конкурентоспроможність підприємств електронного бізнесу в умовах цифрової економіки

The article highlights the current challenges posed by the intensive digital transformation of the business environment, in particular in the field of e-entrepreneurship, which is increasingly subject to complex digital threats. The author conducts a comprehensive study aimed at identifying and critically evaluating management strategies that can ensure both a rapid response to cybersecurity threats and long-term organisational sustainability in the digital economy. It is emphasised that, given the high level of vulnerability of electronic enterprises to cyber incidents, the integration of digital security policies into strategic planning is not only desirable, but a systemic condition for ensuring their competitiveness. The methodological basis of the study includes an analysis of the current scientific discourse on digital risk management, as well as empirical results of a questionnaire survey of Ukrainian e-businesses. The data obtained indicate the growing attention to preventive cyber defence measures, the expediency of institutionalising response functions, and the need to transform

organisational structures towards digital adaptability. The author proposes a conceptual model for integrating digital security into the strategic framework of enterprise development, taking into account the provisions of the Sustainable Development Goals, which are a systemic element of modern economic thinking. It is proved that the combination of strategic risk management and sustainability principles forms the basis for increasing the innovation capacity, operational efficiency and social responsibility of e-business. As a result, it is emphasised that the strategic focus on digital security in combination with globally recognised sustainable development benchmarks is one of the determining factors of the long-term stability of enterprises in the post-industrial economic landscape. The results indicate that e-business executives are paying increased attention to preventive cyber defence measures and organisational incident response. Such management approaches contribute to the development of sustainable protection systems and open up new opportunities for innovation.

Ключові слова: *бізнес-процеси, електронний бізнес, кібербезпека, управління, сталий розвиток, цифровізація.*

Keywords: *business processes, e-business, cybersecurity, governance, sustainable development, digitalisation.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. У сучасному цифровізованому світі бізнес-середовище зазнає глибоких трансформацій, спричинених інтенсивним впровадженням інформаційно-комунікаційних технологій. Ці зміни зумовлюють як нові можливості для економічного зростання, так і суттєві ризики, пов’язані з цифровими загрозами. Особливо актуальною є ця проблема для підприємств електронного бізнесу, які функціонують в умовах високої залежності від цифрової інфраструктури. Український сектор електронного бізнесу, перебуваючи у стадії активного розвитку та структурних змін, особливо чутливий до впливу кіберзагроз,

порушення конфіденційності даних, фінансових шахрайств і нестабільності цифрових платформ. Водночас, досягнення Цілей сталого розвитку (ЦСР), проголошених ООН, передбачає забезпечення безпечного та інклюзивного цифрового середовища, що сприятиме сталості економічних процесів. У такому контексті важливо дослідити, яким чином цифрові загрози впливають на досягнення стратегічних цілей підприємств, та які механізми управління ризиками можуть бути інтегровані у їхню діяльність. Аналіз викликів цифрової безпеки у поєднанні зі стратегією сталого розвитку дозволяє сформувати ефективні підходи до підвищення адаптивності українських підприємств електронного бізнесу в умовах цифрової трансформації.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення не вирішених раніше частин загальної проблеми, котрим присвячується означена стаття. У науковій літературі, обґрунтування та шляхи вирішення проблем, пов’язаних із цифровими загрозами у бізнес-середовищі розглядаються у контексті економічної безпеки, безпеки інформаційних систем, стратегічного управління та сталого розвитку. У роботах українських науковців, таких як Гайдук О., Звєрєв В. [2] та Мазур Я. [4] проаналізовано сучасний спектр кіберзагроз, пов’язаних зі стрімким розвитком інформаційних технологій та інформаційними війнами. Мальцева І., Черниш Ю., Штонда Р. [5] та Онищенко С., Маслій О., Дрібна А. [8] у своїх дослідженнях розглянули специфіку цифрових атак на критичну інфраструктуру, виокремивши ключові вектори ризиків для підприємств. Дослідження Шишкової Н. [9] та Ясінської А. [10] присвячені захисту облікової та корпоративної інформації, вони підкреслюють необхідність інтеграції засобів безпеки в управлінські процеси. Питання цифрових загроз у контексті трансформації цифрової інфраструктури малого бізнесу розглядаються у дослідженні Овсієнко О. [7], вплив цифрових загроз на стратегічну стійкість підприємств досліджено у працях Мануйлова О. [6] та Коробко С. [3]. Іноземні та вітчизняні дослідники у своїх працях акцентують

увагу на важливості адаптації моделей кібербезпеки до специфіки бізнес-середовища, управлінських підходів, обмежених ресурсів та викликів, пов'язаних із розвитком штучного інтелекту [11-14].

Попри значну увагу до технічних і правових аспектів кіберзахисту, недостатньо вивченими залишаються питання впливу цифрових загроз на досягнення Цілей сталого розвитку, зокрема, у контексті соціальної інклюзії, економічної стійкості та інноваційної спроможності українських підприємств електронного бізнесу. У вітчизняній науковій літературі недостатньо глибоко дослідженими є комплексні підходи, які б поєднували аналіз ризиків із розробкою адаптивних управлінських стратегій сталого розвитку в умовах змін.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження впливу цифрових загроз на бізнес-середовище у контексті досягнення Цілей сталого розвитку. Дослідження проводиться на прикладі українських підприємств електронного бізнесу. Основним завданням дослідження є розробка управлінських підходів до мінімізації кіберзагроз. Особлива увага приділяється можливості інтеграції заходів цифрової безпеки у стратегії розвитку підприємств електронного бізнесу з урахуванням сучасних викликів цифрової трансформації.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. У межах цього дослідження, електронний бізнес – це форма організації підприємницької діяльності, заснована на цифрових технологіях для реалізації комерційних процесів – від електронної комерції до електронного управління операціями, комунікаціями з клієнтами, постачальниками й партнерами. Електронний бізнес вирізняється високим рівнем залежності від цифрових платформ, що створює нові можливості та посилює ризики.

Цифрові загрози – це сукупність потенційних або реальних ризиків, спричинених впливом інформаційно-комунікаційних технологій на функціонування підприємств, зокрема, і в цифровому середовищі. До них належать кібератаки, несанкціонований доступ до даних, фішинг, втрати

конфіденційної інформації, цифрове шахрайство, а також вразливість до маніпуляцій штучним інтелектом. Ці загрози мають пряму та опосередковану дію на економічну безпеку, сталий розвиток та конкурентоспроможність підприємств.

Стратегія розвитку підприємств електронного бізнесу у контексті взаємодії з цифровими загрозами – це системний підхід до довгострокового планування і реалізації цілей підприємства, спрямований на забезпечення стабільного зростання, ефективного використання ресурсів і адаптації до змін зовнішнього середовища. В умовах цифрової трансформації стратегія повинна інтегрувати інноваційні цифрові рішення, інструменти забезпечення кіберстійкості та шляхи досягнення Цілей сталого розвитку.

У площині електронного бізнесу особливо релевантними є ЦСР 8 (гідна праця і економічне зростання), ЦСР 9 (інновації та інфраструктура), ЦСР 12 (відповідальне споживання), ЦСР 16 (інституційна спроможність і безпека). Інтеграція зазначених цілей в управлінські підходи сприяє формуванню бізнес-моделі, орієнтованої на стійкість, інноваційність і цифрову відповідальність.

Для досягнення мети і завдань дослідження у 2025 році було проведено анкетування 25 підприємств електронного бізнесу в Україні. Зміст анкети узагальнено у табл. 1.

Таблиця 1. Зміст анкети, яка була використана для опитування підприємств електронного бізнесу у 2025 році

Питання	Варіанти відповідей
1. Які з наведених цифрових загроз, на Вашу думку, є найбільш актуальними для Вашого підприємства? (можна обрати до 3 варіантів включно)	– кібератаки (DDoS, фішинг, злом мереж) витік конфіденційної інформації – несанкціонований доступ до клієнтських баз – збої в цифровій інфраструктурі (сервери, CRM тощо) – недостатній рівень цифрової грамотності персоналу
2. Як часто Ваша компанія зіштовхувалася з цифровими інцидентами протягом останніх 12 місяців?	– жодного разу – 1–2 інциденти – 3–5 інцидентів – понад 5 випадків

Продовження таблиці 1.

Питання	Варіанти відповідей
3. Наскільки суттєво, на Вашу думку, цифрові загрози впливають на загальну стійкість бізнесу?	– впливають критично – мають помірний вплив – мінімальний вплив – не мають впливу
4. Які функціональні зони підприємства найбільш вразливі до цифрових ризиків? (можна обрати до 2 варіантів включно)	– онлайн-продажі / e-commerce платформи – фінансові операції – облік клієнтів / CRM – управління персоналом
5. Чи має підприємство затверджену політику або протокол дій у разі кіберінциденту?	– так – частково – у процесі розробки – ні
6. Які заходи з цифрової безпеки впроваджені на підприємстві? (можна обрати кілька)	– антивірусне програмне забезпечення – двофакторна автентифікація – резервне копіювання даних – навчання працівників із питань кібербезпеки – зовнішній аудит кіберзахисту
7. Хто відповідає за управління цифровими ризиками у Вашій компанії?	– IT-відділ – безпековий менеджер – керівник підприємства – залучені зовнішні спеціалісти – ніхто / немає чітко визначеної ролі
8. Як Ви оцінюєте загальний рівень кіберготовності Вашого підприємства?	– високий – середній – низький – важко сказати
9. Які управлінські дії Ви вважаєте найбільш ефективними для зниження цифрових ризиків? (оберіть один варіант відповіді)	– регулярне навчання персоналу – інвестиції в IT-інфраструктуру – формалізація внутрішніх процедур безпеки – залучення зовнішніх експертів
10. Чи враховує Ваша стратегія розвитку аспекти цифрової безпеки як елемент сталості?	– так, повною мірою – частково – формально / номінально – не враховує
11. На Вашу думку, чи сприяє підвищення рівня цифрової безпеки досягненню Цілей сталого розвитку?	– так, безумовно – так, але частково – ні – важко відповісти
12. Чи існує у Вашій організації окремий розділ у стратегічних документах, присвячений цифровій трансформації та кібербезпеці?	– так – ні – у процесі розробки
13. Які бар'єри заважають ефективній інтеграції цифрової безпеки у стратегію розвитку підприємства?	– брак фінансування – нестача фахівців – відсутність розуміння важливості кібербезпеки
14. Які напрями цифрової трансформації є пріоритетними для Вашого бізнесу у найближчі 2 роки?	– автоматизація бізнес-процесів – захист даних і конфіденційності – розширення онлайн-каналів збуту – аналітика великих даних (Big Data)

Результати проведеного опитування дозволили визначити підходи до інтеграції заходів цифрової безпеки у стратегії розвитку підприємств електронного бізнесу з урахуванням Цілей сталого розвитку. Розподіл досліджуваних підприємств електронного бізнесу за сферами діяльності наведено на рис. 1.

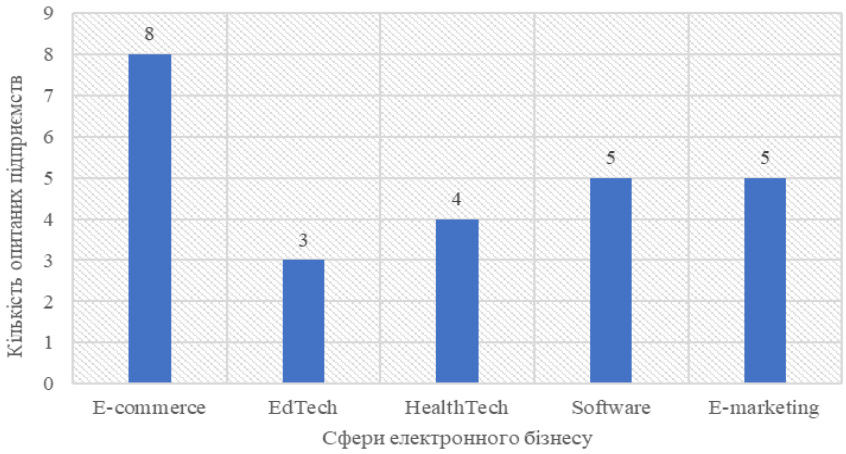

Рис. 1. Розподіл підприємств електронного бізнесу, що взяли участь в опитуванні за сферами діяльності

У процесі дослідження було розроблено анкету, яка наведена у додатку А. Опитування проводилося з метою виявлення рівня обізнаності, досвіду та управлінських практик, пов’язаних із цифровими ризиками та їхнім впливом на сталість електронного бізнесу в Україні.

Узагальнений результат відповідей респондентів на питання «Які з наведених цифрових загроз, на Вашу думку, є найбільш актуальними для Вашого підприємства? (можна обрати до 3 варіантів)» наведено на рис. 2.

Рис. 2. Узагальнені результати відповідей респондентів на питання 1 анкети

На думку респондентів найбільшими цифровими загрозами для підприємств електронного бізнесу є несанкціонований доступ до клієнтських баз та Кібератаки (DDoS, фішинг, злом мереж). Проте, інші види цифрових загроз, наведені як варіанти відповідей у анкеті також є важливими на думку респондентів.

Незважаючи, на визнання та підготовку підприємств до цифрових інцидентів, їх кількість коливається від 1 до 2 інцидентів на рік у 45 % опитаних, та від 3 до 5 інцидентів на рік у 55 %. Серед опитаних не виявлено підприємств, які б не мали цифрових інцидентів протягом останні 12 місяців, яких і тих підприємств, що мали їх більше 5.

Вплив цифрових загроз на стійкість бізнесу за рівнем впливу, респонденти оцінили таким чином: 1) відповідь «впливають критично» дали 23 % респондентів; 2) «мають помірний вплив» – 43 %; 3) «мінімальний вплив» – 31 %; 4) «не мають впливу» – 4 %.

Узагальнений результат відповідей респондентів на питання «Які функціональні зони підприємства найбільш вразливі до цифрових ризиків? (можна обрати до 2 варіантів)» наведено на рис. 3.

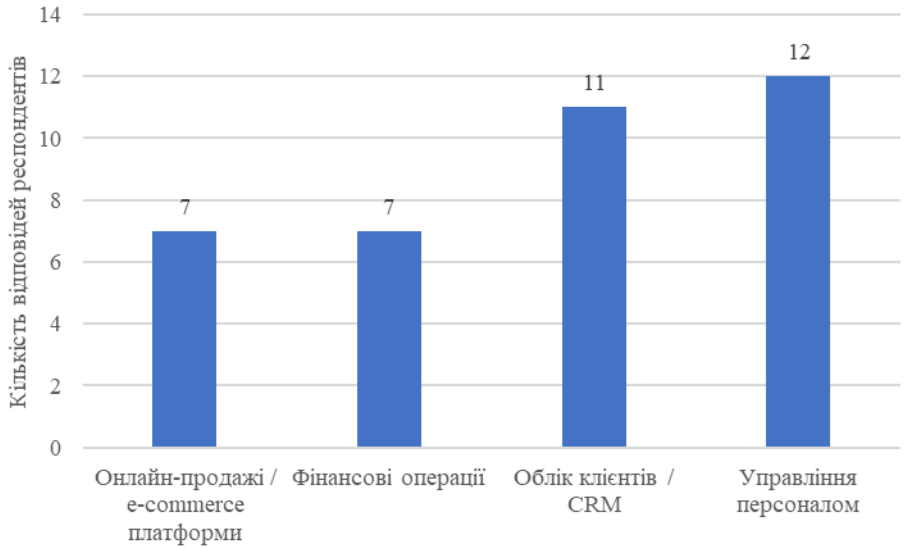

Рис. 3. Узагальнені результати відповідей респондентів на питання 4 анкети

За даними рис. 3, можна зробити висновок, що найбільш вразливими до цифрових ризиків зонами є облік клієнтів / CRM та управління персоналом. Сфери діяльності пов’язані із онлайн-продажами та фінансовими операціями є менш ризикованими на думку респондентів.

Більшість досліджуваних підприємств (51 % респондентів дали позитивну відповідь) стверджують, що мають затверджену політику або протокол дій у разі кіберінциденту, тоді як лише 3 % опитаних, дали відповідь «ні» на питання 5 анкети.

Відповідальними за управління цифровими ризиками в компанії є: 1) «ІТ-відділ», таку відповідь дали 13 % опитаних; 2) «безпековий менеджер» – 5 % опитаних; 3) «керівник підприємства» – 33 %; 4) «залучені зовнішні спеціалісти» – 20 %; 5) «немає чітко визначеної ролі» – 29 %.

Узагальнений результат відповідей респондентів на питання «Які управлінські дії Ви вважаєте найбільш ефективними для зниження цифрових ризиків? (оберіть один із варіантів)» наведено на рис. 4.

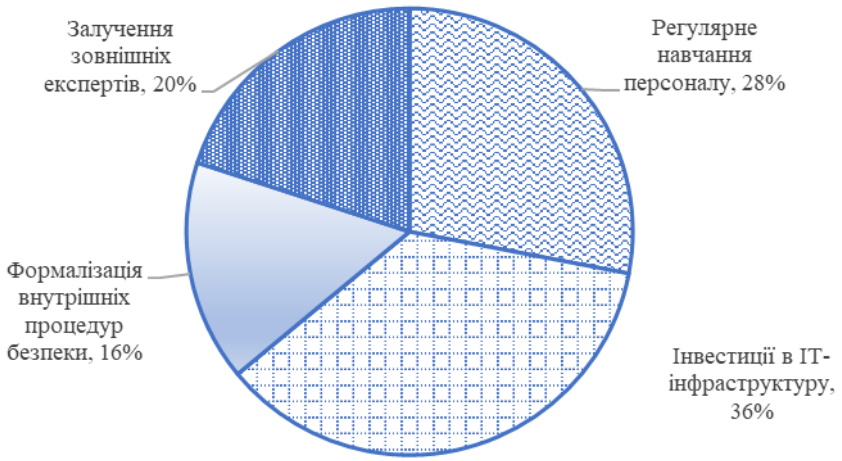

Рис. 4. Узагальнені результати відповідей респондентів на питання 9 анкети

Узагальнені результати опитування респондентів, відображені на рис. 4 свідчать, що найбільш ефективними управлінськими діями, направленими на зниження цифрових ризиків є інвестиції в ІТ-інфраструктуру (на думку 36 % респондентів) та регулярне навчання персоналу (28 %), такі дії як залучення зовнішніх експертів та формалізація внутрішніх процедур є найбільш ефективними на думку 20 % та 16 % респондентів відповідно.

На питання «На Вашу думку, чи сприяє підвищення рівня цифрової безпеки досягненню Цілей сталого розвитку?», 62 % респондентів обрали відповідь «важко відповісти», 3 % – «ні», 18 % – «так, але частково», 17 % – «так, безумовно»; що свідчить про недостатню увагу керівників підприємств щодо цього питання та низький рівень обізнаності працівників щодо узгодження стратегічних цілей підприємства з Цілями сталого розвитку.

Аналіз узагальнених результатів опитування представників підприємств українського електронного бізнесу, дав можливість зробити такі висновки. У сучасному цифровому середовищі підприємства електронного бізнесу стикаються з подвійним завданням: з одного боку, необхідністю адаптації до стрімких технологічних змін, з іншого – забезпеченням стабільного та безпечного функціонування у межах Цілей сталого розвитку.

Активна цифровізація бізнес-процесів супроводжується посиленням кіберзагроз, що створює загрозу порушення конфіденційності даних, безперервності операцій та зниження довіри з боку клієнтів і партнерів. Таким чином, цифрова безпека перетворюється з технічних функцій на стратегічний компонент довгострокового розвитку.

Інтеграція заходів цифрової безпеки у стратегії сталого розвитку передбачає формування комплексного підходу до ризик-менеджменту, що охоплює економічні, соціальні та екологічні аспекти діяльності підприємства. Доцільним, на нашу думку, є впровадження відповідної політики кіберзахисту, яка охоплює моніторинг цифрових ризиків, навчання персоналу, розробку сценаріїв реагування на інциденти, а також регулярну оцінку кіберготовності.

Особливу увагу слід приділяти інституційній готовності до впровадження таких заходів, зокрема, через створення окремих структур або функціональних одиниць, відповідальних за цифрову безпеку. У зв’язку з обмеженими ресурсами, підприємства електронного бізнесу, які належать до суб’єктів малого та середнього підприємництва, можуть застосовувати гнучкі моделі співпраці: спільне використання платформ безпеки, аутсорсинг захисних послуг, участь у освітніх кластерах з кіберграмотності.

Реалізація таких стратегій сприяє не лише зниженню рівня цифрових загроз, а й забезпечує досягнення кількох Цілей сталого розвитку, зокрема, ЦСР 8 (гідна праця і економічне зростання), ЦСР 9 (інновації та інфраструктура), ЦСР 12 (відповідальне споживання), ЦСР 16 (інституційна спроможність і безпека). Таким чином, поєднання цифрової трансформаціями з заходами кіберзахисту дозволяє підприємствам електронного бізнесу не лише підтримувати конкурентоспроможність, а й сприяти формуванню безпечного та сталого цифрового простору.

Основні етапи формування стратегії підприємства електронного бізнесу, адаптовані до викликів цифрових загроз і пріоритетів сталого розвитку наведено у табл. 2.

Таблиця 2. Етапи формування стратегії підприємства електронного бізнесу, адаптовані до викликів цифрових загроз і пріоритетів сталого розвитку

Етапи	Управлінські дії
Формування місії, бачення та цінностей	Визначення стратегічного призначення підприємства з акцентом на цифрову безпеку, сталий розвиток і соціальну відповідальність. Формування бачення як інноваційної, безпечної та екологічно чутливої бізнес-моделі
Аналіз зовнішнього та внутрішнього середовища	Проведення PEST- та SWOT-аналізів з обов'язковим урахуванням цифрових загроз (кіберризики, регуляторні обмеження, технологічні зміни) та можливостей сталого розвитку (гранти, партнерства, «зелені» технології)
Оцінка рівня цифрової готовності та кіберстійкості	Визначення вразливих ланок IT-інфраструктури, оцінка навичок персоналу з цифрової грамотності, готовність до інцидентів, наявність планів реагування на кібератаки
Формулювання стратегічних цілей	Встановлення чітких цілей за принципом SMART, які поєднують операційну ефективність, цифрову безпеку та внесок у реалізацію Цілей сталого розвитку (ЦСР 9, 12, 16 тощо)
Розробка стратегічних ініціатив	Планування конкретних заходів: впровадження технологій шифрування, автоматизованого моніторингу безпеки, енергоефективних рішень, сталого ланцюга постачання, підвищення цифрових компетенцій команди
Вбудовування безпекових практик у бізнес-моделі	Інтеграція політик кіберзахисту, контроль доступів, управління ризиками, аудит цифрових активів та інфраструктури
Ресурсне та організаційне забезпечення	Розподіл відповідальності за реалізацію ініціатив. Бюджетування заходів з кібербезпеки та сталого розвитку, створення команд або посад з відповідними функціями
Моніторинг, оцінка ефективності та ревізія стратегії	Визначення KPI з цифрової безпеки (кількість інцидентів, час реагування), екологічного впливу (енерговитрати) та соціальних показників. Регулярне оновлення стратегії відповідно до змін у ризиковому цифровому середовищі

Джерело: запропоновано автором

Запропонований послідовний підхід дозволяє сформувати адаптивну та стійку стратегію підприємств електронного бізнесу, здатну не лише реагувати на цифрові виклики, а й створювати довготривалу цінність у межах Цілей сталого розвитку.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. У результаті проведеного дослідження можна зробити висновок, що цифрова трансформація бізнес-середовища, зокрема, у сфері

електронного бізнесу, супроводжується не лише зростанням можливостей, а й підвищеним рівнем цифрових загроз, які суттєво впливають на стійкість, ефективність та інноваційність підприємств. Аналіз наукових джерел та емпіричних даних засвідчив, що управлінські практики, орієнтовані на превентивний кіберзахист, системне реагування на інциденти та розвиток цифрової грамотності персоналу, поступово набувають пріоритетного значення у структурі стратегічного управління.

Інтеграція політик цифрової безпеки у стратегії розвитку підприємств електронного бізнесу є необхідною умовою адаптації до вимог цифрової економіки. У контексті Цілей сталого розвитку така інтеграція набуває додаткової ваги як інструмент підвищення інституційної зрілості, соціальної відповідальності та інноваційної спроможності підприємств. Розглянуті етапи формування стратегії підприємства електронного бізнесу, адаптовані до викликів цифрових загроз і пріоритетів сталого розвитку є актуальним управлінським інструментом для формування довгострокової конкурентоспроможності.

Таким чином, цифрова безпека має розглядатися не як ізольована технічна функція, а як інтегрований компонент стратегічного бачення бізнесу в умовах постіндустріального розвитку. Спрямованість на системне управління цифровими ризиками у поєднанні зі сталими підходами забезпечує підґрунтя для формування сталих бізнес-моделей нового покоління.

Матеріал підготовлено у межах проєкту «Формування стратегії розвитку особистості в цифровому освітньому просторі: Україна-ЄС». № 101127592 - FPDSDESUEU - ERASMUS-JMO-2023-HEI-TCH-RSCH.

Література

1. Бортнік А. М. Моделювання бізнес-архітектури підприємства. *Економічний простір*. 2020. № 156. С. 116-119.

2. Гайдук О., Звєрєв В. Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій. *Кібербезпека: освіта, наука, техніка*. 2024. № 3(23). С. 225-236.

3. Коробка С. В. Стратегія сталого розвитку в управлінні організацією. *Проблеми сучасних трансформацій*. 2024. № 16.

4. Мазур Я. П. Основні кіберзагрози в умовах ведення інформаційної війни. *Аналітично-порівняльне правознавство*. 2024. № 6. С. 599-604.

5. Мальцева І. Р., Черниш Ю. О., Штонда Р. М. Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка*. 2022. № 4(16). С. 37-44.

6. Мануйлов О. В. Формування стратегії сталого розвитку підприємств в умовах невизначеності. *Український журнал прикладної економіки та техніки*. 2024. № 2. С. 60-64.

7. Овсієнко О. В. Цифрова інфраструктура підтримки малого бізнесу в Україні. *Ефективна економіка*. 2021. № 2.

8. Онищенко С., Маслій О., Дрібна А. Оцінювання фінансово-економічної безпеки підприємства критичної інфраструктури. *Вісник Хмельницького національного університету*. 2022. № 6. С. 249-258.

9. Шишкова Н. Л. Засоби підвищення керованості безпекою облікової інформації. *Економічний вісник*. 2016. № 3. С. 119-127.

10. Ясінська А. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації. *Економіка і суспільство*. 2023. № 56.

11. Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2020). Integrated framework for cybersecurity auditing. *Information Security Journal: A Global Perspective.* Vol. 30(4). P. 189-204.

12. Tsikalo Ye., Zinevych O., Osipenko D., Kulyk V., Lagovska O. Using Artificial Intelligence to Improve Tax Security and Control over Tax Avoidance Schemes. *Journal of Theoretical and Applied Information Technology*. 2024. Vol. 102. P. 8530-8542.

13. Wang, S., & Wang, H. (2019). Knowledge Management for Cybersecurity in Business Organizations: A Case Study. *Journal of Computer Information Systems.* P. 1-8.

14. Wilson, M., & McDonald, S. (2024). One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses. *Information Security Journal: A Global Perspective.* Vol. 34(1). P. 15-49.

References

1. Bortnik, A.M. (2020), "Modelling the business architecture of an enterprise", *Ekonomichnyi prostir*, vol. 156, pp. 116-119.

2. Haiduk, O. and Zverev, V. (2024), "Analysis of cyber threats in the context of rapid development of information technology", *Kiberbezpeka: osvita, nauka, tekhnika*, vol. 3(23), pp. 225-236.

3. Korobka, S.V. (2024), "Sustainable development strategy in organisational management", *Problemy suchasnykh transformatsij*, vol. 16.

4. Mazur, Y. (2024), "The main cyber threats in the conditions of information warfare", *Analitychno-porivnialne pravoznavstvo*, vol. 6, pp. 599-604.

5. Maltseva, I. Chernish, Y. and Shtonda, R. (2022), "Analysis of some cyber threats in war", *Kiberbezpeka: osvita, nauka, tekhnika*, vol. 4(16), pp. 37-44.

6. Manuilov, O. (2024), "Development of a strategy for sustainable development of enterprises in conditions of uncertainty", *Ukrains'kyj zhurnal prykladnoi ekonomiky ta tekhniky*, vol. 2, pp. 60-64.

7. Ovsiienko, O. (2021), "Digital infrastructure of small business support in Ukraine", *Efektyvna ekonomika*, vol. 2.

8. Onyshchenko, S. Maslii, O. and Dribna, A. (2022), "Assessment of financial and economic security of the critical infrastructure enterprise", *Visnyk Khmelnytskoho natsionalnoho universytetu*, vol. 6, pp. 249-258.

9. Shyshkova, N.L. (2016), "Tools to improve the manageability of accounting information security", *Ekonomichnyi visnyk*, vol. 3, pp. 119-127.

10. Yasinska, A. (2023), “Information security of an enterprise: conceptual foundations of effective information protection”, *Ekonomika i suspilstvo*, vol. 56.

11. Al-Matari, O.M.M. Helal, I.M.A. Mazen, S.A. and Elhennawy, S. (2020), “Integrated framework for cybersecurity auditing”, *Information Security Journal: A Global Perspective*, vol. 30(4), pp. 189-204.

12. Tsikalo, Ye. Zinevych, O. Osipenko, D. Kulyk, V. and Lagovska, O. (2024), “Using Artificial Intelligence to Improve Tax Security and Control over Tax Avoidance Schemes”, *Journal of Theoretical and Applied Information Technology*, vol. 102, pp. 8530-8542.

13. Wang, S. and Wang, H. (2019), “Knowledge Management for Cybersecurity in Business Organizations: A Case Study”, *Journal of Computer Information Systems*, vol. 1-8.

14. Wilson, M. and McDonald, S. (2024), “One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses”, *Information Security Journal: A Global Perspective*, vol. 34(1), pp. 15-49.

Стаття надійшла до редакції 26.06.2025 р.