

УДК 330.34.014.2

DOI: <https://doi.org/10.30838/EP.204.182-191>

Лерін О.В.

Миколаївський національний аграрний університет

Lehin Oleh

Mykolaiv National Agrarian University

<https://orcid.org/0009-0009-6967-3557>

ІНТЕГРОВАНА ЦИФРОВІЗАЦІЯ ПІДПРИЄМСТВ

Інтегрована цифровізація підприємств з урахуванням кібербезпеки та екологічної відповідальності відповідає глобальним трендам сталого розвитку, технологічного прогресу та зростання кіберзагроз. Ключовими аспектами ефективності інтегрованої цифровізації постають: цифрові технології, які дозволяють підприємствам оптимізувати процеси, підвищувати продуктивність і знижувати витрати; кібербезпека як критична необхідність, оскільки підприємства, що не інвестують у кібербезпеку, ризикують втратою даних, репутації та фінансових ресурсів; екологічна відповідальність як спосіб оптимізації ресурсів та переходу на «зелені» дата-центри.

Інтегрована цифровізація підприємств вимагає балансу між технологічними інноваціями, захистом даних і екологічними цілями. Підприємства, які успішно поєднують ці аспекти, отримують конкурентну перевагу, залучаючи клієнтів і партнерів, які цінують сталий розвиток і безпеку.

Робота присвячена розробці науково-обґрунтованих рекомендацій з цифровізації підприємств, що враховують вимоги кібербезпеки та екологічної відповідальності в Україні в умовах воєнного та поствоєнного станів. Завданнями роботи є: аналіз теоретичних засад цифровізації підприємств, кібербезпеки та екологічної відповідальності; оцінка сучасного стану цифрової трансформації, рівня кіберзахищеності та екологічної відповідальності підприємств; розробка інтегрованої моделі цифровізації з компонентами кіберзахисту та екологічного моніторингу.

Зроблено висновок про те, що в умовах адаптації до швидкозмінного цифрового світу, де кібербезпека та екологічна відповідальність стають невід'ємними компонентами успішної бізнес-стратегії, підприємства, які інтегрують ці принципи, не лише підвищують ефективність, але й відповідають вимогам сучасного ринку та суспільства.

Ключові слова: цифровізація підприємств, кібербезпека, екологічна відповідальність, інтегрована цифровізація, модель інтегрованої цифровізації.

INTEGRATED DIGITALIZATION OF ENTERPRISES

Integrated digitalization of enterprises, considering cybersecurity and environmental responsibility, aligns with global trends in sustainable development, technological progress, and rising cyber threats. Key aspects of effective integrated digitalization include: digital technologies that enable enterprises to optimize processes, increase productivity, and reduce costs; cybersecurity as a critical necessity, as enterprises that do not invest in it risk data loss, reputational damage, and financial losses; and environmental responsibility as a means of resource optimization and transitioning to "green" data centers. Integrated digitalization of enterprises requires a balance between technological innovation, data protection, and environmental goals. Enterprises that successfully combine these aspects gain a competitive advantage, attracting clients and partners who value sustainability and security.

The purpose of the article is to develop scientifically based recommendations for the digitalization of entrepreneurship, taking into account the requirements of cybersecurity and environmental responsibility in war and post-war situations.

The theoretical foundations of enterprise digitalization, cybersecurity, and environmental responsibility were analyzed. The current state of digital transformation, the level of cybersecurity, and environmental responsibility of enterprises was assessed. An integrated model of enterprise digitalization with components of cybersecurity and environmental monitoring and recommendations for the implementation of the developed solutions were developed.

It is concluded that in the context of adapting to a rapidly changing digital world, where cybersecurity and environmental responsibility are becoming integral components of a successful business strategy, enterprises that integrate these principles not only increase efficiency, but also meet the requirements of the modern market and society. Such an approach ensures resilience, long-term competitiveness, and sustainable economic growth.

Keywords: enterprise digitalization, cybersecurity, environmental responsibility, integrated digitalization, integrated digitalization model.

JEL classification: M10, M14.

Постановка проблеми. Внаслідок надзвичайного прискорення темпів змін у світовому бізнес-середовищі та системах управління сучасні організації стикаються з багатоаспектними проблемами, такими як цифровізація, забезпечення кібербезпеки, екологічні й соціальні виклики. Вони є ключовими факторами підвищення конкурентоспроможності, ефективності та адаптивності бізнесу. Отже, актуальність теми зумовлена інтенсивною цифровізацією одночасно з кібезагрозами, що зростають, та екологічними викликами в умовах воєнного і поствоєнного станів в Україні. Ці фактори вимагають комплексного підходу до трансформації бізнес-моделей. Забезпечення надійного кіберзахисту і мінімізація негативного впливу на довкілля стають ключовими факторами стійкості та конкурентоспроможності підприємств.

Важливість інтегрованого підходу до цифровізації підприємств може забезпечити такі процеси, як оптимізація виробництва, аналіз даних та прийняття рішень, покращення клієнтської бази, економічна ефективність тощо. Цифровізація дозволяє автоматизувати бізнес-процеси, зменшуючи витрати часу та ресурсів. Цифрові інструменти, наприклад, омніканальні платформи, дозволяють персоналізувати взаємодію з клієнтами, підвищуючи їхню лояльність. Інтернет-магазини, чат-боти та мобільні додатки стають невід'ємною частиною сучасного бізнесу. У світі, де компанії з різних країн конкурують на одному ринку, цифровізація забезпечує швидший доступ до міжнародних ринків, оптимізує ланцюги постачань і зменшує бар'єри для масштабування. Інтеграція технологій, таких як штучний інтелект, Інтернет речей або блокчейн, відкриває нові можливості для створення продуктів і послуг. Споживачі, партнери та регуляторні органи все частіше вимагають від компаній використання цифрових рішень, наприклад, для забезпечення прозорості, кібербезпеки чи відповідності стандартам ESG (Environmental, Social, Governance). Хмарні технології та SaaS (Software as a Service) знижують витрати на ІТ-інфраструктуру, дозволяючи навіть малим підприємствам використовувати передові рішення без значних капіталовкладень. Отже, цифровізація підприємств у комплексі з кібербезпекою та екологічною відповідальністю постають однією з важливих задач сучасності.

Аналіз останніх досліджень і публікацій. Дослідження інтегрованої цифровізації підприємств є міждисциплінарною темою, яка охоплює внесок багатьох вчених і практиків. У світі над цією проблемою працює велика кількість дослідників, які зробили значний внесок у розробку цифровізації підприємств, зокрема в контексті малих і середніх підприємств (далі - МСП), інновацій, організаційних змін та технологічної інтеграції.

Shaofeng Wan та Hao Zhang, з компанії Fuzhou University of International Studies and Trade (Китай), вивчають вплив цифровізації на інноваційні результати МСП з системної перспективи, аналізуючи взаємозв'язки між цифровим впровадженням, цифровим драйвом і цифровою культурою [1].

Aylin Işık Yener, автор дослідження про

цифровізацію та її вплив на інновації та підприємництво, аналізує взаємодію цифрових технологій (ШІ, блокчейн, великі дані) з організаційною трансформацією та підприємницькими екосистемами [2].

Satyam Pathak та Amandeep Kaur, дослідники, які провели систематичний огляд літератури про взаємозв'язок цифровізації та соціального підприємництва, використовуючи TCCM-фреймворк для аналізу цифрових можливостей і стійкості організацій [3].

Jorge Anibal Restrepo-Morales, Jaime Andrés Ararat-Herrera, Diego Alejandro López-Cadavid, Aquileo Camacho-Vargas, автори дослідження про бар'єри та драйвери цифровізації МСП, використовуючи нечітку логіку (fuzzy logic) для оцінки впровадження цифрових технологій у колумбійському МСП [4].

Sari Nour та Anna Arbussà, дослідники, які вивчають інтеграцію передових цифрових технологій через організаційну реструктуризацію в провідній компанії-виробнику, акцентуючи на клієнтоорієнтованості та підвищенні операційної ефективності [5].

Momeena Mehdi, автор конференційної статті, яка аналізує сучасні тенденції цифровізації підприємств, зокрема вплив на ринкові структури, бізнес-моделі та інноваційні екосистеми [6].

Ці дослідники представляють різні регіони (Китай, Колумбія, Європа, США) та підходи, включаючи системну теорію, нечітку логіку, ресурсну теорію та аналіз підприємницьких екосистем. Їхні роботи зосереджені на різних аспектах цифровізації: від технологічного впровадження до організаційних змін і соціального впливу.

В Україні дослідження інтегрованої цифровізації підприємств є актуальною темою, яка активно розвивається в контексті економічних, технологічних і соціальних викликів, особливо з урахуванням воєнного стану та повоєнного відновлення. Серед українських дослідників, які зробили внесок у вивчення цифровізації підприємств такі імена, як: І. Губарева, Н. Белікова, О. Ягольницький [7], Л. Лазебник, В. Войтенко [8], автор монографії про інструментарій стратегічного управління в контексті цифрових трансформацій М.І. Чепелюк [9], М.О. Кравченко та В.О. Салабай [10], Н.М. Андріїв [11], Ю. Шкригун, Н. Трушкіна [12] та інші.

Ці дослідники представляють різні академічні установи, зокрема Науково-дослідний центр індустріальних проблем розвитку НАН України, НТУУ «Київський політехнічний інститут», НУХТ. Їхні роботи охоплюють теоретичні основи, практичні аспекти впровадження цифрових технологій, управління бізнес-процесами та вплив цифровізації на конкурентоспроможність.

Для України, внаслідок воєнного стану, а також з урахуванням потреб повоєнного відновлення країни, інтегрована цифровізація стає не просто трендом, а необхідною умовою для виживання та розвитку підприємств у сучасному світі. Вона дозволяє оптимізувати операції, адаптуватися до змін і створювати нові можливості для зростання. Для українських підприємств, враховуючи економічні та геополітичні виклики,

цифровізація стає стратегічним інструментом для підвищення стійкості й конкурентоспроможності.

Проте, попри очевидні переваги, інтегрована цифровізація потребує значних інвестицій, перебудови бізнес-процесів, навчання персоналу та забезпечення кібербезпеки. Недостатня готовність до змін або брак стратегічного підходу можуть знизити ефективність впровадження інтегрованої цифровізації підприємств.

Отже, **мета статті** полягає у розробці науково-обґрунтованих рекомендацій з цифровізації підприємництва, що враховують вимоги кібербезпеки та екологічної відповідальності в умовах воєнного та поствоєнного станів України.

Для досягнення цієї мети визначено наступні *завдання*:

- Аналіз теоретичних засад цифровізації підприємств, кібербезпеки та екологічної відповідальності.
- Оцінка сучасного стану цифрової трансформації, рівня кіберзахищеності та екологічної відповідальності підприємств.
- Розробка інтегрованої моделі цифровізації з компонентами кіберзахисту та екологічного моніторингу та рекомендації для впровадження розроблених рішень.

Виклад основних результатів дослідження.

Теоретичні засади цифровізації підприємств, кібербезпеки та екологічної відповідальності.

Цифровізація визначається як використання цифрових технологій для зміни бізнес-моделі та створення нових можливостей генерувати доходи і підвищувати цінність організації [13].

Поняття цифрової трансформації охоплює інтеграцію цифрових технологій у всі сфери діяльності підприємства, що призводить до кардинальних змін у

способах його функціонування й надання цінності клієнтам.

Підприємства можуть вдатися до цифрової трансформації з кількох причин, але, найімовірнішою причиною постає необхідність — це питання виживання. В умовах воєнного стану здатність організації швидко адаптуватися до перебоїв у ланцюжку постачань, тиску часу виходу на ринок та швидкозмінних очікувань клієнтів стала критично важливою. Цифровізація підприємств стимулює автоматизацію операцій, оптимізацію ланцюга постачання, персоналізацію клієнтського досвіду та розвиток онлайн-продажів [14].

Проте в умовах інтенсивної цифровізації, окрім очевидних переваг, перед підприємствами постає низка викликів, основним із яких є кібератаки, що вимагає залучення додаткових ресурсів для забезпечення кібербезпеки.

«Кібербезпека – це практика захисту систем, мереж і програм від цифрових атак. Такі кібератаки зазвичай спрямовані на отримання доступу до конфіденційної інформації, її зміну або знищення; вимагання грошей у користувачів за допомогою програм-вимагачів (ransomware); або порушення нормального функціонування бізнес-процесів» [15].

Отже, у контексті цифрової трансформації підприємств важливим аспектом є впровадження ефективної системи кібербезпеки. Одним із провідних інструментів у цій сфері є NIST Cybersecurity Framework, CSF, розроблена Національним інститутом стандартів і технологій США. NIST CSF надає структурований підхід до управління кіберризиками, допомагаючи організаціям ідентифікувати, захищати, виявляти, реагувати та відновлюватися після кіберінцидентів (рис. 1).

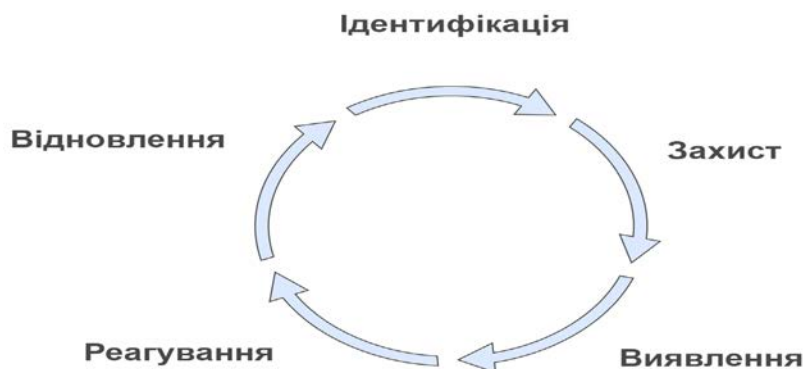


Рис. 1. Структура кібербезпеки

Джерело: узагальнено автором за інформацією [16].

Для кібербезпеки широко застосовуються стандарти ISO/IEC 27001 [17] та ISO/IEC 27002 [18], які визначають вимоги до систем управління інформаційною безпекою. Стандарт ISO 14001 регламентує систему екологічного менеджменту та встановлює вимоги для зниження екологічних ризиків і поліпшення екологічних показників організації. Крім того, в Україні діють національні ініціативи з розвитку цифрової безпеки та зеленої економіки, наприклад, урядова програма «Дія.Цифрова освіта» та національний план дій з імплементації ESG-принципів у бізнесі [19].

Водночас із викликами в сфері кібербезпеки сучасні підприємства стикаються з необхідністю дотримання екологічних стандартів і посилення своєї відповідальності перед суспільством та довкіллям. Тому цифрова трансформація має супроводжуватися не лише захистом інформаційних ресурсів, а й впровадженням принципів сталого розвитку.

Екологічна відповідальність бізнесу базується на концепції корпоративної стійкості, що інтегрує економічні, соціальні та екологічні аспекти діяльності.

Принципи екологічної відповідальності

передбачають зобов'язання підприємств:

- мінімізувати викиди CO₂ та інший негативний вплив на довкілля;
- оптимізувати використання ресурсів і впроваджувати практики циркулярної економіки;
- забезпечувати прозорість екологічної звітності та взаємодію з зацікавленими сторонами; принципи екологічної відповідальності в бізнес-процесах [20].

«Циркулярна економіка – це альтернатива традиційній лінійній економічній моделі, коли ресурси використовуються якомога довше, з них отримують максимальну цінність, а відходи повертаються з кінця ланцюга постачання на початок, даючи використаним матеріалам нове життя» [21].

Отже, в Україні існують необхідні умови на законодавчому рівні, в актах стандартизації, які уможливають інтегральну цифровізацію підприємств з урахуванням кібербезпеки та екологічної відповідальності.

Аналіз рівня цифровізації, кібербезпеки та

екологічної відповідальності підприємств.

Основою цифрової трансформації економіки є доступ до Інтернету. Він забезпечує можливість використання цифрових технологій, створює середовище для обміну інформацією, розвитку інновацій та інтеграції бізнес-процесів.

Частка підприємств, які мають доступ до мережі Інтернет, залишалася стабільно високою впродовж 2018-2024 рр. (рис. 2). У 2018 р. цей показник становив 88%, а до 2024 р. він зріс до 93,8%. Це свідчить про те, що Інтернет став базовою потребою для українських підприємств. Покращення доступу можна пояснити розвитком телекомунікаційної інфраструктури, особливо в умовах потреби дистанційної роботи та модернізації бізнес-процесів під час війни. Швидкість і доступність Інтернету визначають потенціал підприємств у впровадженні інноваційних технологій, таких як хмарні обчислення, Інтернет речей, штучний інтелект тощо.

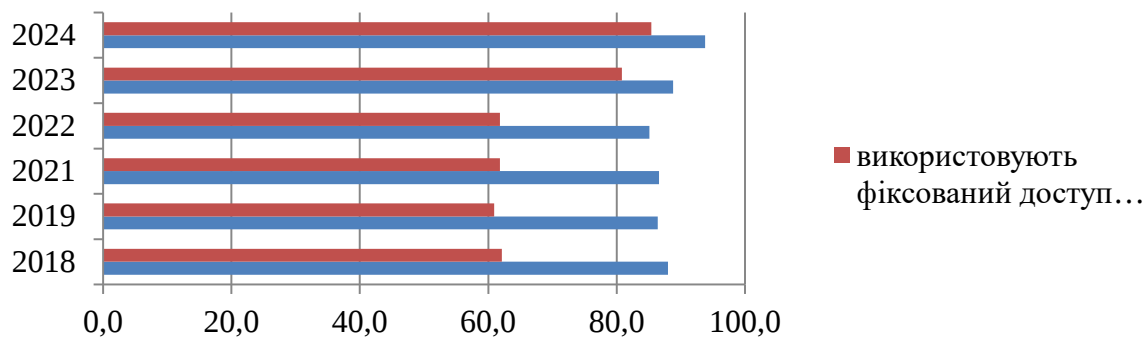


Рис. 2. Частка підприємств, які мають доступ до мережі Інтернет та фіксованого доступу до Інтернету.

Узагальнено автором за інформацією [22].

Проте, разом із технологічним прогресом зростає важливість кібербезпеки. Україна належить до числа країн, які стикаються з найбільшою кількістю кібератак у світі. Найпоширенішими типами кібератак є фішинг, програми-вимагачі та DDos. Згідно з дослідженням DataDriven Research & Consulting, повномасштабна війна спричинила сплеск кібератак в Україні, що збільшило попит на інноваційні технології та автоматизовані рішення [23].

Хакерські атаки переважно спрямовані на урядові

та місцеві органи, сектор енергетики, безпеки та оборони, комерційні організації тощо. Як зазначає Державна служба спеціального зв'язку та захисту інформації України: «Найпоширенішими типами інцидентів є розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису та компрометація системи» [24].

Так, у 2024 р. кількість кібератак на Україну сягнула 4315, що майже в двічі більше, аніж у 2022 р. – 2194 [25] (рис. 3).

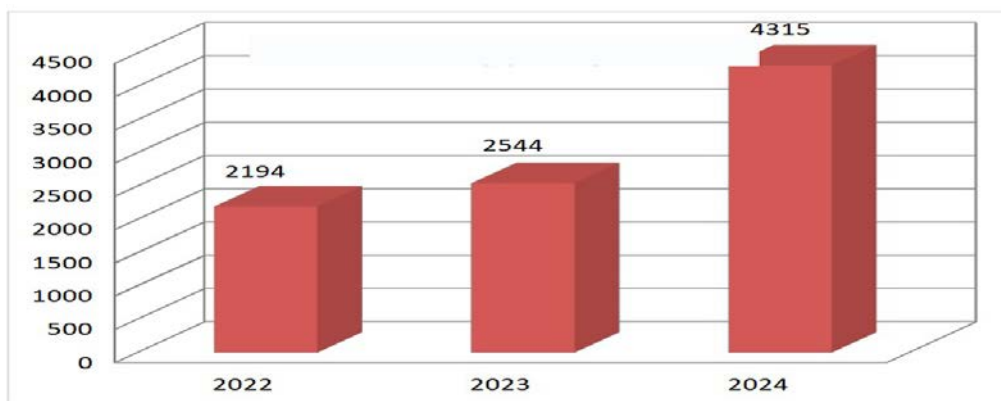


Рис. 3. Кількість кібератак на Україну

Джерело: узагальнено автором за інформацією [25].

Як наслідок, зростає потреба у впровадженні системного кіберзахисту на рівні держави та підприємств – від базових заходів (антивірусні програми та двофакторна автентифікація) до повноцінних структур кібербезпеки (наприклад NIST Cybersecurity Framework, CSF) [23].

Згідно з аналітичним оглядом Digital State, російське повномасштабне вторгнення стимулювало небажане зростання зацікавленості українського бізнесу в кіберзахисті, зокрема в автоматизованих рішеннях, продуктах на основі штучного інтелекту та інструментах управління вразливостями.

Сектор кібербезпеки почав активно інтегруватися у бізнес-моделі підприємств, особливо у тих, хто працює з критичними інфраструктурами або персональними

даними клієнтів.

За даними звіту IT Ukraine Association, на 2024 р. великі українські компанії витрачали близько 10-15% на кібербезпеку з загального річного бюджету. А невеликі компанії – більше 20%. У абсолютних значеннях на прикладі компаній розміром в 200 працівників витрати на кіберзахист склали \$98 000, тобто, приблизно \$500 на працівника.

Дані тенденції спонукають зростання українського ринку кібербезпеки. У період з 2016-2024 роки український ринок кібербезпеки зріс більш ніж у 4 рази із 32 млн. дол. США до 138 млн. дол. США і, за прогнозами, зростає ще на 50% до 2029 р. – до 209 млн. дол. США (рис. 4).

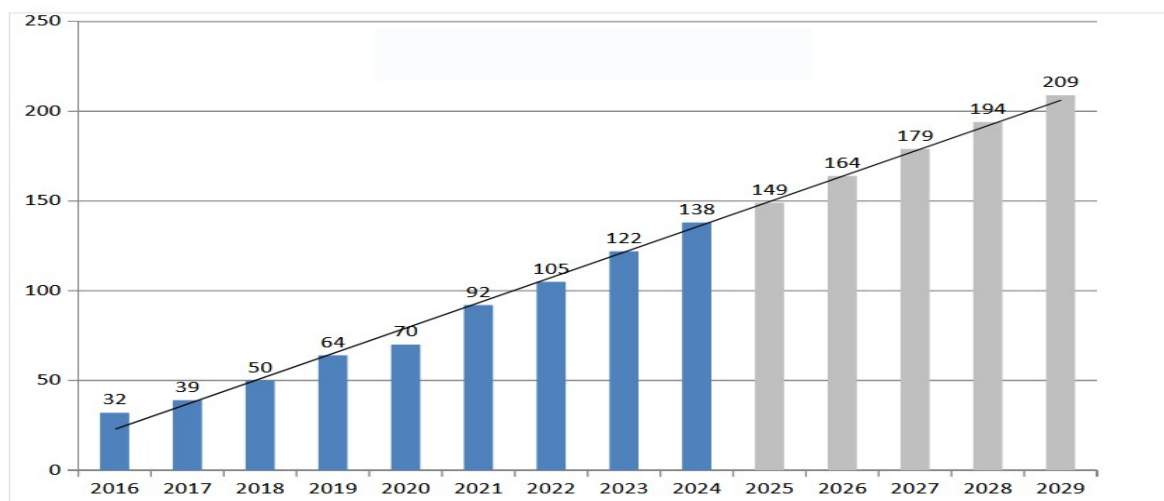


Рис. 4. Обсяг українського ринку кібербезпеки у 2016-2029 роках.

Джерело: узагальнено автором за інформацією [26].

Головними чинниками розвитку вітчизняного ринку є прискорена цифровізація та зростання реального ризику втрат через кібератаки. Фактичне перебування у стані кібервійни є основною причиною збільшення кількості кібератак. Сьогодні підприємства усіх секторів стикаються з сильними загрозами для своєї діяльності, через що змушені вкладати кошти в новітні рішення для кіберзахисту. При цьому, незважаючи на швидкі темпи зростання, частка України на світовому ринку кібербезпеки складає лише близько 0,07%.

Не менш важливим є впровадження екологічних ініціатив, що дозволяють мінімізувати вплив цифрової інфраструктури на довкілля. Тому паралельно з розбудовою кіберзахисту варто звернути увагу на «зелені» практики, які забезпечать стійкий розвиток підприємства.

«Екологічна відповідальність бізнесу – це зобов'язання компанії мінімізувати свій вплив на довкілля, використовуючи екологічно безпечні технології, ресурси та підходи у своїй діяльності» [27].

Ключові принципи екологічної відповідальності [28]:

1. Принцип інтеграції – передбачає, що при розробці економічних, соціальних чи технічних програм і проєктів має враховуватися вплив на довкілля.

2. Принцип превентивності – охоплює раннє виявлення та нейтралізацію потенційних загроз довікілью, перш ніж вони нанесуть реальну шкоду.

3. Принцип обережності – якщо є підстави вважати, що діяльність може завдати значної чи незворотної шкоди довкіллю, але наукові дані недостатні для повного підтвердження ризику, слід упроваджувати запобіжні заходи.

4. Принцип усунення джерела забруднення – передбачає впровадження технологій та практик, які не тільки знижують обсяги відходів, але й перезапуск процесів у такий спосіб, щоб джерело забруднення було усунене.

5. Принцип «забруднювач платить» – компанії або індивідууми, чий дії спричинили забруднення, мусить компенсувати витрати на ліквідацію його наслідків та відновлення довкілля.

За даними ISO Survey of Management System Standard Certifications у 2023 році в Україні всього 11 сертифікатів ISO 50001, що охоплюють 11 об'єктів [29].

Стандарт ISO 50001 – це міжнародний стандарт, розроблений Міжнародною організацією зі стандартизації (ISO), він визначає вимоги до систем управління енергоефективністю. Як зазначає сама організація:

«Отримання сертифіката ISO 50001 - це крок у майбутнє, де бізнес стає більш конкурентоспроможним, ефективним та екологічно відповідальним» [30].

Це свідчить про те, що впровадження енергоефективних систем управління в Україні наразі лише починається й охоплює обмежену кількість підприємств. Відповідно до звіту OECD (Організації економічної співпраці і розвитку) загальні надходження від екологічних податків в Україні у 2020 році становили близько 2 % ВВП. При цьому їхня частка в загальних надходженнях від податків та соціальних внесків досягала 5 %, що відповідає аналогічним показникам у низці країн ЄС. Надходження виключно від податків на забруднення (відходи, воду, повітря) становили лише 0,1 % ВВП, що також зіставно з середніми значеннями для ЄС.

«Екологічна відповідальність – не просто тренд, а необхідна умова для розвитку українського бізнесу» – Міністерство захисту довкілля та природних ресурсів України [31].

Інтегрована модель цифровізації підприємств з урахуванням кібербезпеки та екологічної відповідальності.

Зважаючи на вищеописане, нагальною є потреба у розробці моделі цифровізації підприємств з урахуванням кібербезпеки та екологічної відповідальності [32]. Одними із ключових чинників такої моделі є:

- енергоефективність;
- безперебійний доступ до електроенергії;
- ціна електроенергії.

У інтегрованій моделі цифровізації підприємств локальні ВДЕ-системи з'єднуються з цифровою платформою через API екологічного моніторингу: дані про вироблену «зелену» електроенергію автоматично враховуються в розрахунок вуглецевого сліду та коригуванні тарифів на внутрішнє енергоспоживання. Паралельно шар кібербезпеки слідує за безпечністю цих підключень, захищаючи мережу підприємства від зовнішніх атак на енергетичні вузли (рис. 5).

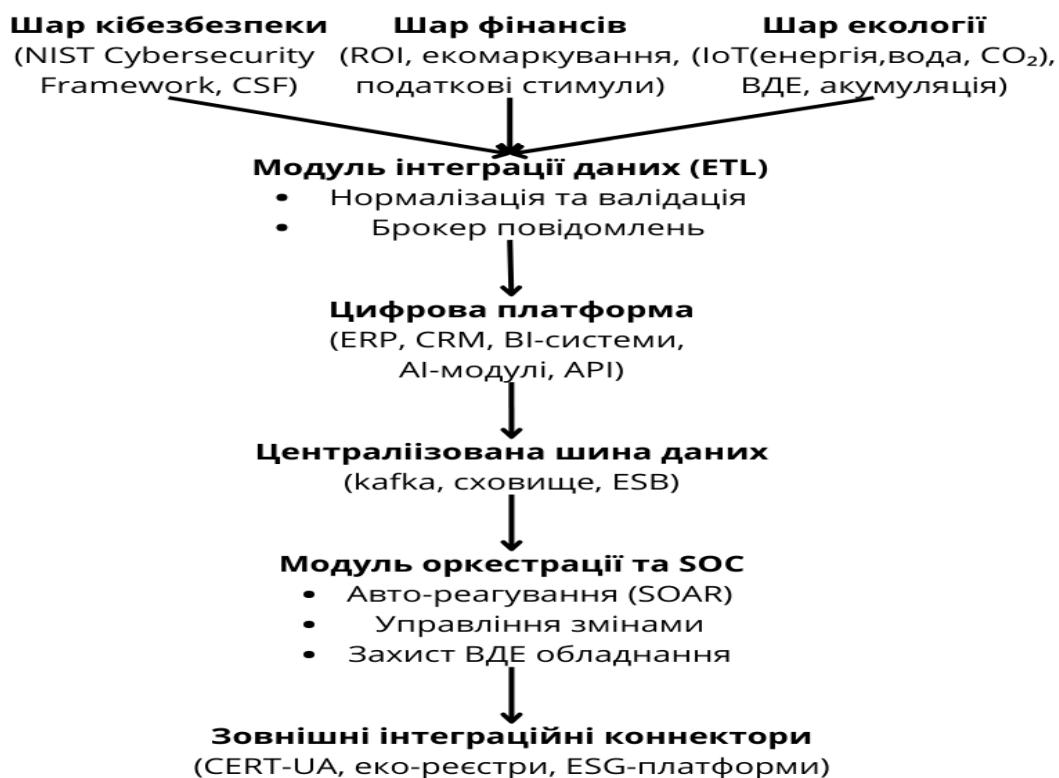


Рис. 5. Інтегрована модель цифровізації підприємства з урахуванням кібербезпеки та екологічної відповідальності.

Джерело: складено автором самостійно за джерелами [33, 34].

Запропонована модель складається із декількох ключових елементів:

1. Шари-джерела даних:

- Шар кібербезпеки – призначений для захисту інформаційних систем та даних від несанкціонованого доступу та атак; моніторингу і виявлення загроз; автоматизації реагування на інциденти та управління доступом та ідентифікації користувачів.
- Шар екології – потрібен для збору показників споживання ресурсів; інтеграції децентралізованих ВДЕ і систем накопичення енергії; забезпечення

стійкості енергопостачання.

- Шар фінансів – управління бюджетами та контролю витрат; оцінка ефективності інвестицій; підготовка ESG-звітності для інвесторів.

2. Модуль інтеграції даних (ETL) – відповідає за «очищення» даних, тобто трансформацію даних із різних джерел до єдиного формату й завантаження в цифрову платформу.

3. Цифрова платформа – це центральний вузол, який об'єднує аналітичні та бізнес сервіси (CRM, ERP, BI-системи) та API для внутрішніх і зовнішніх

клієнтів.

4. Централізована шина даних – служить для обміну «очищеними» даними платформою та операційними модулями. Забезпечує високу пропускну спроможність [33].

5. Модуль оркестрації – поєднує можливості SOAR (автоматизації реагування на інциденти) [34] і Change Management (управління процесами та навчання персоналу).

6. Зовнішні інтеграційні конектори – включає API-інтерфейси до держреєстрів та екологічних баз для автоматичного оновлення даних та звірки показників.

Перевагами даної моделі є:

1. Єдність інформації – ETL гарантує, що всі підсистеми працюють з достовірними даними.

2. Модульність – кожний елемент можна розвивати незалежно, не порушуючи загальну архітектуру моделі.

3. Автоматизоване реагування – запропонована модель передбачає автоматизацію відновлення сервісів та збирання інформації.

4. Повний енергетичний цикл – ВДЕ та акумуляція забезпечують безперебійність та зниження витрат на електроенергію.

5. Відповідність стандартам – впровадження запропонованої моделі спрощує сертифікацію та взаємодію з регуляторами.

Проте, варто зазначити, і про слабкі сторони моделі, насамперед це висока вартість впровадження. Вирішенням даної проблеми може бути: впровадження хмарних сервісів замість капітальних інвестицій та залучення грантових коштів від держави та міжнародних організацій [35].

Висновки. Проведене дослідження демонструє, що

цифровізація підприємств із одночасним впровадженням систем кібербезпеки та екологічної відповідальності створює синергетичний ефект, який підсилює фінансову стійкість та економічну ефективність бізнесу. Також створює нові можливості для підвищення їхньої конкурентоспроможності та продуктивності в умовах воєнного стану. Сертифікація стандартами ISO/IEC 27001, ISO/IEC 27002, ISO 14001 закладають необхідну основу для інтеграції українських підприємств у європейську та глобальну економіку.

Аналіз сучасного стану діджиталізації підприємств України показав позитивну динаміку інтеграції цифрових технологій. Частка підприємств, які використовують фіксований доступ до мережі Інтернет, значно зростає, а впровадження високошвидкісного Інтернету поступово набуває поширення. Однак відставання від європейських країн залишається значним, особливо серед малих підприємств, які часто обмежені у фінансових та кадрових ресурсах для реалізації цифрових стратегій. А, отже, український бізнес потребує великих інвестицій, податкових стимулів та допомоги держави.

Запропонована модель з трьома шарами-джерелами, модулем ETL, централізованою шиною даних, модулем оркестрації та SOC, а також зовнішніми конекторами до CERT-UA та еко-реєстрів забезпечує єдність інформації, гнучкість масштабування та автоматизацію процесів. Впровадження хмарних сервісів, етапне впровадження та залучення грантового фінансування допомагають подолати бюджетні та кадрові бар'єри.

Отже, синергія цифровізації, кіберзахисту та екологічних практик формує конкурентну перевагу, особливо в умовах воєнного стану: підприємства отримують стійкість операцій, підвищену фінансову віддачу й зменшений екологічний вплив.

Список використаних джерел:

1. Wang, S., & Zhang, H. (2025). Digital Transformation and Innovation Performance in Small-and Medium Sized Enterprises: A Systems Perspective on the Interplay of Digital Adoption, Digital Drive, and Digital Culture. *Systems*, No. 13. P. 43. DOI: <https://doi.org/10.3390/systems13010043>
2. Aylin Işık Yener. (2025). Digitalization: Reshaping Innovation and Entrepreneurship. *Human Computer Interaction*, Vol. 9 No. 1. DOI: <https://doi.org/10.62802/hz97r764>
3. Pathak, S., & Kaur, A. (2025). Mapping the intersection of digitalization and social entrepreneurship: a systematic literature review using the TCCM framework. *Futur Bus J*, No. 11. P. 144. DOI: <https://doi.org/10.1186/s43093-025-00565-z>.
4. Restrepo-Morales, J.A., Ararat-Herrera, J.A., López-Cadavid, D.A. et al. (2024). Breaking the digitalization barrier for SMEs: a fuzzy logic approach to overcoming challenges in business transformation. *J Innov Entrep*, No. 13. P. 4. DOI: <https://doi.org/10.1186/s13731-024-00429-w>
5. Sari Nour, & Anna Arbussà; (2024). Driving innovation through organizational restructuring and integration of advanced digital technologies: a case study of a world-leading manufacturing company. *European Journal of Innovation Management*. DOI: <https://doi.org/10.1108/EJIM-02-2024-0156>
6. Mehdi, M. (2025). The Situation of Digitalization in Enterprises: Analyzing Current Trends and Practices. In: Dhoska, K., Spaho, E. (eds) *Bridging Horizons in Artificial Intelligence, Robotics, Cybersecurity, Smart Cities, and Digital Economy*. ICITBT 2024. Sustainable Economy and Ecotechnology. Springer, Cham. Pp. 171-180. DOI: https://doi.org/10.1007/978-3-031-72029-1_14
7. Губарева, І., Белікова, Н., Ягольницький, О. (2024). Управління цифровою трансформацією підприємства. *Економіка та суспільство*, № 64. DOI: <https://doi.org/10.32782/2524-0072/2024-64-46>
8. Лазебник Л.Л., Войченко В.О. (2020). Інформаційна інфраструктура в цифровізації бізнес-процесів підприємства. *Науковий вісник Міжнародного гуманітарного університету*. Вип. 42. С. 18–22. URL: <http://www.vestnik-econom.mgu.od.ua/journal/2020/42-2020/5.pdf>

9. Чепелюк М.І. (2021). Інструментарій стратегічного управління в контексті сучасних концепцій та трендів світового економічного розвитку: монографія. Харків: ФОП Лібуркіна Л.М., 396 с. URL: <https://repository.hneu.edu.ua/handle/123456789/29911>
10. Кравченко М.О., Салабай В.О. (2023). Роль цифрових трансформацій бізнес-процесів підприємств. Економічний вісник НТУУ КПІ, № 26. DOI: <https://doi.org/10.20535/2307-5651.26.2023.286988>
11. Андрійв Н.М. (2022). Цифрова трансформація підприємства: теоретичний базис. Ефективна економіка, № 4. DOI: <https://doi.org/10.32702/2307-2105-2022.4.79>
12. Шкригун Ю., Трушкіна Н. (2022). Цифрова трансформація бізнес-процесів: зарубіжна практика. II International Scientific and Practical Conference «Grundlagen der modernen wissenschaftlichen forschung», (Zurich. Switzerland, August 12, 2022). Цюріх. DOI: <https://doi.org/10.36074/logos-12.08.2022.14>
13. Digitalization. Gartner. URL: <https://www.gartner.com/en/information-technology/glossary/digitalization>
14. Wang, Z., etc. (2023). Digitalization Effect on Business Performance: Role of Business Model Innovation. Sustainability, Vol. 15 No. 11. DOI: <https://doi.org/10.3390/su15119020>
15. What is cybersecurity?. Cisco. URL: <https://surl.lu/ypbmfr>
16. Olaes, T. (2025). What is the NIST Cybersecurity (CSF) 2.0 Framework?. Balbix. URL: <https://www.balbix.com/insights/nist-cybersecurity-framework/>
17. ISO 27001:2022 – Information security management system (isms). URL: <https://surl.li/hkuujm1>
18. ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Controls – Changes and Implementation Training Course. URL: <https://surl.lu/mhjjes>
19. ESG для бізнесу й держави: правила та інструменти відповідального управління. (2025). Офіс зеленого переходу. URL: <https://surl.li/izdbuk>
20. Beattie, A. (2024). The 3 Pillars of Corporate Sustainability. Investopedia. URL: <https://surl.li/xgeclm>
21. Циркулярна економіка в Україні. Центр ресурсоефективного та чистого виробництва. URL: <https://www.recpc.org/circular-economy-ua/>
22. Використання інформаційно-комунікаційних технологій на підприємствах: використання мережі інтернет, програмного забезпечення для бізнесу, послуг хмарних обчислень, штучного інтелекту. Державна служба статистики України. URL: https://ukrstat.gov.ua/operativ/operativ2018/zv/ikt/arh_ikt_u.html
23. Ukraine Leading in Cybersecurity Resilience. (2025). Digital State UA. URL: <https://digitalstate.gov.ua/news/tech/ukraine-leading-in-cybersecurity-resilience>
24. Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти. (2024). Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti>
25. Дячук К. (2025). У 2024 році кількість кібератак на Україну зросла на 70%. Інститут масової інформації. URL: <https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931>
26. Український ринок кібербезпеки зріс у чотири рази за вісім років. (2025). IT Ukraine Association. URL: <https://itukraine.org.ua/ukrayinskij-rinok-kiberbezpeki-zris-u-chotiri-razi-za-visim-rokiv/>
27. Що таке екологічна відповідальність бізнесу і чому це важливо. (2025). Щедрий Вівторок. URL: <https://surl.li/blzyhn>
28. Winfried, L. (1999). UN-Principles and International Environmental Law. Max Planck Yearbook Of United Nations Law. 3rd ed. P. 172.
29. Survey of certifications to management system standards. International Organization for Standardization. URL: <https://surl.li/anoahs>
30. ISO 50001. ISO-Certify. URL: <https://iso-certify.com/ua/iso-50001/>
31. Екологічна відповідальність – не просто тренд, а необхідна умова для розвитку українського бізнесу. (2025). Міністерство захисту довкілля та природних ресурсів України. URL: <https://surl.li/wuzldd>
32. Легін О.В. Інтегрована модель цифровізації підприємств з урахуванням кібербезпеки та екологічної відповідальності. VII Міжнародна науково-практична інтернет-конференція «Integration of Education, Science and Business in Modern Environment: Summer Debates», (Дніпро, 7-8 серпня 2025). Дніпро: FOP Marenichenko V.V., Dnipro, С. 159-161.
33. What is a Computer Bus?. (2025). GeeksforGeeks. URL: <https://www.geeksforgeeks.org/what-is-a-computer-bus/>
34. Що таке операційний центр безпеки (SOC)?. Microsoft. URL: <https://surl.li/vazuok>
35. Гранти 2025. Центр розвитку Час змін.. URL: <https://chaszmin.com.ua/granty-2025/>

References:

1. Wang, S., & Zhang, H. (2025). Digital Transformation and Innovation Performance in Small-and Medium Sized Enterprises: A Systems Perspective on the Interplay of Digital Adoption, Digital Drive, and Digital Culture. Systems, No. 13. P. 43. DOI: <https://doi.org/10.3390/systems13010043> [in English].
2. Aylin Işık Yener. (2025). Digitalization: Reshaping Innovation and Entrepreneurship. Human Computer Interaction, Vol. 9 No. 1. DOI: <https://doi.org/10.62802/hz97r764> [in English].

3. Pathak, S., & Kaur, A. (2025). Mapping the intersection of digitalization and social entrepreneurship: a systematic literature review using the TCCM framework. *Futur Bus J*, No. 11. P. 144. DOI: <https://doi.org/10.1186/s43093-025-00565-z> [in English].
4. Restrepo-Morales, J.A., Ararat-Herrera, J.A., López-Cadavid, D.A. et al. (2024). Breaking the digitalization barrier for SMEs: a fuzzy logic approach to overcoming challenges in business transformation. *J Innov Entrep*, No. 13. P. 4. DOI: <https://doi.org/10.1186/s13731-024-00429-w> [in English].
5. Sari Nour, & Anna Arbussà; (2024). Driving innovation through organizational restructuring and integration of advanced digital technologies: a case study of a world-leading manufacturing company. *European Journal of Innovation Management*. DOI: <https://doi.org/10.1108/EJIM-02-2024-0156> [in English].
6. Mehdi, M. (2025). The Situation of Digitalization in Enterprises: Analyzing Current Trends and Practices. In: Dhoska, K., Spaho, E. (eds) *Bridging Horizons in Artificial Intelligence, Robotics, Cybersecurity, Smart Cities, and Digital Economy*. ICITBT 2024. Sustainable Economy and Ecotechnology. Springer, Cham. Pp. 171-180. DOI: https://doi.org/10.1007/978-3-031-72029-1_14 [in English].
7. Hubarieva, I., Bielikova, N., & Yaholnytskyi, O. (2024). Upravlinnia tsyfrovou transformatsiieiu pidpriemstva [Managing the Digital Transformation of an Enterprise]. *Economy and Society*, No. 64. DOI: <https://doi.org/10.32782/2524-0072/2024-64-46> [in Ukrainian].
8. Lazebnyk, L.L., & Voitenko, V.O. (2020). Informatsiina infrastruktura v tsyfrovizatsii biznes-protsesiv pidpriemstva [Information infrastructure in the digitalization of business processes of an enterprise.] *Scientific Bulletin of the International Humanitarian University*. Iss. 42. Pp. 18–22. Retrieved from: <http://www.vestnik-econom.mgu.od.ua/journal/2020/42-2020/5.pdf> [in Ukrainian].
9. Chepelyuk, M.I. (2021). Instrumentariy strategichnogo upravlinnya v konteksty suchasnih koncepciy ta trendiv svitovogo ekonomichnogo rozvitku [Strategic Management Toolkit in the Context of Modern Concepts and Trends in World Economic Development]: monograph. Kharkiv: FOP Liburkina L.M., 396 p. Retrieved from: <https://repository.hneu.edu.ua/handle/123456789/29911> [in Ukrainian].
10. Kravchenko, M., & Salabai, V. (2023). Rol cifrovih transformatiy bisnes-prosesiv pidpriemstv [The role of digital transformations of business processes of enterprises]. *Economic Bulletin of NTUU KPI*, No. 26. DOI: <https://doi.org/10.20535/2307-5651.26.2023.286988> [in Ukrainian].
11. Andriyiv, N.M. (2022). Cifrova transformacia pidpriemstva: teoretichnyi basis [Digital transformation of the enterprise: theoretical basis]. *Effective economy*, No. 4. DOI: <https://doi.org/10.32702/2307-2105-2022.4.79> [in Ukrainian].
12. Shkrigun, Yu., & Trushkina, N. (2022). Cifrova transformacia biznes-procesiv : zarubigna praktika [Digital transformation of business processes: foreign practice]. II International Scientific and Practical Conference «Grundlagen der modernen wissenschaftlichen forschung», (Zurich. Switzerland, August 12, 2022). DOI: <https://doi.org/10.36074/logos-12.08.2022.14> [in Ukrainian].
13. Digitalization. Gartner. Retrieved from: <https://www.gartner.com/en/information-technology/glossary/digitalization>.
14. Wang, Z., etc. (2023). Digitalization Effect on Business Performance: Role of Business Model Innovation. *Sustainability*, Vol. 15 No. 11. DOI: <https://doi.org/10.3390/su15119020> [in English].
15. What is cybersecurity?. Cisco. Retrieved from: <https://surl.lu/ypbmfr>
16. Olaes, T. (2025). What is the NIST Cybersecurity (CSF) 2.0 Framework?. Balbix. Retrieved from: <https://www.balbix.com/insights/nist-cybersecurity-framework/> [in English].
17. ISO 27001:2022 – Information security management system (isms). Retrieved from: <https://surl.li/hkuujm>
18. ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Controls – Changes and Implementation Training Course. Retrieved from: <https://surl.lu/mhjjes>
19. ESG dla biznesu y derzhavy: pravyla ta instrumenty vidpovidalnoho upravlinnia [ESG for Business and Government: Rules and Instruments for Responsible Governance]. (2025). Green Transition Office. Retrieved from: <https://surl.li/izdbuk> [in Ukrainian].
20. Beattie, A. (2024). The 3 Pillars of Corporate Sustainability. Investopedia. Retrieved from: <https://surl.li/xgeclm> [in English].
21. Tsyrukliarna ekonomika v Ukraini [Circular Economy in Ukraine]. Resource Efficient and Cleaner Production Center. Retrieved from: <https://www.recpc.org/circular-economy-ua/> [in Ukrainian].
22. Vykorystannia informatsiino-komunikatsiinykh tekhnolohii na pidpriemstvakh: vykorystannia merezhi internet, prohramnoho zabezpechennia dla biznesu, posluh khmarnykh obchyslen, shtuchnoho intelektu [Use of information and communication technologies in enterprises: use of the Internet, business software, cloud computing services, artificial intelligence]. State Statistics Service of Ukraine. Retrieved from: https://ukrstat.gov.ua/operativ/operativ2018/zv/ikt/arh_ikt_u.html [in Ukrainian].
23. Ukraine Leading in Cybersecurity Resilience. (2025). Digital State UA. Retrieved from: <https://digitalstate.gov.ua/news/tech/ukraine-leading-in-cybersecurity-resilience>
24. Uriadova komanda CERT-UA v 2023 rotsi opratsiuvala 2543 kiberintsydeny. The government team CERT-UA processed 2543 cyber incidents in 2023]. (2024). State Service for Special Communications and Information

Protection of Ukraine. Retrieved from: <https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti> [in Ukrainian].

25. Diachuk K. (2025). U 2024 rotsi kilnist kiberatak na Ukrainu zroslo na 70% [In 2024, the number of cyberattacks on Ukraine increased by 70%]. Institute of Mass Information. Retrieved from: <https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zroslo-na-70-i65931> [in Ukrainian].

26. Ohliad rynku kiberbezpeky v Ukraini [Ukrainian cybersecurity market has grown fourfold in eight years]. (2025). IT Ukraine Association. Retrieved from: <https://itukraine.org.ua/ukrayinskij-rinok-kiberbezpeki-zris-u-chotiriraz-za-visim-rokiv/> [in Ukrainian].

27. Shcho take ekolohichna vidpovidalnist biznesu i chomu tse vazhlyvo [What is the environmental responsibility of business and why is it important?] (2025). Giving Tuesday. Retrieved from: <https://surl.li/blzyhn> [in Ukrainian].

28. Winfried, L. (1999). UN-Principles and International Environmental Law. Max Planck Yearbook Of United Nations Law. 3rd ed. P. 172. [in English].

29. Survey of certifications to management system standards. International Organization for Standardization. Retrieved from: <https://surl.li/anoahys>

30. ISO 50001. ISO-Certify. Retrieved from: <https://iso-certify.com/ua/iso-50001/>

31. Ekolohichna vidpovidalnist – ne prosto trend, a neobkhdna umova dlia rozvytku ukrainskoho biznesu [Environmental responsibility is not just a trend, but a necessary condition for the development of Ukrainian business]. (2025). Ministry of Environmental Protection and Natural Resources of Ukraine. Retrieved from: <https://surl.li/wuzldd> [in Ukrainian].

32. Lehin, O.V. (2025). Intehrovana model tsyfrovizatsii pidpriemstv z urakhuvanniam kiberbezpeky ta ekolohichnoi vidpovidalnosti [Integrated model of enterprise digitalization taking into account cybersecurity and environmental responsibility]. VII International scientific and practical online conference «Integration of Education, Science and Business in Modern Environment: Summer Debates», (Dnipro, August 7-8, 2025). Dnipro: FOP Marenichenko V.V., Dnipro, Pp. 159-161.

33. What is a Computer Bus?. (2025). GeeksforGeeks. Retrieved from: <https://www.geeksforgeeks.org/what-is-a-computer-bus/>

34. Shcho take operatsiinyi tsentr bezpeky (SOC)?. Microsoft. Retrieved from: <https://surl.li/vazuok>

35. Hranty 2025. Tsentr rozvytku ChAS ZMIN. Retrieved from: <https://chaszmin.com.ua/granty-2025/>