Стала економіка

УДК: 005.93:004:332.1

DOI https://doi.org/10.5281/zenodo.20138139

Підвищення рівня інформаційної безпеки переробних підприємств в умовах «зеленого» розвитку економіки

Косінський Петро Миколайович,
доктор філософії, доцент,
доцент кафедри економіки,
Луцький національний технічний університет,
м. Луцьк, Україна, https://orcid.org/0000-0002-3254-2379

Малишко Сергій Олександрович,
аспірант,
Луцький національний технічний університет,
м. Луцьк, Україна, https://orcid.org/0009-0003-6989-8517

Прийнято: 21.04.2026 | Опубліковано: 30.04.2026

Анотація: *Метою статті є обґрунтування теоретичних і прикладних засад підвищення рівня інформаційної безпеки переробних підприємств в Україні в умовах «зеленого» розвитку економіки та визначення ролі економічних інструментів у забезпеченні їх інформаційної стійкості. Дослідження спрямоване на виявлення взаємозв'язку між процесами цифровізації, «екологізації» та трансформацією підходів до формування політики*

інформаційної безпеки підприємств переробної галузі в умовах «зеленого» розвитку.

Методологічною основою дослідження є системний підхід, економіко-статистичний аналіз, методи порівняння, узагальнення та логічного моделювання. Застосування зазначених методів дозволило здійснити оцінку сучасного стану цифровізації переробних підприємств в нашій державі, проаналізувати рівень забезпечення їх кадровими ресурсами у сфері ІКТ, а також визначити ступінь впровадження заходів інформаційної безпеки та екологічно орієнтованих ІКТ-рішень.

У результаті дослідження встановлено, що розширення доступу працівників до мережі Інтернет та активне використання цифрових технологій супроводжується зростанням інформаційних ризиків, що потребує посилення системи їх управління. Виявлено тенденцію до зниження частки підприємств, що мають власних ІКТ-фахівців, що свідчить про обмеженість кадрового потенціалу у сфері інформаційної безпеки. Доведено наявність дисбалансу між рівнем застосування технічних заходів безпеки та їх нормативним забезпеченням, що проявляється у низькій частці підприємств, які мають формалізовані політики та процедури захисту інформації. Обґрунтовано, що інтеграція інформаційної безпеки у систему «зеленого» розвитку є необхідною умовою підвищення конкурентоспроможності підприємств. Визначено пріоритетні напрями економічного стимулювання підвищення рівня інформаційної безпеки. Доведено, що ефективна політика інформаційної безпеки має формуватися на основі поєднання організаційних, технологічних та економічних інструментів з урахуванням стратегічних цілей підприємства.

Отримані результати підтверджують досягнення поставленої мети та формують підґрунтя для подальших досліджень у напрямі розробки

ISSN: 2786-9431

інтегрованих моделей управління інформаційною безпекою в умовах сталого розвитку.

Ключові слова: *інформаційна безпека, переробні підприємства, цифровізація, інформаційно-комунікаційні системи і технології, ІКТ, кіберризики, політика інформаційної безпеки, «зелений» розвиток, «зелена» економіка, економічне стимулювання, екологізація.*

Enhancing the Level of Information Security of Processing Enterprises under Conditions of "Green" Economic Development

Petro Kosinskyi,
PhD in Economics, Associate Professor,
Associate Professor of the Department of Economics,
Lutsk National Technical University,
Lutsk, Ukraine, https://orcid.org/0000-0002-3254-2379

Serhii Malyshko,
Postgraduate Student,
Lutsk National Technical University,
Lutsk, Ukraine, https://orcid.org/0009-0003-6989-8517

Abstract: *The purpose of the article is to substantiate the theoretical and applied foundations for enhancing the level of information security of processing enterprises in Ukraine under the conditions of "green" economic development and to determine the role of economic instruments in ensuring their information resilience. The study is aimed at identifying the interrelation between digitalization processes, "greening,"*

and the transformation of approaches to the formation of information security policy at processing enterprises within the framework of "green" development.

The methodological basis of the research is a systemic approach, economic and statistical analysis, as well as methods of comparison, generalization, and logical modeling. The application of these methods made it possible to assess the current state of digitalization of processing enterprises in Ukraine, to analyze the level of their staffing with ICT specialists, and to determine the extent of implementation of information security measures and environmentally oriented ICT solutions.

The results of the study indicate that the expansion of employees' access to the Internet and the active use of digital technologies are accompanied by an increase in information risks, which necessitates strengthening their management systems. A downward trend in the share of enterprises employing in-house ICT specialists has been identified, indicating limitations in human resource capacity in the field of information security. An imbalance between the level of implementation of technical security measures and their regulatory support has been proven, manifested in the low share of enterprises with formalized information protection policies and procedures. It is substantiated that the integration of information security into the system of "green" development is a necessary condition for enhancing enterprise competitiveness. Priority directions for economic stimulation of information security improvement have been identified. It is demonstrated that an effective information security policy should be formed through a combination of organizational, technological, and economic instruments, taking into account the strategic objectives of the enterprise.

The obtained results confirm the achievement of the stated goal and provide a basis for further research aimed at developing integrated models of information security management in the context of sustainable development.

ISSN: 2786-9431

Keywords: *information security, processing enterprises, digitalization, information and communication systems and technologies, ICT, cyber risks, information security policy, "green" development, green economy, economic incentives, greening.*

Постановка проблеми. Стрімке поширення сучасних інформаційно-комунікаційних технологій формує нові підходи до використання інформаційно-комунікаційних систем в економіці та стимулює цифрову трансформацію підприємств у регіонах нашої держави, що надає особливої актуальності питанню належного захисту їх інформаційних ресурсів. Вітчизняні підприємства поступово пристосовуються до роботи в оновленому інформаційному середовищі, враховуючи всі фактори, що впливають на їх економічну безпеку. Проте, посилення несанкціонованого впливу на інформаційні активи в системі управління підприємствами й процеси «зеленої» трансформації, що супроводжуються впровадженням нових цифрових рішень, екологічно орієнтованих технологій, обумовлює необхідність удосконалення політик та наявних систем захисту інформації.

Таким чином, виникає об'єктивна суперечність між необхідністю цифровізації та «екологізації» діяльності переробних підприємств і недостатнім рівнем адаптації їхніх систем інформаційної безпеки до нових умов функціонування. Розв'язання цієї проблеми має важливе як наукове, так і практичне значення.

Аналіз останніх досліджень і публікацій. Питання інформаційної безпеки підприємств посідає вагоме місце у сучасних економічних дослідженнях. Зокрема, М.А. Мащенко та Є.М. Іполітов [1] обґрунтовують необхідність формування цілісної стратегії захисту з урахуванням різнорівневих загроз, тоді

 ISSN: 2786-9431

як Д.В. Дячков [2] акцентує увагу на доцільності використання багаторівневих підходів, заснованих на концепції «глибинного захисту».

У свою чергу, М. Сороколіт [3] розглядає аудит як інструмент оцінювання ефективності систем безпеки, а Т.С. Перун [4] підкреслює значення належного нормативно-правового забезпечення цієї сфери.

У контексті поєднання безпекових і екологічних викликів Т.Ю. Білик та І.І. Максимова [5] доводять взаємозалежність безпеки, стійкості та конкурентоспроможності в умовах «зеленого» переходу, тоді як А.І. Ясінська [6] обґрунтовує необхідність системного підходу до захисту інформації. Додатково, В. Г. Бєлозерцев та В. В. Моргуненко [7] акцентують на зростанні кіберризиків у цифровій економіці та потребі їх комплексної мінімізації.

Попри значну кількість наукових праць, більшість із них зосереджена на технічних або організаційних аспектах інформаційної безпеки. При цьому, економічні механізми зміцнення інформаційної безпеки в умовах «зеленого» розвитку залишаються недостатньо розкритими, а їх інтеграція у систему управління підприємством має фрагментарний характер.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на вагомі наукові напрацювання, залишаються недостатньо дослідженими питання формування комплексних підходів до підвищення рівня інформаційної безпеки переробних підприємств з урахуванням специфіки «зеленого» розвитку. Зокрема, потребують подальшого обґрунтування економічні інструменти стимулювання впровадження сучасних систем кіберзахисту, інтеграція інформаційної безпеки у стратегії «зеленого» розвитку переробних підприємств, а також розробка методичних підходів до оцінювання ефективності таких заходів. Недостатньо уваги приділено також взаємозв’язку

ISSN: 2786-9431

між рівнем цифровізації, «екологізації» виробництва та інформаційною вразливістю підприємств.

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування теоретико-методичних засад та розробка практичних рекомендацій щодо підвищення рівня інформаційної безпеки переробних підприємств в умовах «зеленого» розвитку економіки.

Для досягнення поставленої мети визначено такі завдання: дослідити вплив цифровізації та «екологізації» діяльності підприємств на формування інформаційних ризиків; оцінити рівень цифрового розвитку та безпеки вітчизняних переробних підприємств на основі статистичних показників; обґрунтувати пріоритетні напрями й інструменти економічного стимулювання підвищення рівня інформаційної безпеки переробних підприємств в наші державі; сформувати відповідні висновки.

Виклад основного матеріалу дослідження. Сьогодні, в економічній системі нашої держави відбуваються зміни, зумовлені посиленою орієнтацією вітчизняних переробних підприємств на принципи «зеленого» розвитку. Такі трансформації сприяють розвитку «зеленої» інфраструктури й стимулюють впровадження сучасних цифрових рішень, що, у свою чергу, формує нову конфігурацію інформаційного середовища суб'єктів господарювання. За таких умов інформаційна складова діяльності переробних підприємств набуває стратегічного значення, що підвищує вимоги до рівня її безпеки.

Внаслідок зростання обсягів обробки даних, необхідності більш активнішого використання хмарних технологій, автоматизованих систем управління виробничою і логістичною системами, підвищується рівень вразливості вітчизняних переробних підприємств до можливих кіберзагроз й нових типів інформаційних ризиків[8; 9], що створює об'єктивну необхідність

ISSN: 2786-9431

оптимізації політики їхньої інформаційної безпеки.

Розвиток цифрових технологій і поширення цифровізації господарської діяльності суттєво трансформують інформаційне середовище переробних підприємств. За таких умов інформація набуває статусу стратегічно важливого ресурсу бізнесу, що підвищує її цінність та одночасно посилює інтерес до неї як до об'єкта потенційних загроз і неправомірного доступу [6].

З огляду на вище зазначене, інформаційні потоки стають не лише інструментом підвищення ефективності діяльності, але й джерелом нових ризиків, що вимагає системного підходу до їх управління. Водночас, інтеграція екологічно орієнтованих («зелених») технологій у виробничі процеси посилює залежність вітчизняних переробних підприємств від цифрової інфраструктури, що лише надає все більшої важливості питанню інформаційної безпеки.

Інформаційна безпека в умовах цифрової економіки набуває стратегічного значення, оскільки кібератаки створюють суттєві фінансові та репутаційні ризики для підприємств. У зв'язку з цим, заходи інформаційної безпеки повинні інтегруватися у загальну систему управління підприємством, а інвестиції у безпеку слід розглядати, як необхідну умову його подальшого економічного розвитку [7]. Виходячи з цього, стає зрозуміло, що рівень ефективності політики інформаційної безпеки визначатиме здатність вітчизняних переробних підприємств протистояти сучасним викликам у процесі «зеленого» розвитку.

Варто відзначити, що «зелений» розвиток економіки хоча не напряму, проте тісно пов'язаний із цифровою трансформацією, що передбачає активне впровадження інноваційних технологій у сфері енергоефективності та ресурсозбереження [10].

Така взаємодія створює, як додаткові можливості для підвищення конкурентоспроможності, так і нові загрози, пов'язані з кібербезпекою.

ISSN: 2786-9431

На думку Т.Ю. Білик та І.І. Максимової такі взаємозв'язки повинні зменшувати ймовірні ризики, що створюють загрозу економічній та інформаційній безпеці. Але як стверджують самі ж автори «загострення безпекових загроз, енергетична вразливість чи відставання у цифровій трансформації здатні одночасно послаблювати і стійкість, і здатність до збереження конкурентних позицій» [5].

Відповідно, формування політики інформаційної безпеки має здійснюватися з урахуванням екологічних пріоритетів розвитку переробного підприємства.

Проаналізуємо дані про кількість й динаміку частки зайнятих працівників, що працюють на вітчизняних переробних підприємствах та мають доступ до мережі Інтернет, адже це дозволить зробити певні висновки про розвиток цифрового середовища і зростання рівня залежності результатів їх діяльності від цифрових технологій (рис. 1).

За період 2018-2025 рр. кількість зайнятих працівників, що працюють на переробних підприємствах України і мають доступ до мережі Інтернет зросла на 68600 осіб (26,8%). За цей період також спостерігається зростання частки таких працівників на підприємствах переробної сфери, з 19,2% у 2018 році до 35,6% у 2025 році.

Тобто, в нашій державі більш ніж третина зайнятих працівників безпосередньо залучена до цифрового середовища переробних підприємств, що створює, як передумови для підвищення ефективності діяльності, так і суттєво розширює поле потенційних інформаційних загроз.

ISSN: 2786-9431

Рис. 1. Динаміка кількості та частки зайнятих працівників, що працюють на вітчизняних переробних підприємствах і мають доступ до мережі Інтернет за період 2018-2025 рр.

Джерело: сформовано автором на основі джерела [11]

Варто звернути увагу на те, що можливість віддаленого доступу до інформаційних систем працівників переробних підприємств, а також значний рівень використання мобільного інтернету та Wi-Fi інфраструктури, формують нові вектори ризиків, пов'язаних із несанкціонованим доступом й витоком інформації. Мається на увазі, що поширення бездротових і мобільних технологій, попри їх зручність, підвищує вразливість інформаційно-комунікаційних систем, що піднімає питання впровадження сучасних протоколів захисту даних. Тому, зростання гнучких форм організації праці об'єктивно потребує удосконалення механізмів захисту інформаційних ресурсів.

Порівняння частки переробних підприємств, що надають Wi-Fi доступ до

мережі Інтернет та використовують для цього мобільний зв'язок із часткою всіх підприємств, у загальній кількості підприємств, засвідчує достатньо високий рівень поширення сучасних форм підключення (рис. 2).

Рис.2. Порівняння частки переробних підприємств, що надають Wi-Fi доступ до мережі Інтернет та використовують для цього мобільний зв'язок із часткою всіх підприємств, у загальній кількості підприємств в Україні

Джерело: сформовано автором на основі джерела [11]

Зокрема, частка підприємств в Україні, що використовують мобільний доступ до мережі Інтернет, становить 48,8%, тоді як серед переробних підприємств цей показник становить 45,4%. Подібна ситуація спостерігається і щодо використання Wi-Fi доступу – частка всіх підприємств в державі складає 69,7%, тоді як частка підприємств у переробній галузі складає 67,7%

Хоч й вище зазначені показники свідчать про відносно високий рівень цифрової інфраструктури переробних виробництв в нашій державі, однак важливо відзначити, що поширення бездротових і мобільних технологій, попри

їх зручність, підвищує вразливість інформаційних систем.

«Інформаційна безпека підприємства має комплексний характер і охоплює сукупність організаційних, технічних і фізичних заходів, спрямованих на зниження ризиків й забезпечення стабільності його функціонування. Її ефективність досягається завдяки впровадженню інтегрованих систем захисту, дотриманню міжнародних стандартів, підготовці персоналу та систематичному контролю тощо» [3].

На думку М.А. Мащенко та Є.М. Іполітова основні функції інформаційної безпеки полягають у «забезпеченні безпечної роботи програмного забезпечення, реалізованої в системах інформаційних технологій будь-якого підприємства; здійсненні захисту даних, які підприємство збирає та використовує; захисті технологічних активів, що використовуються на підприємстві; захисті спроможності підприємства функціонувати» [1].

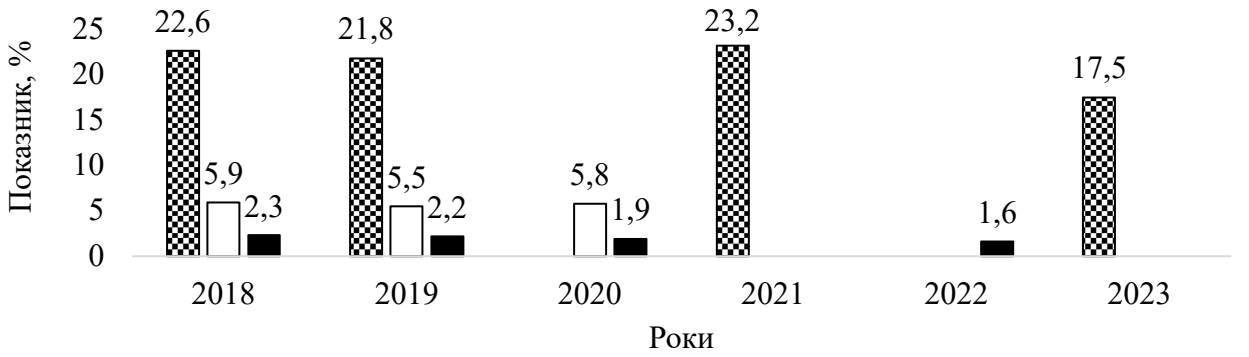
У даному контексті важливо зауважити, що технічні засоби захисту не можуть забезпечити належного рівня безпеки без відповідного організаційного забезпечення та підготовки кадрів. Саме тому важливу роль у забезпечені належного рівня переробних підприємств відіграє кадровий потенціал й рівень цифрових компетентностей працівників.

У забезпеченні інформаційної безпеки підприємства важливу роль відіграє технічна складова, проте вона не є вичерпною. З цього приводу, Д.В. Дячков слушно зазначає, наступне: «залишаються недостатньо вивченими питання, пов’язані з моделлю реалізації політики інформаційної безпеки з позиції досягнення мети бізнесу та застосування економічних методів управління інформаційними ризиками» [2], що, з рештою, лише посилює необхідність у розширенні способів її формування. З огляду на це, особливо в умовах «зеленої» трансформації, важливо розуміти, що політика інформаційної безпеки має

ISSN: 2786-9431

орієнтуватися не лише на технічний захист, а й на забезпечення економічної доцільності заходів безпеки.

Оцінка кадрового забезпечення вітчизняних переробних підприємств у сфері інформаційно-комунікаційних технологій (ІКТ) демонструє неоднозначні тенденції (рис. 3).



Частка кількості підприємств, що мають найманих фахівців у сфері ІКТ, у загальній кількості підприємств, %

Частка кількості підприємств, що наймали/намагалися наймати фахівців у сфері ІКТ, у загальній кількості підприємств, %

Частка кількості підприємств, що мали вакансії фахівців ІКТ, які складно було заповнити, у загальній кількості підприємств, %

Рис. 3. Стан кадрового забезпечення вітчизняних переробних підприємств у сфері інформаційно-комунікаційних технологій у 2018-2023 рр.

Джерело: сформовано автором на основі [11]

За період 2018-2023 рр. в Україні частка підприємств, що мають найманих ІКТ-фахівців, знизилася з 22,6% до 17,5% у 2023, що свідчить про скорочення внутрішнього кадрового потенціалу у сфері цифрової безпеки. Водночас частка переробних підприємств, які намагалися залучати таких фахівців, коливається в межах 5,5-6,5%, що вказує на наявність попиту, який не повною мірою задовольняється. Показник складності заповнення вакансій ІКТ-фахівців знизився з 2,3% 1,6%, що може інтерпретуватися як наслідок або зменшення попиту, або адаптації підприємств до альтернативних форм залучення

ISSN: 2786-9431

спеціалістів, зокрема аутсорсингу. У контексті інформаційної безпеки така ситуація свідчить про наявність системної кадрової проблеми, що обмежує можливості формування ефективної політики захисту інформації.

Також дуже важливим є проведення оцінки практичного впровадження заходів інформаційної безпеки. Попри те, що значна частка вітчизняних переробних підприємств застосовує певні технічні заходи захисту інформації, рівень формалізації політик безпеки та наявності відповідної документації залишається недостатнім, що свідчить про фрагментарний характер підходів до забезпечення інформаційної безпеки.

Розглянемо показники, що характеризують рівень заходів безпеки ІКТ на переробних підприємствах в нашій державі (рис. 4).

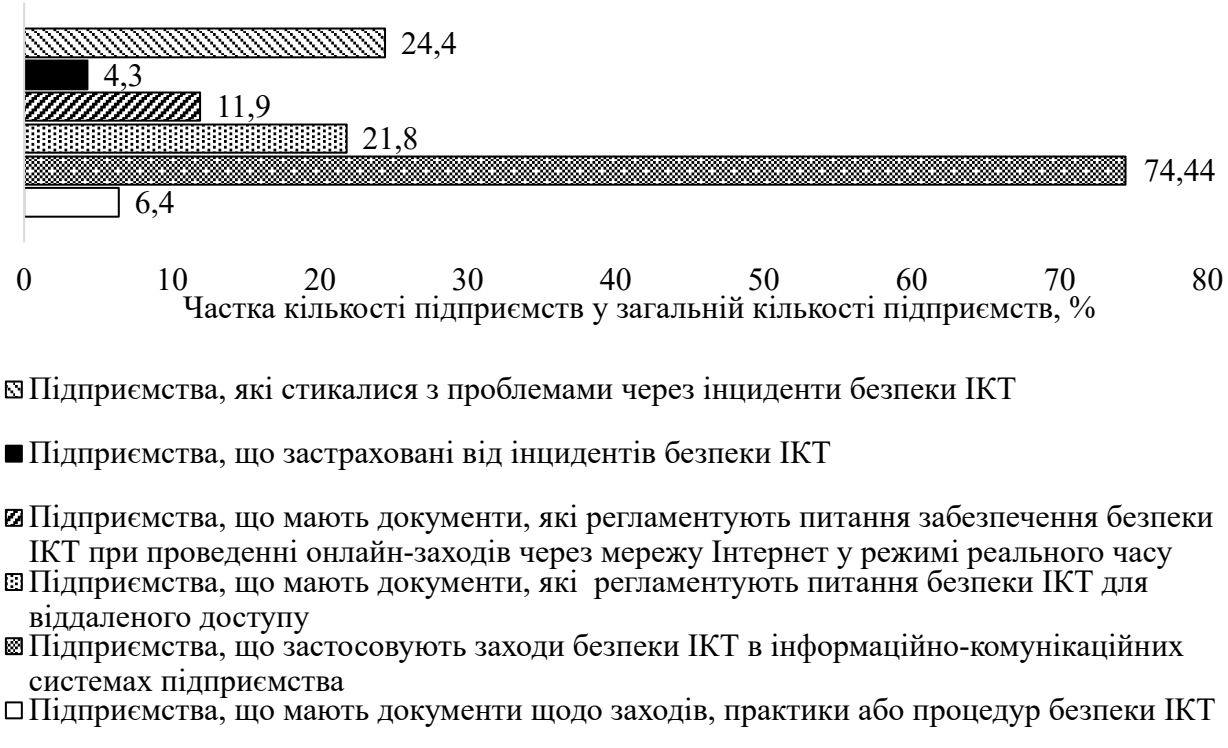


Рис. 4. Показники, що характеризують рівень заходів безпеки ІКТ на переробних підприємствах в Україні

Джерело: сформовано автором на основі [11]

ISSN: 2786-9431

В Україні 74,4% переробних підприємств використовують певні заходи захисту в інформаційно-комунікаційних системах, однак лише 6,4% мають документи, що регламентують відповідні процедури.

Крім того, лише 21,8% переробних підприємств мають документи, що регламентують питання безпеки для віддаленого доступу, а 11,9% – для проведення онлайн-заходів.

Враховуючи те, що частка переробних підприємств в Україні, які стикалися з проблемами через інциденти безпеки ІКТ становить 24,4% і лише 4,3% таких підприємств здійснюють страхування кіберризиків, можна говорити про наявність реальних загроз, недостатній рівень їх попередження та недостатню ефективність відповідних інструментів управління інформаційними ризиками.

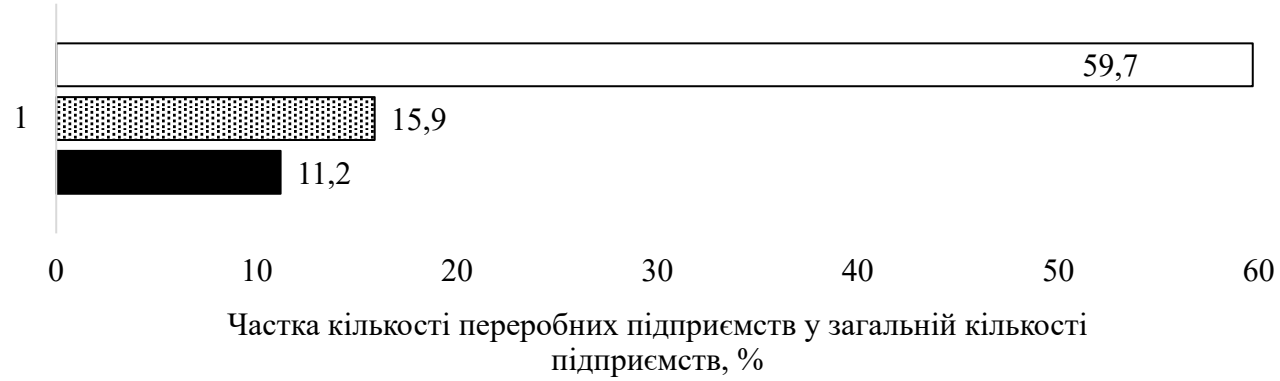
У процесі євроінтеграції для підвищення рівня інформаційної безпеки в умовах «зеленого» розвитку вітчизняним переробним підприємствам доцільно використовувати досвід європейських держав.

Для прикладу, політика інформаційної безпеки Європейського Союзу базується на скоординованій співпраці країн-учасниць у сфері інформаційно-комунікаційних технологій (ІКТ) та орієнтована на формування єдиного інформаційного простору. Її суть полягає у переході від традиційних підходів безпеки до пріоритетів інформаційного суспільства, що реалізується через діяльність міжнародних інституцій, покликаних протидіяти сучасним інформаційним викликам [4].

Показники, що характеризують рівень використання ІКТ у контексті «зеленого» розвитку свідчать про низький рівень впровадження ІКТ-рішень переробними підприємствами в нашій державі у сфері ресурсоефективності, а також вказують на недостатній рівень інтеграції цифровізації й «екологізації» їх діяльності (рис. 5).

ISSN: 2786-9431

На рисунку 5 видно, що лише 11,2% вітчизняних переробних підприємств застосовують цифрові рішення для оптимізації використання матеріалів або підвищення рівня їх повторного використання, а 15,9% – для зниження енергоспоживання.



□ Підприємства, що враховують при виборі комп'ютерного обладнання та технічних засобів електронних комунікацій їх вплив на навколишнє середовище

▨ Підприємства, що використовують системи та рішення ІКТ для зменшення споживання енергії

■ Підприємства, що використовують системи та рішення ІКТ для зменшення кількості матеріалів, що використовуються, або збільшення використання вторинної сировини

Рис. 5. Показники, що характеризують рівень використання ІКТ у контексті «зеленого» розвитку переробних підприємств в Україні

Джерело: сформовано автором на основі [11]

Водночас 59,7% переробних підприємств в Україні враховують екологічні характеристики при виборі технічного обладнання, що свідчить про поступове формування екологічно орієнтованого мислення.

Загалом, в результати проведеного аналізу, можна зазначити, що вітчизняні переробні підприємства перебувають на етапі активного розширення цифрового середовища, що проявляється у зростанні доступу до Інтернету та розвитку інфраструктури.

Цей процес супроводжується посиленням інформаційних ризиків, що не компенсуються належним рівнем розвитку кадрового потенціалу та нормативного забезпечення інформаційної безпеки. Водночас виявлено дисбаланс між технологічним розвитком і системністю підходів до захисту інформації, що створює передумови для зростання вразливості підприємств переробної галузі.

Вважаємо, що ефективне підвищення рівня інформаційної безпеки вітчизняних переробних підприємств у контексті «зеленого» розвитку можливе лише за умови інтеграції економічних стимулів у систему стратегічного управління підприємством, що забезпечує одночасне досягнення економічних, екологічних та безпекових цілей.

З огляду на обмеженість фінансових ресурсів більшості вітчизняних переробних виробництв, особливого значення набуває формування цілеспрямованих напрямів економічного стимулювання, здатних активізувати інвестиції у сферу інформаційної безпеки у контексті «зеленого» розвитку. Думки вчених, що стосуються даного питання, дають змогу узагальнити основні ідеї та визначити релевантні інструменти впливу. Насамперед, важлива увага в дослідженнях приділяється ролі стимулів – економічних, нормативних та інституційних, що визначають готовність підприємств інвестувати у заходи захисту інформації. При цьому наголос робить на економічних стимулах [12].

Деякі дослідження демонструють, що інформаційна безпека поступово інтегрується у фінансову та інвестиційну політику підприємств. Зокрема, доведено, що розкриття інформації про інвестиції у кібербезпеку сприяє зниженню вартості капіталу підприємства та покращує доступ до фінансових ресурсів [13]. Це свідчить про трансформацію інформаційної безпеки з витратної

ISSN: 2786-9431

категорії у фактор підвищення інвестиційної привабливості, що формує додаткові економічні стимули для її розвитку.

Запропоновані напрями та інструменти економічного стимулювання підвищення рівня інформаційної безпеки вітчизняних переробних підприємств наведено в таблиці 1.

Таблиця 1

Напрями та інструменти економічного стимулювання підвищення рівня інформаційної безпеки вітчизняних переробних підприємств

Напрями стимулювання	**Інструменти стимулювання**	**Очікуваний результат**
Залучення інвестицій у цифрову та кіберзахисну інфраструктуру підприємств	Податкові пільги, кредити, прискорена амортизація IT-активів, державні гранти на впровадження кіберзахисту	Підвищення рівня технічної захищеності інформаційно-комунікаційних систем, забезпечення безпечного функціонування «зелених» цифрових технологій
Розвиток людського капіталу у сфері інформаційної безпеки	Фінансування програм підготовки та перепідготовки ІКТ-фахівців, навчання персоналу, державні ваучери на цифрову освіту	Зростання рівня кваліфікації персоналу, зменшення людського фактору як джерела загроз, підвищення ефективності політики інформаційної безпеки
Інституційне забезпечення та страхування кіберризиків	Розвиток ринку кіберстрахування, державні гарантії страхових виплат, впровадження стандартів управління ризиками	Мінімізація фінансових втрат від кіберзагроз, підвищення відповідальності підприємств за дотримання стандартів безпеки, інтеграція інформаційної безпеки у систему «зеленого» розвитку
Розвиток публічно-приватного партнерства у сфері кібербезпеки та «зелених» технологій	Спільні інвестиційні проєкти, державні програми підтримки цифрової трансформації, платформи обміну кіберзагрозами, кластерні ініціативи	Забезпечення координації дій у сфері інформаційної безпеки, доступ до інноваційних технологій захисту, формування стійкої та безпечної цифрової екосистеми підприємств

Джерело: сформовано автором на основі [12–16]

Запропоновані напрями економічного стимулювання відображають комплексний підхід до підвищення рівня інформаційної безпеки, який враховує

як внутрішні можливості вітчизняних переробних підприємств, так і зовнішні інституційні умови їх функціонування. Їх реалізація дозволить забезпечити не лише зниження рівня інформаційних ризиків, але й підвищення загальної ефективності діяльності переробних підприємств у контексті «зеленого» розвитку. Водночас поєднання зазначених інструментів створює передумови для формування стійкої системи управління інформаційною безпекою, інтегрованої у стратегічні пріоритети розвитку переробних підприємств в Україні.

Висновки. Отже, політика інформаційної безпеки повинна розглядатися як базовий інструмент координації заходів захисту та інтеграції їх у загальну стратегію розвитку вітчизняних переробних підприємства. Її значення полягає не лише у встановленні формальних вимог, а й у забезпеченні узгодженості між цілями цифровізації, екологічними пріоритетами та необхідністю мінімізації інформаційних ризиків.

Підвищення рівня інформаційної безпеки вітчизняних переробних підприємств в умовах «зеленого» розвитку економіки є комплексним завданням, що потребує системного підходу. Активне впровадження інформаційно-комунікаційних систем та технологій з метою підвищення екологізація діяльності суб’єктів господарювання формують нові виклики у сфері інформаційної безпеки, що не можуть бути вирішені виключно технічними засобами.

У зв’язку з цим, політику інформаційної безпеки доцільно розглядати як базовий інструмент координації заходів захисту та інтеграції їх у загальну стратегію розвитку вітчизняних переробних підприємства. При цьому, потрібно розуміти, що її значення полягтиме не лише у встановленні формальних вимог, а й у забезпеченні узгодженості між цілями цифровізації, екологічними пріоритетами та необхідністю мінімізації інформаційних ризиків. Крім того,

ISSN: 2786-9431

вище зазначена, обумовлює необхідність формування нових підходів щодо її подальшого удосконалення.

Список використаних джерел:

1. Мащенко М. А., Іполітов Є. М. Формування стратегії посилення інформаційної безпеки підприємства // Економіка та суспільство. 2024. Вип. 70. DOI: https://doi.org/10.32782/2524-0072/2024-70-147.

2. Дячков Д. В. Формування моделі політики інформаційної безпеки на основі концепцій «глибинного захисту» // Підприємництво і торгівля. 2019. № 25. С. 116–121. DOI: https://doi.org/10.36477/2522-1256-2019-25-17.

3. Сороколіт М. Аудит інформаційної безпеки в умовах автоматизації облікових даних вітчизняних підприємств // Herald of Khmelnytskyi National University. Economic sciences. 2025. № 3, т. 2. С. 61–66. DOI: https://orcid.org/0009-0005-2024-0727.

4. Перун Т. С. Організаційно-правові моделі реалізації політики інформаційної безпеки України. *Право і суспільство*. 2020. № 3. С. 166–173. DOI: https://doi.org/10.32842/2078-3736/2020.3.25.

5. Білик Т. Ю., Максимова І. І. Стійкість, безпека, конкурентоспроможність: концептуальні орієнтири розвитку бізнесу в умовах зеленого-цифрового переходу. *Сталий розвиток економіки*. 2025. № 6 (57). С. 644–652. DOI: https://doi.org/10.32782/2308-1988/2025-57-89.

6. Ясінська А. І. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації // Економіка та суспільство. 2023. Вип. 56. DOI: https://doi.org/10.32782/2524-0072/2023-56-118.

7. Бєлозерцев В. Г., Моргуненко В. В. Інформаційна безпека в цифровій економіці: ризики та захисні механізми в бізнес-середовищі // Інвестиції:

практика та досвід. 2025. № 15. С. 235–241. DOI: https://doi.org/10.32702/2306-6814.2025.15.235.

8. Global Cybersecurity Outlook 2023. World Economic Forum. 2023. URL: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf (дата звернення: 22.02.2026).

9. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. 2023. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf (дата звернення: 22.02.2026).

10. Polish-Ukrainian borderland as an area of transformation / за ред. A. Miszczuk, O. Shubalyi. Lublin : Maria Curie-Skłodowska University Press, 2025. 459 p. URL: https://wydawnictwo.umcs.eu/js/elfinder/files/Ebook/Polish-Ukrainian_borderland_ebook_2025.pdf (дата звернення: 22.02.2026).

11. Державна служба статистики України : офіційний веб-сайт. URL: https://stat.gov.ua/ (дата звернення: 22.02.2026).

12. Wessels M., van den Brink P., Verburgh T., Cadet B., van Ruijven T. Understanding incentives for cybersecurity investments: Development and application of a typology. *Digital Business*. 2021. Vol. 1, Issue 2. 100014. DOI: https://doi.org/10.1016/j.digbus.2021.100014.

13. Havakhor T., Rahman M. S., Zhang T. Disclosure of cybersecurity investments and the cost of capital. *Information Systems Research*. 2026. Vol. 0 (0). DOI: https://doi.org/10.1287/isre.2023.0260.

14. Chebbi K. The impact of cyber threats on environmental, social, and governance performance. *Journal of Environmental Management*. 2025. Vol. 389. 126184. DOI: https://doi.org/10.1016/j.jenvman.2025.126184.

15. Dinh T., Chou H.-I., Zhao J. Cybersecurity risk and firm investment efficiency. *Finance Research Letters*. 2025. Vol. 85, part E. 108266. DOI: https://doi.org/10.1016/j.frl.2025.108266.

16. Tan W., Guo B., Zhang Q. Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust. *Pacific-Basin Finance Journal*. 2025. Vol. 90. 102646. DOI: https://doi.org/10.1016/j.pacfin.2024.102646.

ISSN: 2786-9431