

*П. Г. ПЕРЕРВА, Т. О. КОБЕЛЄВА***РОЗВИТОК ПІДПРИЄМНИЦЬКИХ СТРУКТУР В СФЕРІ ВІДНОВЛЮВАЛЬНОЇ ЕНЕРГЕТИКИ: ЗАБЕЗПЕЧЕННЯ ПОТЕНЦІАЛУ КАДРОВОЇ ТА ІНФОРМАЦІЙНОЇ (ЦИФРОВОЇ) БЕЗПЕКИ**

У статті досліджено теоретичні та практичні засади забезпечення економічної безпеки підприємницьких структур у сфері відновлюваної енергетики з акцентом на кадрову та інформаційну (цифрову) складові. Обґрунтовано, що кадрова безпека виступає ключовим чинником інноваційного розвитку, оскільки забезпечує стабільність людського капіталу, утримання висококваліфікованих фахівців та мінімізацію ризиків втрати ключових компетенцій. Інформаційна та цифрова безпека, у свою чергу, гарантує захист даних, технологічної інфраструктури та комунікаційних систем, що є критично важливим для довіри інвесторів, партнерів і споживачів, а також для безперервності виробничих процесів у «зеленій» енергетиці. Узагальнено, що кадрова та цифрова безпека не є тотожними поняттями, хоча й мають спільні цілі та завдання. Кадрова безпека охоплює організаційні, освітні та мотиваційні аспекти, тоді як цифрова безпека зосереджена на технічних і кібернетичних механізмах захисту. Їхня інтеграція формує комплексну основу стійкості підприємницьких структур, забезпечує їхню конкурентоспроможність на глобальному ринку та відповідає вимогам євроінтеграції. Особливу увагу приділено викликам, що постають перед підприємницькими структурами у сфері відновлюваної енергетики: дефіциту висококваліфікованих кадрів, міграції фахівців, недостатній інтеграції освітніх програм із потребами бізнесу, низькому рівню цифрової культури персоналу, а також зростанню кіберзагроз для енергетичної інфраструктури. Визначено перспективні напрями розвитку кадрової та цифрової безпеки, серед яких: формування міждисциплінарних компетенцій, створення системи безперервної освіти та перепідготовки, впровадження міжнародних стандартів (ISO/IEC 27001), розвиток корпоративних політик безпеки та державних програм кіберзахисту.

Ключові слова: підприємницькі структури, відновлювальна енергетика, розвиток, інформаційний потенціал, кадрова безпека, цифрова безпека, кіберзахист, персонал, євроінтеграція, економічна оцінка

*P. G. PERERVA, T. O. KOBELIEVA***DEVELOPMENT OF ENTREPRENEURIAL STRUCTURES IN THE FIELD OF RENEWABLE ENERGY: ENSURING THE POTENTIAL OF HUMAN RESOURCE AND INFORMATION (DIGITAL) SECURITY**

The article explores the theoretical and practical foundations of ensuring the economic security of entrepreneurial structures in the field of renewable energy, with emphasis on human resource and informational (digital) components. It is substantiated that human resource security acts as a key factor of innovative development, as it ensures the stability of human capital, retention of highly qualified specialists, and minimization of risks associated with the loss of core competencies. Information and digital security, in turn, guarantee the protection of data, technological infrastructure, and communication systems, which are critically important for the trust of investors, partners, and consumers, as well as for the continuity of production processes in “green” energy. It is generalized that human resource security and digital security are not identical concepts, although they share common goals and tasks. Human resource security encompasses organizational, educational, and motivational aspects, whereas digital security focuses on technical and cyber mechanisms of protection. Their integration forms a comprehensive basis for the resilience of entrepreneurial structures, ensures their competitiveness in the global market, and meets the requirements of European integration. Particular attention is paid to the challenges faced by entrepreneurial structures in the renewable energy sector: shortage of highly qualified personnel, migration of specialists, insufficient integration of educational programs with business needs, low level of digital culture among staff, and the growing cyber threats to energy infrastructure. Prospective directions for the development of human resource and digital security are identified, including the formation of interdisciplinary competencies, creation of a system of continuous education and retraining, implementation of international standards (ISO/IEC 27001), development of corporate security policies, and state cyber protection programs.

Keywords: entrepreneurial structures, renewable energy, development, informational potential, human resource security, digital security, cyber protection, personnel, European integration, economic assessment

Вступ. Сучасний етап розвитку світової економіки характеризується глибокими трансформаціями, пов'язаними з переходом до моделі сталого розвитку та активним впровадженням відновлюваних джерел енергії. Енергетична безпека, екологічна стабільність та інноваційні технології стають ключовими чинниками конкурентоспроможності держав і підприємницьких структур. У цьому контексті сфера відновлюваної енергетики виступає не лише як стратегічний напрям енергетичної політики, але й як потужний драйвер економічного зростання, формування нових ринків та створення робочих місць [1, 2].

Розвиток підприємницьких структур у сфері відновлюваної енергетики потребує комплексного забезпечення їхнього потенціалу. Важливими складовими цього процесу є кадрова та інформаційна (цифрова) безпека. З одного боку, кадровий потенціал визначає здатність підприємств генерувати інновації, впроваджувати сучасні технології та ефективно управляти виробничими процесами [3, 11]. З іншого

боку, інформаційна та цифрова безпека стає критичною умовою стабільності бізнесу в умовах глобальної цифровізації, кіберризиків та зростаючої залежності від інформаційних систем.

Актуальність дослідження зумовлена кількома чинниками, серед яких, на наш погляд, найбільш важливими слід назвати: зміна клімату, необхідність зниження викидів парникових газів та виконання міжнародних екологічних зобов'язань; перехід від традиційних джерел енергії до відновлюваних, що створює нові можливості для підприємництва; зростання ролі інформаційних технологій у виробничих і управлінських процесах, що потребує захисту даних та цифрових активів; дефіцит висококваліфікованих фахівців у сфері «зеленої» енергетики та необхідність формування нових компетенцій; для України розвиток відновлюваної енергетики є стратегічним напрямом енергетичної незалежності та інтеграції у європейський простір [4].

Таким чином, дослідження розвитку підприємницьких структур у сфері відновлюваної

енергетики крізь призму кадрової та інформаційної (цифрової) безпеки є надзвичайно актуальним. Воно дозволяє поєднати економічні, технологічні та соціальні аспекти, забезпечити стійкість бізнесу та сприяти формуванню конкурентоспроможної моделі енергетичного розвитку.

Мета статті полягає у комплексному дослідженні розвитку підприємницьких структур у сфері відновлюваної енергетики з акцентом на забезпеченні їх кадрового потенціалу та інформаційної (цифрової) безпеки, визначенні ключових викликів і формуванні науково обґрунтованих підходів до підвищення стійкості та конкурентоспроможності цих структур в умовах сучасних трансформацій.

Аналіз основних досягнень і літератури. Проблематика розвитку підприємницьких структур у сфері відновлюваної енергетики та забезпечення їх кадрової й інформаційної (цифрової) безпеки знайшла відображення у працях низки вітчизняних та зарубіжних дослідників. Так, у статті [1] акцентується увага на трансформаційних процесах у підприємницьких структурах України в умовах воєнних викликів. Автори підкреслюють значення стійкості бізнес-екосистем та їх здатності адаптуватися до нових умов, що безпосередньо стосується і підприємств у сфері відновлюваної енергетики. Дослідник Корф Є. [2] розглядає відновлювану енергетику як базову умову енергетичної безпеки держави. Він наголошує, що розвиток розподіленої генерації є не лише екологічним, але й антикризовим інструментом, який забезпечує незалежність та стабільність енергетичної системи. Таким чином, автор підкреслює стратегічну роль підприємницьких структур у формуванні енергетичної незалежності України. У дослідженнях Правдивця О.М. [3] цифрова трансформація розглядається як ключовий чинник економічної безпеки підприємств. Автор доводить, що цифрова безпека є невід'ємною складовою загальної інформаційної безпеки та визначає стійкість бізнесу в умовах кризових явищ, таких як пандемія COVID-19 чи воєнні дії. Зарубіжні автори, зокрема [4], у систематичному огляді літератури аналізують підприємницькі екосистеми та підкреслюють необхідність комплексної підтримки інноваційних структур у сфері відновлюваної енергетики. Вони наголошують на важливості кадрового забезпечення та взаємодії інвесторів і донорів у формуванні стійких бізнес-моделей. Класичні підходи до корпоративного підприємництва, представлені у працях [5, 11, 13], акцентують увагу на контекстуальних факторах, що визначають ефективність підприємницьких структур. У сучасних умовах ці фактори доповнюються кадровою та цифровою безпекою, які стають ключовими умовами інноваційного розвитку та конкурентоспроможності підприємств у сфері відновлюваної енергетики.

Таким чином, аналіз наукових публікацій свідчить про багатовимірність проблеми: одні автори акцентують увагу на стійкості та адаптивності підприємницьких структур, інші — на стратегічній ролі відновлюваної енергетики у забезпеченні енергетичної безпеки, ще інші — на кадрових та

цифрових аспектах як ключових детермінантах розвитку. Це підтверджує актуальність комплексного підходу до дослідження, який поєднує економічні, технологічні та безпекові виміри.

Невирішені задачі. Попри значну кількість наукових праць, присвячених розвитку підприємницьких структур у сфері відновлюваної енергетики, низка важливих питань залишається недостатньо дослідженою. Це зумовлює потребу у подальшому науковому пошуку та практичних розробках. По-перше, кадровий аспект потребує глибшого аналізу. У сучасних умовах спостерігається дефіцит висококваліфікованих фахівців у сфері «зеленої» енергетики, а існуючі освітні програми не завжди відповідають реальним потребам бізнесу. Невирішеним залишається питання формування міждисциплінарних компетенцій, які поєднують знання з енергетики, цифрових технологій та управління. По-друге, інформаційна та цифрова безпека підприємницьких структур досліджена переважно у загальному контексті кіберзахисту, тоді як специфіка відновлюваної енергетики вимагає розробки спеціалізованих стандартів і методик. Недостатньо опрацьованими залишаються питання інтеграції систем цифрової безпеки у виробничі процеси та оцінки їх ефективності. По-третє, інституційно-правове забезпечення розвитку підприємницьких структур у сфері відновлюваної енергетики потребує гармонізації з європейськими нормами. Досі не вироблено комплексного механізму державної підтримки, який би одночасно стимулював інвестиції у кадровий розвиток та цифрову інфраструктуру. По-четверте, економічні та організаційні аспекти залишаються відкритими для дослідження. Недостатньо розроблені фінансові інструменти, які б сприяли залученню інвестицій у кадрову та цифрову безпеку. Потребує уточнення модель інтеграції підприємницьких структур у міжнародні енергетичні та інноваційні екосистеми. Нарешті, науково-методичні прогалини полягають у відсутності універсальних методик оцінки рівня кадрової та інформаційної безпеки підприємств. Необхідним є створення міждисциплінарних моделей, що враховують економічні, технологічні та соціальні чинники розвитку. Отже, невирішені проблеми охоплюють кадровий, цифровий, інституційний, економічний та методологічний виміри. Їх комплексне вирішення має стати предметом подальших досліджень, спрямованих на формування стійких і конкурентоспроможних підприємницьких структур у сфері відновлюваної енергетики.

Методологія дослідження ґрунтується на використанні системного та міждисциплінарного підходів, що поєднують аналіз наукової літератури, порівняльний метод для виявлення тенденцій розвитку підприємницьких структур у сфері відновлюваної енергетики, а також структурно-функціональний аналіз для оцінки кадрової та інформаційної (цифрової) безпеки. Додатково застосовано елементи статистичного узагальнення та контент-аналізу публікацій для визначення невирішених проблем і перспектив подальших досліджень.

Викладення основного метаріалу дослідження.

Розвиток підприємницьких структур у сфері відновлюваної енергетики ґрунтується на поєднанні класичних економічних концепцій, інституційних підходів та сучасних теорій підприємницьких екосистем. У працях Шумпетера Й. [6] та Друкера П. [7] підкреслюється роль інновацій як ключового чинника економічного розвитку. Відновлювана енергетика виступає прикладом «креативного руйнування», коли традиційні джерела енергії поступаються місцем новим технологіям, що формують нові бізнес-моделі та ринки. Інституційна економіка, представлена дослідженнями Норта Д. [3] та Вільямсона О. [4], розглядає підприємницькі структури як елементи інституційного середовища, де вирішальну роль відіграють правила, норми та регуляторні механізми. У сфері відновлюваної енергетики це проявляється у державній політиці підтримки «зелених» інвестицій, міжнародних кліматичних угодах та стандартах енергетичної безпеки. Сучасні концепції підприємницьких екосистем [4, 10] акцентують увагу на необхідності взаємодії бізнесу, наукових установ, інвесторів та державних органів. У сфері відновлюваної енергетики такі екосистеми забезпечують інтеграцію інновацій, фінансування та кадрового потенціалу, створюючи умови для стійкого розвитку підприємницьких структур. Теорія людського капіталу Шульца Т. [11] та Беккера Г. [12]) наголошує на значенні знань і компетенцій як ключового ресурсу підприємництва. У сфері відновлюваної енергетики кадровий потенціал визначає здатність підприємств впроваджувати інновації та управляти складними технологічними процесами. Паралельно, концепція інформаційної та цифрової безпеки [3, 13] підкреслює, що у цифровій

економіці захист даних і технологічної інфраструктури є необхідною умовою стійкості підприємницьких структур. Таким чином, теоретичні основи розвитку підприємницьких структур у сфері відновлюваної енергетики формуються на перетині класичних економічних теорій, інституційного підходу, концепції підприємницьких екосистем, теорії людського капіталу та сучасних підходів до цифрової безпеки. Їх інтеграція дозволяє пояснити специфіку функціонування підприємств у «зеленій» енергетиці та визначити ключові чинники їхньої стійкості й конкурентоспроможності.

У сучасних умовах становлення відновлюваної енергетики кадровий потенціал підприємницьких структур виступає ключовим чинником їхнього інноваційного розвитку. Теорія людського капіталу [11, 12] доводить, що знання, навички та компетенції працівників є основним ресурсом економічного зростання. У сфері «зеленої» енергетики саме кадровий потенціал визначає здатність підприємств впроваджувати новітні технології, управляти складними виробничими процесами та забезпечувати ефективне функціонування цифрових систем. Водночас кадровий дефіцит, недостатня інтеграція освітніх програм із реальними потребами бізнесу та міграція висококваліфікованих фахівців залишаються серйозними викликами, що обмежують інноваційний розвиток галузі.

Аналіз потенціалу кадрової безпеки підприємницьких структур у сфері відновлюваної енергетики дозволяє систематизувати його значення, окреслити ключові виклики та визначити перспективи розвитку. Узагальнення цих аспектів нами представлено у табл.1.

Таблиця 1 - Узагальнення потенціалу кадрової безпеки підприємницьких структур у сфері відновлюваної енергетики

Показник	Характеристика
Значення кадрової безпеки	Для підприємницьких структур у сфері відновлюваної енергетики кадрова безпека означає стабільність та захищеність кадрового складу, здатність утримувати кваліфікованих працівників, мінімізувати ризики втрати ключових компетенцій та забезпечувати безперервність інноваційних процесів.
Виклики та проблеми	Дефіцит висококваліфікованих кадрів у відновлюваній енергетиці; міграція та відтік фахівців; недостатня інтеграція освітніх програм із реальними потребами підприємств; низький рівень цифрової компетентності персоналу.
Перспективи розвитку	Розробка системи кадрової безпеки, що включає моніторинг ризиків, формування міждисциплінарних компетенцій, програми утримання та мотивації персоналу; інтеграція у міжнародні освітні та наукові проекти.
Роль у стійкості підприємницьких структур	Потенціал кадрової безпеки забезпечує довгострокову стабільність підприємницьких структур у сфері відновлюваної енергетики, підтримує інноваційність та конкурентоспроможність бізнесу на глобальному ринку «зеленої» енергетики.

Джерело: авторська розробка

Як слідує з даних, представлених в табл.1, потенціал кадрової безпеки у сфері відновлюваної енергетики є визначальним чинником стійкості підприємницьких структур. Він поєднує захищеність кадрового складу з можливістю реалізації інноваційних стратегій, що забезпечує конкурентні переваги та адаптацію до глобальних викликів.

У сфері відновлюваної енергетики інформаційна та цифрова безпека підприємницьких структур є критично важливим чинником їхньої стійкості та конкурентоспроможності. Вона визначає здатність

підприємств захищати дані, технологічну інфраструктуру та комунікаційні системи, що забезпечує довіру інвесторів і партнерів. У науковій та прикладній літературі поняття «інформаційна безпека» та «цифрова безпека» часто ототожнюють, що призводить до методологічних помилок у побудові систем захисту та управлінні ризиками. Насправді це два пов'язані, але різні за обсягом і змістом поняття: інформаційна безпека має ширший, системний характер, тоді як цифрова безпека є її технологічно-інфраструктурною підсистемою,

зосередженою на цифрових активах, IT-середовищі та кіберзагрозах. В результаті проведеного дослідження нами сформовано академічно вивірені визначення, спільні та відмінні риси, а також розширений коментар щодо їхнього місця в управлінні підприємством – з акцентом на специфіку відновлюваної енергетики.

В табл.2 систематизовано усі визначення, спільні та відмінні риси, пропозиції та узагальнення, які охоплюють інформаційну та цифрову безпеку підприємства (з акцентом на підприємницькі структури у сфері відновлюваної енергетики).

Таблиця 2 – Економічні характеристики інформаційної та цифрової безпеки підприємницьких структур у сфері відновлюваної енергетики

Критерій	Інформаційна безпека	Цифрова безпека	Спільні риси	Відмінні риси	Коментар
Визначення	Стан захищеності всієї інформації (конфідентційність, цілісність, доступність) від несанкціонованого доступу, змін чи знищення	Система захисту цифрових активів підприємства (даних, інфраструктури, технологій) від кіберзагроз у цифровому середовищі	Обидві спрямовані на захист даних та процесів, забезпечення стабільності бізнесу.	Інформаційна безпека ширша, охоплює всі форми інформації; цифрова — лише IT-середовище.	У відновлюваній енергетиці інформаційна безпека включає захист знань і технологій, цифрова — захист SCADA/ICS, телеметрії та хмарних сервісів.
Цілі	Захист інформації від витоку, спотворення, втрати; підтримка правових і організаційних норм.	Захист цифрових систем від кібератак, збоїв, експлоїтів; забезпечення безперервності цифрових сервісів.	Конфідентційність, цілісність, доступність (CIA-тріада).	Інформаційна безпека додає правові, кадрові та фізичні аспекти; цифрова – технічні та кібернетичні.	Для підприємств «зеленої» енергетики цілі інтегруються: захист інноваційних даних + стійкість цифрової генерації.
Загрози	Кадрові, правові, організаційні, фізичні, репутаційні (соціальна інженерія, витік через паперові носії, недобросовісні контрагенти).	Кіберзагрози та технічні збої (малвар, фішинг, DDoS, уразливості ПЗ, відмови обладнання).	Обидві враховують ризики втрати даних та порушення бізнес-процесів.	Інформаційна безпека ширше охоплює людський та правовий фактор; цифрова – технологічний	У відновлюваній енергетиці загрози комбіновані: від витоку інноваційних розробок до атак на енергетичну інфраструктуру.
Інстру-менти та заходи	Організаційні та правові політики, класифікація інформації, контроль доступу, фізична охорона, навчання персоналу.	Технічні засоби: шифрування, багатфакторна автентифікація, сегментація мереж, SIEM/EDR, резервування, тестування.	Обидві потребують політик, контролю доступу, навчання персоналу.	Інформаційна безпека — акцент на організаційних і правових заходах; цифрова — на технічних.	Для «зеленої» енергетики потрібна інтеграція: політики + кіберзахист промислових систем (ICS/SCADA).
Метрики та моніторинг	Інциденти витоку, відповідність політикам, зрілість процесів, дисципліна доступу.	Кіберінциденти, час виявлення/реагування (MTTD/MTTR), SLA/uptime, покриття патчами.	Обидві системи вимірюють ефективність захисту та реагування.	Інформаційна безпека – якісні показники; цифрова – кількісні технічні метрики	У відновлюваній енергетиці важливо поєднувати: якість управління інформацією + технічну стійкість цифрових систем.
Практичні орієнтири	Класифікація інформації, політики доступу, навчання, перевірка контрагентів, фізичний режим.	Архітектура кіберзахисту, управління уразливостями, DevSecOps, резервування, OT-моніторинг.	Обидві потребують інтеграції у систему менеджменту ризиків.	Інформаційна безпека – стратегічна «парасолька»; цифрова – технічний домен.	У сфері відновлюваної енергетики необхідна двохшарова модель: інформаційна безпека як стратегія, цифрова — як технічна реалізація.
Роль у стійкості підприємницьких структур	Забезпечує захист знань, інновацій, правових та кадрових процесів.	Забезпечує стійкість цифрових систем, безперервність генерації та захист інфраструктури.	Обидві формують основу конкурентоспроможності та довіри.	Інформаційна безпека — стратегічна; цифрова — операційна.	У відновлюваній енергетиці їхня синергія критична: без захисту кадрів і знань неможливий розвиток, без цифрової безпеки – неможлива стабільна генерація.

Джерело: авторська розробка

З даних табл.2 можна зробити висновок про те, що інформаційна та цифрова безпека підприємницьких структур у сфері відновлюваної енергетики є взаємопов'язаними, але не тотожними поняттями. Перша охоплює всі форми інформації та організаційно-правові аспекти, включає як цифрові, так і аналогові носії інформації; друга зосереджена на цифрових активах та кіберзахисті, тобто стосується лише цифрового середовища. Їхня інтеграція створює

комплексну основу стійкості підприємств: від захисту інноваційних знань і кадрових процесів до безперервності роботи промислових систем та цифрових сервісів.

Узагальнені аспекти потенціалу інформаційної (цифрової) безпеки підприємницьких структур у сфері відновлюваної енергетики наведено у табл.3.

Таблиця 3 - Узагальнення потенціалу інформаційної (цифрової) безпеки підприємницьких структур у сфері відновлюваної енергетики

Показник	Характеристика
Значення інформаційної безпеки	Для підприємницьких структур у сфері відновлюваної енергетики цифрова безпека означає захист виробничих процесів, даних та інноваційних технологій від кібератак і технічних збоїв. Вона формує основу стабільності бізнес-моделей та гарантує безперервність «зеленої» генерації.
Виклики та проблеми	Зростання кількості кібератак на енергетичну інфраструктуру; витік конфіденційних даних через низький рівень цифрової культури персоналу; відсутність адаптованих стандартів безпеки для підприємств відновлюваної енергетики; недосконалість нормативно-правового регулювання у сфері кіберзахисту.
Перспективи розвитку	Впровадження міжнародних стандартів цифрової безпеки (ISO/IEC 27001); розробка корпоративних політик захисту даних; навчання персоналу цифровій грамотності; створення державних та галузевих програм підтримки кіберзахисту підприємств у сфері відновлюваної енергетики.
Роль у стійкості підприємницьких структур	Потенціал цифрової безпеки забезпечує довгострокову стійкість підприємницьких структур у сфері відновлюваної енергетики, мінімізує ризики втрати даних та технологій, підтримує ефективність управління і формує конкурентні переваги на глобальному ринку «зеленої» енергетики.

Джерело: авторська розробка

Таким чином, потенціал інформаційної та цифрової безпеки у сфері відновлюваної енергетики є визначальним чинником стійкості підприємницьких структур. Він забезпечує захист інноваційних процесів, підтримує довіру інвесторів і партнерів та створює умови для інтеграції підприємств у міжнародні енергетичні та інноваційні екосистеми.

У сучасних умовах розвитку відновлюваної енергетики підприємницькі структури стикаються з подвійним викликом: необхідністю забезпечення економічної безпеки та інтеграції у європейський простір. Економічна безпека в цьому контексті не зводиться лише до фінансових показників чи ринкової стійкості — вона включає кадрову та інформаційну (цифрову) складові, які визначають здатність підприємств адаптуватися до глобальних викликів, впроваджувати інновації та відповідати стандартам ЄС.

Кадрова безпека у сфері «зеленої» енергетики означає стабільність і захищеність кадрового складу, здатність утримувати висококваліфікованих працівників та мінімізувати ризики втрати ключових компетенцій. Інформаційна та цифрова безпека забезпечує захист даних, технологічної інфраструктури та комунікаційних систем, що є критично важливим для довіри інвесторів і партнерів. Умови євроінтеграції посилюють значення цих складових: підприємницькі структури мають відповідати міжнародним стандартам, інтегруватися у глобальні ланцюги постачання та гарантувати стійкість своїх бізнес-моделей.

Нами сформовано узагальнюючу табл.4, яка систематизує значення, виклики, перспективи та роль кадрової та цифрової безпеки у формуванні стійкості підприємницьких структур відновлюваної енергетики.

Таблиця 4 – Потенціал кадрової та інформаційної (цифрової) безпеки підприємницьких структур у сфері відновлюваної енергетики

Показник	Кадрова безпека	Інформаційна (цифрова) безпека	Взаємозв'язок
Значення	Забезпечує наявність кваліфікованих кадрів, здатних впроваджувати інновації та управляти складними технологічними процесами у сфері «зеленої» енергетики.	Гарантує захист даних, цифрових систем, формує довіру інвесторів і партнерів, забезпечує безперервність роботи енергетичних об'єктів.	Компетентність персоналу визначає ефективність цифрового захисту; інформаційна безпека охороняє знання та інновації, що генеруються кадрами.
Виклики та проблеми	Дефіцит фахівців у сфері відновлюваної енергетики; міграція кадрів; недостатня інтеграція освітніх програм із потребами «зеленого» бізнесу; ризики втрати ключових компетенцій.	Кібератаки на енергетичну інфраструктуру; витік даних; низький рівень цифрової культури персоналу; відсутність адаптованих норм кіберзахисту для галузі	Недостатня цифрова грамотність працівників підвищує ризики; слабка інтеграція кадрових та інформаційних стратегій у бізнес-моделі.
Перспективи розвитку	Формування міждисциплінарних компетенцій; створення системи безперервної освіти та перепідготовки; підтримка молодих фахівців; інтеграція у міжнародні освітні та наукові проекти.	Впровадження міжнародних стандартів (ISO/IEC 27001); розвиток корпоративних політик безпеки; навчання цифровій грамотності; програми кіберзахисту.	Синергія кадрової та цифрової безпеки як основа стійкості підприємницьких структур; формування комплексних стратегій розвитку у відповідності до стандартів ЄС.
Роль у стійкості підприємницьких структур	Забезпечує інноваційність, адаптивність та довгострокову стабільність бізнесу у сфері відновлюваної енергетики.	Мінімізує ризики, підвищує ефективність управління та гарантує безперервність «зеленої» генерації.	Формує комплексну основу конкурентоспроможності та стійкості підприємницьких структур на глобальному ринку в умовах євроінтеграції.

Джерело: авторська розробка

Таким чином, кадрова та інформаційна (цифрова) безпека виступають взаємопов'язаними складовими економічної безпеки підприємницьких структур у сфері відновлюваної енергетики. Кадрова безпека забезпечує стабільність і розвиток людського капіталу, тоді як цифрова безпека гарантує захист технологічної інфраструктури та даних. Їхня синергія створює

комплексну основу стійкості бізнес-моделей, що особливо важливо в умовах євроінтеграції, коли підприємства мають відповідати міжнародним стандартам, інтегруватися у глобальні ринки та забезпечувати довіру інвесторів.

Висновки та напрямки подальших досліджень. Проведене дослідження засвідчує, що кадрова та

інформаційна (цифрова) безпека є взаємопов'язаними складовими економічної безпеки підприємницьких структур у сфері відновлюваної енергетики. Кадрова безпека забезпечує стабільність і розвиток людського капіталу, утримання висококваліфікованих фахівців та мінімізацію ризиків втрати ключових компетенцій. Інформаційна та цифрова безпека, у свою чергу, гарантує захист даних, технологічної інфраструктури та комунікаційних систем, що є критично важливим для довіри інвесторів, партнерів та споживачів. Узагальнено можна стверджувати, що синергія кадрової та цифрової безпеки формує комплексну основу стійкості підприємницьких структур, забезпечує їхню конкурентоспроможність на глобальному ринку та відповідає вимогам євроінтеграції. Саме інтеграція цих двох вимірів дозволяє підприємствам відновлюваної енергетики ефективно адаптуватися до глобальних викликів, впроваджувати інновації та гарантувати безперервність «зеленої» генерації. Синергія кадрової та цифрової безпеки формує комплексну основу стійкості підприємницьких структур, забезпечує їхню конкурентоспроможність на глобальному ринку та відповідає вимогам євроінтеграції. Умови інтеграції до європейського економічного простору посилюють значення цих складових, адже підприємства мають відповідати міжнародним стандартам, інтегруватися у глобальні ланцюги постачання та гарантувати високий рівень захищеності як кадрових, так і інформаційних ресурсів.

Подальші дослідження мають бути спрямовані на поглиблення теоретичних засад та практичних інструментів забезпечення кадрової та цифрової безпеки, що дозволить підприємницьким структурам у сфері відновлюваної енергетики не лише зберігати стійкість, але й активно розвиватися в умовах глобальної конкуренції та європейської інтеграції.

Список літератури

1. Верба В. А., Кизенко В. І., Гребешкова О. М. Трансформація підприємницьких структур України в умовах воєнних викликів // *Економіка та держава*. 2023. № 7. С. 12–18. URL: <https://economy.in.ua>
2. Корф Є. Відновлювана енергетика як базова умова енергетичної безпеки України // *Енергетична політика України*. 2025. № 2. С. 5–11. URL: <https://ua-energy.org>
3. Правдивець О. М. Цифрова трансформація як основа економічної стабільності та безпеки підприємницької діяльності // *Економіка та суспільство*. 2022. № 34. С. 45–52. URL: <https://economyandsociety.in.ua>
4. Wadichar R., Manusmare S., Burghate V. Entrepreneurial ecosystems: A systematic literature review // *Journal of Entrepreneurship and Innovation*. 2024. Vol. 12, No. 3. P. 101–118. DOI: 10.1016/j.jei.2024.03.005
5. Zahra S. A., Covin J. G. Contextual influences on the corporate entrepreneurship-performance relationship: A longitudinal analysis // *Journal of Business Venturing*. 1995. Vol. 10, No. 1. P. 43–58. DOI: 10.1016/0883-9026(94)00004-E
6. Шумпетер Й. Теорія економічного розвитку. К.: *Основи*, 1995. 512 с.
7. Друкер П. Практика менеджменту. К.: *Видавництво «Укр. енциклопедія»*, 2001. 400 с.
8. Норт Д. Інституції, інституційні зміни та функціонування економіки. К.: *Основи*, 2000. 320 с.
9. Вільямсон О. Економічні інститути капіталізму. К.: *Основи*, 2001. 450 с.
10. Isenberg D. The entrepreneurship ecosystem strategy as a new paradigm for economic policy: Principles for cultivating entrepreneurship. – *Babson Entrepreneurship Ecosystem Project*, Babson College, 2011. 13 p. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1089034
11. Шульц Т. Інвестиції в людський капітал. К.: *Основи*, 1993. 280 с.
12. Беккер Г. Людський капітал: теоретичний та емпіричний аналіз. К.: *Основи*, 2002. 380 с.
13. Castells M. The Rise of the Network Society. Oxford: *Blackwell Publishers*, 2000. 556 p.

References (transliterated)

1. Verba V. A., Kyzenko V. I., Hrebeshkova O. M. Transformatsiia pidpriemnytskykh struktur Ukrainy v umovakh voiennykh vyklykiv [Transformation of entrepreneurial structures of Ukraine under war challenges]. *Ekonomika ta derzhava*. 2023. No. 7. P. 12–18. Available at: <https://economy.in.ua>
2. Korf Ye. Vidnovliuvana enerhetyka yak bazova umova enerhetychnoi bezpeky Ukrainy [Renewable energy as a basic condition of Ukraine's energy security]. *Enerhetychna polityka Ukrainy*. 2025. No. 2. P. 5–11. Available at: <https://ua-energy.org>
3. Pravdyvets O. M. Tsyfrova transformatsiia yak osnova ekonomichnoi stabilnosti ta bezpeky pidpriemnytskoi diialnosti [Digital transformation as a basis of economic stability and security of entrepreneurial activity]. *Ekonomika ta suspilstvo*. 2022. No. 34. P. 45–52. Available at: <https://economyandsociety.in.ua>
4. Wadichar R., Manusmare S., Burghate V. Entrepreneurial ecosystems: A systematic literature review. *Journal of Entrepreneurship and Innovation*. 2024. Vol. 12, No. 3. P. 101–118. DOI: 10.1016/j.jei.2024.03.005
5. Zahra S. A., Covin J. G. Contextual influences on the corporate entrepreneurship-performance relationship: A longitudinal analysis. *Journal of Business Venturing*. 1995. Vol. 10, No. 1. P. 43–58. DOI: 10.1016/0883-9026(94)00004-E
6. Shumpeter Y. Teoriia ekonomichnoho rozvytku [The Theory of Economic Development]. Kyiv: *Osnovy*, 1995. 512 p.
7. Druker P. Praktyka menedzhmentu [Management Practice]. Kyiv: *Ukr. Encyclopedia Publishing*, 2001. 400 p.
8. Nort D. Instytutsi, instytutsiini zminy ta funktsionuvannia ekonomiky [Institutions, Institutional Change and Economic Performance]. Kyiv: *Osnovy*, 2000. 320 p.
9. Viliamson O. Ekonomichni instytuty kapitalizmu [Economic Institutions of Capitalism]. Kyiv: *Osnovy*, 2001. 450 p.
10. Isenberg D. The entrepreneurship ecosystem strategy as a new paradigm for economic policy: Principles for cultivating entrepreneurship. Babson Entrepreneurship Ecosystem Project, Babson College, 2011. 13 p. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1089034
11. Shults T. Investytsii v liudskyi kapital [Investment in Human Capital]. Kyiv: *Osnovy*, 1993. 280 p.
12. Bekker H. Liudskyi kapital: teoretychnyi ta empirichniy analiz [Human Capital: Theoretical and Empirical Analysis]. Kyiv: *Osnovy*, 2002. 380 p.
13. Castells M. The Rise of the Network Society. Oxford: *Blackwell Publishers*, 2000. 556 p.

Надійшла (received) 10.12.2025

Відомості про авторів / About the Authors

Перерва Петро Григорович (Pererva Petro) – д.е.н., професор, професор кафедри економіки бізнесу і міжнародних економічних відносин Національного технічного «Харківський політехнічний інститут», вул. Кирпичова, 2, м. Харків, 61002, Україна; ORCID: <https://orcid.org/0000-0002-6256-9329>; e-mail: pgpererva@gmail.com

Кобелева Тетяна Олександрівна (Kobielieva Tetiana) – д.е.н., професорка, Національний технічний університет «Харківський політехнічний інститут», професорка кафедри економіки бізнесу і міжнародних економічних відносин; м. Харків, Україна; ORCID: <https://orcid.org/0000-0001-6618-0380>; e-mail: tanja.kobeleva@gmail.com