ISSN (print) 2708-7530
Наукові перспективи № 2(32) 2023

УДК 330.658.1

https://doi.org/10.52058/2708-7530-2023-2(32)-234-246

Боднар Олена Андріївна кандидат економічних наук, доцент кафедри фінансів, банківської справи та страхування, Миколаївський національний аграрний університет, вул. Георгія Гонгадзе, 9, м. Миколаїв, 54008, тел.: (067)799-70-70, https://orcid.org/0000-0002-0152-4290

МОДЕРНІЗАЦІЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВІЗАЦІЇ

Анотація. В сучасних реаліях розвитку економіки все вагомішим є питання її цифровізації. В даному контексті стає пріоритетним питання забезпечення економічної безпеки держави у цілому та фінансово-економічної безпеки підприємства зокрема з урахуванням цифрових трансформацій, що в свою чергу виділяє фінансово-економічну безпеку підприємства в таких умовах в самостійний елемент. Актуальність дослідження зумовлена необхідністю вирішення питання модернізації фінансово-економічної безпеки підприємства з урахуванням нових ризиків і можливостей цифровізації.

Метою наукової роботи є виявлення особливостей запобігання внутрішнім та зовнішнім негативним впливам (загрозам) з метою забезпечення ефективного та стабільного функціонування та динамічного соціального розвитку підприємства в умовах цифровізації.

Результати. Запропоновано ввести поняття «цифрова безпека підприємства» на заміну поняттю «інформаційна складова економічної безпеки» з метою приведення термінології у відповідність до нових економічних реалій.

Впровадження моделі «чорної скриньки» дозволило ідентифікувати новітні ризики та загрози економічній безпеці підприємства в умовах цифровізації, що відрізняється від існуючих. Оцінка цифрової безпеки підприємств країн-членів Європейського Союзу показала, що рівень цифрової безпеки не залежить від розміру країни, але на нього впливає інституційне середовище (зокрема, інструменти цифрового розвитку в ЄС) і розмір підприємств. Також в рамках дослідження запропоновано оцінку рівня цифрової безпеки підприємств в умовах цифровізації. Для характеристики підприємств за рівнем цифрової безпеки запропоновано методику розрахунку за методом коефіцієнтів.

Визначено необхідність модернізації системи фінансово-економічної безпеки підприємства в умовах розвитку цифрової економіки та умов

цифровізації як необхідного елемента внутрішньогосподарського механізму підприємства для захисту діяльності від зовнішніх, так і внутрішніх негативних чинників та впровадження інноваційних інформаційних технологій і програмного забезпечення для її стабільного та динамічного розвитку.

Ключові слова: економічна безпека, фінансово-економічна безпека підприємства, цифрова економіка, цифрова безпека підприємства, загрози, ризики, інституційне середовище, цифровізація, ЄС.

Bodnar Olena Andriivna Candidate of Economic Sciences, Assistant professor of the Department of Finance, Banking and Insurance, Mykolayiv National Agrarian University, Georgiya Gongadze St., 9, Mykolaiv, 54008, tel.: (067) 799-70-70, https://orcid.org/0000-0002-0152-4290

MODERNIZATION OF THE FINANCIAL AND ECONOMIC SECURITY OF THE ENTERPRISE WITHIN THE CONDITIONS OF DIGITALIZATION

Abstract. In today's realities of economic development, the issue of its digitalization is increasingly important. In this context, the issue of ensuring the economic security of the state as a whole and the financial and economic security of the enterprise in particular, taking into account digital transformations, which in turn separates the financial and economic security of the enterprise in such conditions into an independent element, becomes a priority. The relevance of the study is determined by the need to solve the issue of modernization of the financial and economic security of the enterprise, taking into account new risks and possibilities of digitalization.

The purpose of the scientific work is to identify the features of prevention of internal and external negative influences (threats) in order to ensure effective and stable functioning and dynamic social development of the enterprise in the conditions of digitalization.

The results. It is proposed to introduce the concept of "enterprise digital security" to replace the concept of "informational component of economic security" in order to bring the terminology into line with new economic realities.

The implementation of the "black box" model made it possible to identify the latest risks and threats to the economic security of the enterprise in the conditions of digitization, which is different from the existing ones. The assessment of the digital security of enterprises of the member states of the European Union showed that the level of digital security does not depend on the size of the country, but it is influenced by the institutional environment (in particular, digital development tools in the EU)

and the size of the enterprises. Also, as part of the study, an assessment of the level of digital security of enterprises in the conditions of digitalization is proposed. To characterize enterprises according to the level of digital security, a method of calculation based on the method of coefficients is proposed.

The need to develop and implement a system of financial and economic security of the enterprise in the conditions of the development of the digital economy and the conditions of digitalization as a necessary element of the internal economic mechanism of the enterprise for the protection of activities from external and internal negative factors and the introduction of innovative information technologies and software for its stable, dynamic development

Keywords: economic security, financial and economic security of the enterprise, digital economy, digital security of the enterprise, threats, risks, institutional environment, digitalization, EU.

Постановка проблеми. Постійні зміни зовнішнього та внутрішнього середовища, поява нових чинників, які формують основи фінансово-економічної безпеки, необхідність удосконалених методичних підходів до оцінки рівня фінансово-економічної безпеки в умовах цифровізації, застосування нових методів та алгоритмів забезпечення фінансово-економічної безпеки підприємств потребують подальшого дослідження та привертають увагу як науковців так і практиків.

Накопичений досвід дає можливість стверджувати, що фінансово-економічна безпека є ключовою характеристикою стабільного функціонування та досягнення необхідних показників розвитку як окремих суб'єктів господарювання, так і суспільства в цілому. Безпека економічних процесів характеризується численними політичними, правовими та економічними механізмами та інструментами захисту економічних інтересів. У широкому розумінні фінансово-економічну безпеку можна розглядати як здатність інституційно-організаційної системи захищати інтереси суб'єктів господарювання на основі міжнародних і національних правових норм щодо дотримання національних традицій і цінностей господарювання.

Інноваційні інформаційно-комп'ютерні технології, що становлять основу цифрової економіки, відіграють значну роль у розвитку всіх сторін суспільства.

Незважаючи на пильну увагу до проблем цифровізації з боку численних досліджень, питання впливу цифрових технологій на фінансово-економічну безпеку підприємств вивчені та розроблені недостатньо.

Аналіз останніх досліджень і публікацій. Поняття безпеки розглядається вченими та науковцями на всіх рівнях: міжнародному, державному, регіональному, на рівні підприємства і навіть особистості.

Найдосліджуванішою складовою національної безпеки є економічна або фінансово-економічна, якщо безпека розглядається на рівні підприємства.

Аналіз понятійного апарату фінансово-економічної безпеки підприємства показав, що це поняття розглядається з декількох точок зору, а саме:

1. Захист від загроз (захист науково-технічного, виробничого та кадрового потенціалу підприємства) від активних або пасивних економічних загроз [1].
2. Стан ефективного використання ресурсів [2].
3. Здатність до стабільного функціонування та аналітико-управлінський рівень [3].
4. Наявність конкурентної переваги [4].
5. Досягнення цільових показників як критерій економічної безпеки [5; 6].

Враховуючи науковий досвід досліджень у сфері фінансово-економічної безпеки, слід зазначити, що фінансово-економічна безпека підприємства є поняттям складним і комплексним і її визначають: сукупність робіт, які забезпечують платоспроможність підприємства та ліквідність його оборотних активів; організація контролю усіх видів діяльності підприємства з метою підвищення його ефективності; кваліфікація, компетентність та активність менеджерів; ефективність використання усіх видів ресурсів; процес попередження можливих збитків через внутрішні та зовнішні загрози тощо.

Крім того, треба відмітити, що фінансово-економічна безпека підприємства, зокрема формування системи його забезпечення, цілком залежить від змін у зовнішньому та внутрішньому середовищах. Нині – це розвиток цифрової економіки, пандемія COVID-19 та бойові дії на території України.

Дослідження у сфері фінансово-економічної безпеки підприємства в умовах цифрових трансформацій переважно охоплюють наступні теми: вплив інформаційно-комунікаційних технологій (далі – ІКТ) на ведення бізнесу підприємств, підвищення їх ефективності та конкурентоспроможності [2], вплив ІКТ на економічне зростання та [7], на економіку та суспільство в цілому [8; 9].

Отже, питання модернізації фінансово-економічної безпеки підприємства в умовах цифровізації залишається актуальним та потребує подальшого дослідження.

Мета статті – виявлення особливостей запобігання внутрішнім та зовнішнім негативним впливам (загрозам) з метою забезпечення ефективного та стабільного функціонування, динамічного соціального розвитку підприємства в умовах цифровізації.

Виклад основного матеріалу. Забезпечення фінансово-економічної безпеки підприємства – це важливі для здійснення безперервного процесу відтворення. Фінансово-економічна безпека підприємства включає три

важливі елементи, а саме: економічну та фінансову незалежність, стійкість і розвиток. Економічна незалежність передбачає здійснення контролю над власними ресурсами; фінансова незалежність реалізується через здатність вчасно оплачувати свої зобов'язання. Необхідно отримати такий рівень виробництва, щоб забезпечити конкурентоспроможність підприємства на ринку. Під стійкістю розуміють стабільність функціонування, фінансовий стан, при якому забезпечується виконання всіх своїх зобов'язань перед працівниками, іншими організаціями, державою.

Розвиток передбачає підвищення ефективності діяльності підприємства та доведення його до задовільного стану. Якщо підприємство не розвивається і не досягає ефективності, в майбутньому це знижує його здатність пристосовуватися до зовнішніх і внутрішніх умов, а отже, знижується здатність до виживання. Отже, підприємства перебувають у стані постійного вдосконалення з метою досягнення та підтримки рівня фінансово-економічної безпеки.

На думку авторів [7-10], процес цифрової трансформації полягає у зміщенні акценту з матеріальних активів на нематеріальні (цифрові, віртуальні), автоматизації бізнес-процесів шляхом впровадження сучасних інформаційних (цифрових) технологій і систем, створенні на їх основі нових бізнес-моделей. Весь комплекс інформації, об’єктів інформатизації, інформаційних (цифрових) технологій і систем, впровадження ІКТ, перехід підприємства до функціонування в цифровому середовищі несуть нові ризики та загрози, не властиві традиційним (нецифровим) процесам (табл. 1). Забезпечення фінансово-економічної безпеки, по суті, зводиться до поєднання цих загроз. Тому організація діяльності із забезпечення фінансово-економічної безпеки підприємств значною мірою залежить від методу їх ідентифікації та класифікації.

Таблиця 1

Види ризиків та загроз в контексті цифровізації підприємств за моделлю «чорної скриньки»

Класифікація ризиків	Види ризиків
Ризики на вході	1) ризики та загрози правового характеру 2) зовнішні інформаційні ризики, зумовлені політичними та соціально-економічними ситуаціями в країні 3) ризики, пов’язані з використанням технологій цифрової економіки (технологічний ризик): Інтернет речей, ризики технології блокчейн, ризики використання штучного інтелекту та технологій робототехніки та автоматизації на його основі, ризики та загрози використання імпортних апаратних компонентів та запозичення нових цифрових технологій; ризики та загрози до використання хмарних та розподілених обчислень: ризики та загрози, пов’язані зі стабільністю Інтернету;

	4) високотехнологічні фізичні загрози; 5) ризики низьких цифрових компетенцій потенційних працівників
Ризики у внутрішньому середовищі	1) організаційно-управлінські ризики; 2) внутрішні інформаційні ризики, які безпосередньо пов'язані з діяльністю підприємства та його персоналу і залежать від таких факторів , як виробничі та кадрові ресурси, рівень техніко-технологічної оснащеності та розвитку інформаційної інфраструктури, організація цифрової безпеки; 3) ризики цифрової безпеки: втрата інформаційних ресурсів, втрата доступу до інформаційних ресурсів, порушення їх цілісності, доступності внаслідок свідомого впливу; викрадення інформації та даних у цифровому форматі; навмисне спотворення інформації, збої технічного та програмного забезпечення автоматизованих систем управління та інформаційних систем, а також несправності програмного забезпечення та засобів захисту в наслідок навмисного впливу; поширення шкідливого програмного забезпечення та закладок; шпигунське програмне забезпечення; несанкціонований доступ; порушення авторських прав; 4) використання третіх осіб для управління процесами
Ризики на виході	1) ризики, пов'язані з інтеграцією цифрових технологій між основними зацікавленими сторонами (постачальниками, перевізниками, споживачами); 2) зниження рівня фінансово-економічної безпеки підприємства у цілому та цифрової безпеки зокрема; 3) вразливість до шкідливих впливів; 4) радикальна зміна бізнес-моделей та «злиття» економічних, правових та інформаційних загроз, набуваючи складної цифрової технологічної ознаки

Джерело: побудовано з використанням [4]

В економічній науці поняття фінансово-економічна безпека підприємства розглядається як сукупність складових, серед яких інформаційна виділяється як захист інформації; який в сучасних умовах набув форми цифровізації.

Тому, враховуючи сучасні умови цифрової трансформації, доцільно запровадити цифрову безпеку підприємства як стан цифровізації в економічній науці, що забезпечує економічні та інформаційні інтереси підприємства в поточному періоді та його стратегічну фінансово-економічну безпеку в довгостроковій перспективі з використанням відповідних технологій.

Отже, забезпечення фінансово-економічної безпеки в умовах цифровізації має базуватися на цифровій безпеці – тобто формуванні якісно

нових факторів участі підприємств в єдиній інформаційній системі для забезпечення фінансово-економічної безпеки підприємств та зниження зовнішніх і внутрішніх ризиків.

Цифрова трансформація відрізняється від автоматизації та інформатизації тим, що вимагає системних змін у бізнес-процесах, бізнес-моделях та економічних відносинах як у середині підприємства, так і навколо нього. Створення середовища для цифрової трансформації підприємств, що працюють у традиційних секторах економіки, має включати низку спеціалізованих технологічних та бізнес-консультацій, які можуть проводитися відповідними центрами компетенції. Існує також попит на державно-приватну співпрацю щодо загальнонаціональних ініціатив (тобто, розвиток навичок і спільних стандартів) і комплексну фінансову структуру для підтримки підприємств. Зокрема, ЄС запровадив такі інструменти для підвищення цифрової безпеки підприємств [4]:

– Галузева ініціатива ЄС «Цифровізація європейської промисловості» (Digitalization of European Industry - DEI) в рамках пакету «Єдиного цифрового ринку» з 2016 року та його впровадження на наднаціональному та національному рівнях.

– Фінансування цифрової трансформації для малих та середніх підприємств (SMEs). На рівні ЄС COSME (2014 – 2020). Програма ЄС з підвищення конкурентоспроможності малого та середнього бізнесу забезпечує Механізм гарантування кредитів COSME (LGF), який підтримує фінансування проєктів цифрової трансформації малого та середнього бізнесу в усіх секторах економіки.

– Наявність центрального органу з розробки політики цифрової трансформації підприємств у країнах-членах ЄС;

– Створення Фонду відновлення та стійкості (Recovery and Resilience Fund);

– Мережа центрів цифрових інновацій (DIC – Європейські центри цифрових інновацій (EDIHs));

– Фінансовий пакет для програми «Цифрова Європа» на період 2021–2027 рр.;

– Функціонування Європейського інституту інновацій та технологій (EIT), у тому числі EIT Digital, провідної європейської організації з цифрових інновацій та підприємницької освіти, яка є рушійною силою європейської цифрової трансформації;

– Цифрові індустріальні платформи, що сприяють цифровій трансформації підприємств, зокрема, мережа Європейських цифрових інноваційних хабів;

– План «Цифровий компас-2030»;
– Окремий сайт «Цифрова економіка та Society – Overview»;
– Програма «Шлях до цифрового десятиліття» (The Path to the Digital Decade).

Дослідимо ситуацію в Європейському Союзі, щоб сформувати правильну точку зору. Зокрема, це стосується кампаній, які оцінюють ризики цифрової безпеки, інформують своїх співробітників про зобов'язання щодо цифрової безпеки, проводять тестування безпеки або регулярне резервне копіювання, а також страхують від інцидентів цифрової безпеки.

Оскільки країни-члени ЄС суттєво відрізняються за характеристиками цифровізації, зокрема, дослідження базується на гіпотезі, що відмінності між країнами-членами ЄС, що відображають усі аспекти використання ними інформаційно-комунікаційних технологій, впливають на цифрову безпеку підприємств.

Результати дослідження базуються на статистиці ЄС та Організації економічного співробітництва та розвитку (ОЕСР) [11]. Що стосується досліджень використання ІКТ у країнах ЄС, джерелом даних є Європейський цифровий звіт про прогрес (EDPR), який містить цифровий профіль кожної країни, і щороку публікується Європейською Комісією; дані статистичного дослідження «Використання інформаційно-комунікаційних технологій (ІКТ) на підприємствах», результати якого опубліковані на сайті Євростату в розділі «Цифрова економіка та суспільство» [12].

Європейська комісія опублікувала результати Індексу цифрової економіки та суспільства (DESI) за 2022 рік, який відстежує прогрес, досягнутий у країнах-членах ЄС у сфері цифрових технологій. Індекс цифрової економіки та суспільства (DESI) — це зведений індекс, який узагальнює відповідні показники цифрової ефективності Європи та відстежує розвиток країн-членів ЄС за п'ятьма основними параметрами: людський капітал; підключення; інтеграція цифрових технологій; цифрові державні послуги [13].

З'ясовуючи сутність та особливості цифрової економіки на підставі даних звіту DESI 2022, нами було встановлено, що за останні три роки лідируючі позиції в цифровій економіці посіли Данія, Фінляндія та Нідерланди (найвищий рівень цифровізації) ; найнижчий рівень оцифрування спостерігався в Болгарії, Греції та Румунії.

Однак навіть країни-лідери стикаються з прогалинами в ключових сферах: впровадження передових цифрових технологій, таких як штучний інтелект і великі дані, залишається нижче 30% і дуже далеко від цільового показника Цифрового десятиліття до 2030 року в 75%; широко поширений

дефіцит навичок, який уповільнює загальний прогрес і призводить до цифрового виключення [13].

Цифровий компас спрямований на те, щоб щонайменше 75% компаній використовували штучний інтелект, хмару, технології великих даних до 2030 року. Бізнес все більше цифровізується; однак використання передових цифрових технологій залишається низьким. Лише кожна четверта компанія використовує хмарні обчислення та 14% великих даних [13].

Враховуючи багатофакторність та багатовимірність концепції цифрової безпеки підприємства, доцільно розглянути відсутність єдиного визначення та визнати можливість різних інтерпретацій цього поняття. При цьому в даному випадку виникає ще одна проблема: таке розмаїття концепцій породжує різноманітність методологічних підходів до визначення цифрової безпеки підприємств. До речі, оцінка цифрової безпеки підприємства є відносним показником, що відображає стан цифровізації, дає змогу забезпечити економіку підприємства, виміряну за певний період.

Для зручності та цінності практичного використання методичний підхід має відповідати ряду вимог [4]:

– відображувати ключові фактори цифрової трансформації в контексті сучасних економічних умов;
– забезпечувати простоту розрахунків та економічну інтерпретацію отриманих оціночних значень;
– не викликати труднощів щодо значень окремих показників, які входять до підсумкового показника;
– виключити зайвий суб'єктивізм у розрахункових значеннях.

Орієнтуючись на виконання вищевказаних вимог до оцінки цифрової безпеки підприємств, можна використовувати коефіцієнтний метод оцінки. Його суть полягає в розрахунку конкретних показників, що характеризують ефективність застосування елементів цифровізації підприємств. У цьому випадку кінцевий показник виходить як середнє арифметичне відповідних коефіцієнтів. Відповідно до цього підходу розраховуються показники цифрової безпеки підприємств країн-членів ЄС.

У цьому випадку можна використовувати показники статистичних органів (в ЄС– Євростат «ІКТ-безпека на підприємствах») [12] на рівні підприємств країни.

Оцінка ризиків цифрової безпеки – періодична оцінка ймовірності та наслідків інцидентів цифрової безпеки; це основа для управління ризиками цифрової безпеки (Табл. 3).

Таблиця 3

Особливості оцінки ризиків цифрової безпеки підприємств ЄС

Індикатор	Держава
Частка компаній, які проводять оцінку ризиків цифрової безпеки	Від 14 % в Угорщині до 60 % у Фінляндії. Показник зростає зі збільшенням розміру компанії (менше 1/3 серед малих компаній, наближається до 3/4 серед великих)
Передача ризику (страхування)	Від 4 % у Литві до понад 56 % у Данії. В усіх країнах ЄС, крім двох, схильність до передачі ризику зростає з розміром підприємств. У Данії він значно вищий серед малих підприємств (57 %) порівняно з середніми підприємствами (5 %) і великими підприємствами (40 %). Це також виявлено в Словенії, хоча й у значно меншій мір
Частка підприємств, на яких працюють люди, які знають про свої зобов'язання щодо безпеки ІКТ	Він коливається від 1/3 у Греції до понад 3/4 в Ірландії, де також спостерігається висока концентрація бізнесу в секторі ІКТ. Ця частка також зростає з розміром підприємств: менше 60% серед малих підприємств, але більше 90% серед великих

Джерело: Узагальнено та укладено автором відповідно до OECD на основі [14, 4].

У Європейському Союзі, згідно з даними OECD на основі Eurostat, методи оцінки ризиків цифрової безпеки для підприємств тісно пов'язані з тестами безпеки або процедурами резервного копіювання. У цілому можна зробити висновок, що великі компанії здійснюють цю діяльність в середньому набагато частіше, ніж малі.

Загалом тенденцію до страхування можна розглядати як ознаку серйозного ставлення компанії до цифрової безпеки. Однак це також залежить від наявності в країні страхових полісів, що покривають ризик цифрової безпеки. Традиційні страхові поліси або індивідуальні поліси кіберстрахування можуть покрити ризики.

Таким чином, усі згадані вище показники, засновані на даних Євростату, чітко показують, що тенденція підприємств до впровадження заходів цифрової безпеки зростає з їх розміром.

Дослідження підтвердило дослідницьку гіпотезу про те, що відмінності між країнами-членами впливають на досягнутий рівень впровадження та впровадження інформаційно-комунікаційних технологій на підприємствах країн ЄС.

Висновки. Впровадження цифрових технологій в бізнес-процеси підприємств несуть нові ризики та загрози, не властиві традиційним (нецифровим) процесам; вони зумовлені новими технологіями та особливостями цифрової економіки. Виявлення можливих ризиків і загроз є однією з найважливіших цілей забезпечення економічної безпеки підприємства в умовах цифрової економіки. Підхід до аналізу ризиків і загроз

підприємства в цифровій економіці має бути комплексним; він повинен охоплювати всі основні бізнес-процеси підприємства як у внутрішньому, так і зовнішньому середовищі.

Оцінка цифрової безпеки підприємств у країнах-членах ЄС показала, що малі та динамічні європейські економіки, зокрема, характеризуються вищими показниками безпеки в контексті цифровізації; саме вони досягають найкращих показників у впровадженні ІКТ. Вони шукають можливості для розвитку ІКТ і інтеграції, часто перевершують великі країни з розвиненою економікою щодо застосування цифрової безпеки на підприємствах.

Рівень фінансово-економічної безпеки впливає на впровадження на підприємствах передових інформаційних технологій, таких як хмарні обчислення та електронного бізнесу, сприяє розвитку культури інформаційного бізнесу та прагненню підприємств до впровадження сучасних ІКТ, що потребує відповідної модернізації.

Потрібні додаткові дослідження для з'ясування впливу цих факторів і можливої ідентифікації інших факторів, що впливають на цифрову безпеку підприємств. Зокрема, потребує подальшого вивчення питання впливу регіональної ситуації країн на цифрову безпеку підприємств. Разом з цим, наступними напрямками вивчення може бути розробка методологічних засад визначення рівня цифрової безпеки підприємства та її подальшої модернізації на основі системи показників, зокрема використання цифрового маркетингу, аналіз роботи у віддаленому режимі та використання технологій цифрової економіки.

Література:

1. Ianioglo, A. and Polajeva, T. (2016). Origin and definition of the category of economic security of enterprise, in 9th International Scientific Conference proceedings "Business and Management 2016", 12–13 May 2016, Vilnius, Lituania, 1–8. https://doi.org/10.3846/bm.2016.46.

2. Яниогло А.И. Проблемы обеспечения экономической безопасности на предприятии // Науково-виробничий журнал «Інноваційна економіка», 1-2'2018 [73]. С. 201-211.

3. Бакай В. Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій // Вісник Хмельницького національного університету, 2020, № 4, Том 1. DOI: 10.31891/2307-5740-2020-284-4-5. URL: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/01/7-19.pdf (дата звернення: 09.02.2023).

4. Samoilenko, Y., Britchenko, I., Levchenko, I., Lošonczi, P., Bilichenko, O. and Bodnar, O. (2022). Economic Security of the Enterprise Within the Conditions of Digital Transformation. Econ. Aff., 67(04): 619-629.

5. Zigunova A., Shevkunov N., Logvinova I., Kislov I., Shevchenko V. Ensuring economic security of the enterprise in anti-crisis conditions. URL: https://www.e3s-conferences.org/articles/e3sconf/pdf/2020/17/e3sconf_ktti2020_04030.pdf (дата звернення: 09.02.2023).

6. Неустроєв Ю. Г. Забезпечення економічної безпеки держави: досвід зарубіжних країн. Агросвіт. 2021. № 5-6. С. 87–92. DOI: 10.32702/2306-6792.2021.5-6.87.

7. Stankic, R., Jovanovic Gavrilovic, B. and Soldic Aleksic, J. (2018). Information and communication technologies in education as a stimulus to economic development. Econ. Horizons, 20(1): 59–71.

8. Roztocki, N., Soja, P. and Weistroffer, H.R. (2019). The role of information and communication technologies in socioeconomic development: Towards a multidimensional framework. Information Techno. for Dev., 25(2): 171–183.

9. Касьянова Н. В., Кравчук Н. М., Коваль Ю. Л. Безпека підприємства в умовах цифрової трансформації економіки. Modern Economics. 2020. № 20(2020). С. 124-129. DOI: https://doi.org/10.31521/modecon.V20(2020)-20. (дата звернення: 09.02.2023).

10. Becker, J., Becker, A., Sulikowski, P. and Zdziebko, T. (2018). ANP-based analysis of ICT usage in Central European enterprises. Paper presented at the 22nd International Conference on Knowledge-Based and Intelligent Information, & Engineering Systems. Procedia Computer Science, 126: 2173–2183.

11. OECD (2021). The Digital Transformation of SMEs URL: https:// www.oecd.org/industry/smes/PH-SME-Digitalisationfinal.pdf (дата звернення: 11.02.2023)

12. Eurostat (2022). Security policy: measures, risks and staff awareness by size class of enterprise. URL: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en.https:%2F%2Fec.europa.eu%2Feurostat%2Fdatabrowser%2Fview%2Fisoc_cisce_ic%2Fdefault%2Ftable%3Flang%3Den (дата звернення: 11.02.2023).

13. European commission (2022). Digital Economy and Society Index 2022: overall progress but digital skills, SMEs and 5G networks lag behind. URL: https://ec.europa.eu/ commission/presscorner/detail/en/ip_22_4560. (дата звернення: 11.02.2023).

14. Eurostat (2022). Digital Economy and Society Statistics, Comprehensive Database. URL: https://ec.europa.eu/eurostat/web/digital-economy-and-society. (дата звернення: 11.02.2023).

References:

1. Ianioglo, A. & Polajeva, T. (2016). Origin and definition of the category of economic security of enterprise. *9th International Scientific Conference proceedings "Business and Management 2016"*, Vilnius, Lituania, 1–8. https://doi.org/10.3846/bm.2016.46 [in English].

2. Ianioglo, A.I. (2018). Problemi obespechenyia ekonomycheskoi bezopasnosty na predpryiatyy. [Problems of ensuring economic security at the enterprise]. *Naukovo-vyrobnychyi zhurnal «Innovatsiina ekonomika»*, 1-2, [73], 201-211. [in Russian].

3. Bakai, V.Y. (2020). Zabezpechennia ekonomichnoi bezpeky pidpryiemstva na osnovi vykorystannia tsyfrovykh tekhnolohii. [Ensuring the economic security of the enterprise based on the use of digital technologies]. *Visnyk Khmelnytskoho natsionalnoho universytetu*, № 4, Tom 1. Retrieved from http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/01/7-19.pdf [in Ukrainian].

4. Samoilenko, Y., Britchenko, I., Levchenko, I., Lošonczi, P., Bilichenko, O. and Bodnar, O. (2022). Economic Security of the Enterprise Within the Conditions of Digital Transformation. *Econ. Aff.*, 67(04), 619-629 [in English].

5. Zigunova, A., Shevkunov, N., Logvinova, I., Kislov, I., and Shevchenko, V. (2020). Ensuring economic security of the enterprise in anti-crisis conditions. Retrieved from:: https://www.e3s-conferences.org/articles/e3sconf/pdf/2020/17/e3sconf_ktti2020_04030.pdf [in English].

6. Neustroiev, Y. (2021). Ensuring the economic security of the state: experience of foreign countries. *Agrosvit*, vol. 5-6, pp. 87–92. DOI: 10.32702/2306-6792.2021.5-6.87 [in Ukrainian].

7. Stankic, R., Jovanovic Gavrilovic, B. and Soldic Aleksic, J. (2018). Information and communication technologies in education as a stimulus to economic development. *Econ. Horizons*, 20(1). 59–71. [in English].

8. Roztocki, N., Soja, P. and Weistroffer, H.R. (2019). The role of information and communication technologies in socioeconomic development. *Towards a multidimensional framework. Information Techno*. for Dev., 25(2). 171–183. [in English].

9. Kasianova. N., Kravchuk, N. & Koval, Y. (2020). Enterprise security under digital transformation of economics. *Modern Economics*, 20(2020), 124-129. DOI: https://doi.org/10.31521/modecon.V20(2020)-20 [in Ukrainian].

10. Becker, J., Becker, A., Sulikowski, P. and Zdziebko, T. (2018). ANP-based analysis of ICT usage in Central European enterprises. *Paper presented at the 22nd International Conference on Knowledge-Based and Intelligent Information, & Engineering Systems. Procedia Computer Scienc*e, 126, 2173–2183. [in English].

11. OECD (2021). The Digital Transformation of SMEs. Retrieved from: https:// www.oecd.org/industry/smes/PH-SME-Digitalisationfinal.pdf [in English].

12. Eurostat (2022). Security policy: measures, risks and staff awareness by size class of enterprise. Retrieved from: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en.https:%2F%2Fec.europa.eu%2Feurostat%2Fdatabrowser%2Fview%2Fisoc_cisce_ic%2Fdefault%2Ftable%3Flang%3Den [in English].

13. European commission (2022). Digital Economy and Society Index 2022: overall progress but digital skills, SMEs and 5G networks lag behind. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4560. [in English].

14. Eurostat (2022). Digital Economy and Society Statistics, Comprehensive Database. Retrieved from: https:// ec.europa.eu/eurostat/web/digital-economy-and-society [in English].