

DOI: <https://doi.org/10.32782/2524-0072/2025-78-72>

УДК 336.6:338.24:65.012.8

ТРАНСФОРМАЦІЯ СИСТЕМИ УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА В УМОВАХ СУЧАСНИХ ЗАГРОЗ

TRANSFORMATION OF FINANCIAL AND ECONOMIC SECURITY MANAGEMENT SYSTEM OF AN ENTERPRISE IN THE CONTEXT OF CONTEMPORARY THREATS

Проскура Володимир Федоровичдоктор економічних наук, професор,
Мукачівський державний університет
ORCID: <https://orcid.org/0000-0001-5494-0039>**Лизанець Анжела Гейзівна**кандидат економічних наук, доцент,
Мукачівський державний університет
ORCID: <https://orcid.org/0000-0002-6432-1685>**Гриць Мирон Миронович**магістр,
Мукачівський державний університет
ORCID: <https://orcid.org/0009-0002-6584-6122>**Proskura Volodymyr, Lyzanets Anzhela, Hryts Myron**
Mukachevo State University

У статті проаналізовано виклики та дисфункції системи управління фінансово-економічною безпекою (ФЕБ) українських підприємств в умовах глобальних і локальних ризиків. Ідентифіковано ключові загрози для ФЕБ: кіберзагрози, кадрова нестабільність, відсутність інтегрованих систем ризик-менеджменту, фінансові й логістичні потрясіння, тінізація економіки. Показано, що традиційні моделі ФЕБ, орієнтовані лише на фінансові показники та охоронні механізми, не відповідають вимогам цифрової економіки та воєнних викликів. Обґрунтовано необхідність переходу до інтегрованих, ризик-орієнтованих систем, що поєднують стратегічне планування, цифрові технології, кіберзахист, кадрову політику та антикризовий менеджмент. Запропоновано напрями модернізації системи управління ФЕБ сучасних підприємств через впровадження ERP-рішень, BI-аналітики, AI-моделювання, політики кіберзахисту, інвестицій у людський капітал та гібридних моделей управління ризиками.

Ключові слова: фінансово-економічна безпека, управління фінансово-економічною безпекою підприємства, ризик-менеджмент, цифрова трансформація, інформаційна гігієна та кіберзахист, ризик-орієнтована система управління фінансово-економічною безпекою.

The article examines the transformation of the financial and economic security (FES) management system of Ukrainian enterprises in the context of modern threats. The aim of the work is to identify key risks, assess the state of financial and economic security of national enterprises, and determine directions for modernising business security management systems, taking into account global and local challenges. The relevance of the topic is due to full-scale war, the digitalisation of business processes, the transformation of supply chains, the growth of cyber threats and personnel instability, which together increase the financial and organisational risks of enterprises. The methodological basis of the study was the system approach, methods of logical and comparative analysis, the risk-oriented approach, and structural-functional analysis, which made it possible to identify the main dysfunctions and vulnerability factors of the FES. The article identifies key threats of FES management system, including low levels of cyber security, lack of integrated risk management systems, personnel instability, high dependence on individual specialists, financial and logistical risks, shadow economy and fraudulent schemes that have intensified in the context of war. It shows that most enterprises use a reactive crisis response FES strategy, while modern conditions require the implementation of digital forecasting and crisis management technologies, including BI analytics, artificial



intelligence (AI), Big Data, and ERP solutions. Conceptual approaches to modernising the FES management system have been grounded, which include the digitalisation of business processes, the development of comprehensive cyber security policies, investment in human capital and the implementation of hybrid risk management models that combine international standards and local features of the Ukrainian war economy. The practical value of the scientific work is in the possibility of usage the proposed approaches to form adaptive and sustainable FES management systems capable of ensuring business continuity and increasing the competitiveness of enterprises in the environment of increased uncertainty.

Keywords: financial and economic security, management of financial and economic security of an enterprise, risk management, digital transformation, information hygiene and cyber protection, risk-oriented financial and economic security management system.

Постановка проблеми. Після початку повномасштабної збройної агресії Росії проти України у 2022 році рівень економічних загроз для українських підприємств почав різко зростати і це зростання, нажаль, продовжується і на даний момент часу. Зруйнована логістична інфраструктура, втрата ринків збуту, переміщення виробництва, перебої в електропостачанні, мобілізація персоналу, зростання енергетичних та сировинних витрат, кіберзагрози та постійні кібератаки – усе це сформувало нову реальність для національного бізнесу.

У таких умовах особливої актуальності набуває менеджмент фінансово-економічної безпеки (ФЕБ) підприємств як інструмент адаптації до умов воєнної економіки. Забезпечення платоспроможності, збереження персоналу, управління ризиками, захист інформаційних ресурсів і гнучке стратегічне планування – стають критично важливими чинниками виживання підприємств у коротко- та середньостроковій перспективі.

Аналіз останніх досліджень і публікацій. Проблематика фінансово-економічної безпеки підприємств є предметом активного дослідження як вітчизняних, так і зарубіжних науковців.

Основи теоретичного розуміння ФЕБ в Україні були закладені в працях таких дослідників, як Орлик О. В. [1], який запропонував структурну модель управління ФЕБ (фінансова, інвестиційна, інформаційна, кадрова безпека тощо). Христенко Л. М. та співавтори [4] досліджують проблеми безпеки підприємств у контексті геополітичної та економічної турбулентності, пов'язаної з війною.

Інформаційні аспекти ФЕБ у цифрову епоху висвітлені в працях Атамаса О. П. і Майстера Т. М. [2], які наголошують на ролі IT-інфраструктури в захисті активів підприємства. Кадровий чинник та ризики втрати людського капіталу розкриті у дослідженнях Шири Т. та Чупи Б. [3]. Маркетингову складову ФЕБ у стратегічному управлінні аналізує Келманович О. [5].

На міжнародному рівні концепція фінансово-економічної безпеки (часто – як *corporate security*, *financial resilience*, *enterprise risk management*) розглядається комплексно, з акцентом на стратегічний ризик-менеджмент, кібербезпеку та забезпечення сталості бізнесу.

Зокрема, Robert S. Kaplan та Anette Mikes (Harvard Business School) у своїх працях [6] розробили концепцію Enterprise Risk Management (ERM) як інструмент інтеграції стратегічного, операційного та фінансового ризику в систему управління підприємством; Michael Porter та Mark Kramer (Harvard) [7] підкреслюють важливість створення спільної цінності (*shared value*) як механізму захисту підприємства через посилення його стійкості до зовнішніх шоків; Benoit Mandelbrot та Nassim Taleb [8] акцентували увагу на нестійкості традиційних моделей безпеки в умовах непередбачуваних подій (*black swans*) та необхідності адаптивного, антикрихкого управління; Wim Van Grembergen (Belgium) та Steven De Haes [9] досліджували інформаційну безпеку підприємств як частину загального IT-governance, вказуючи на необхідність включення кіберзахисту до систем управління ризиками.

В Європейському Союзі питання корпоративної безпеки та управління стійкістю бізнесу також розглядаються в межах політик ESG (Environmental, Social, Governance), зокрема в публікаціях OECD та European Risk Management Council [10].

Таким чином, як українські, так і зарубіжні автори погоджуються з тим, що ефективне управління фінансово-економічною безпекою має бути інтегрованим, стратегічним та адаптивним до нових викликів. Однак більшість іноземних концепцій сформовані в умовах стабільного середовища, і потребують адаптації до реалій українських підприємств, які діють в умовах війни, мобілізації та зруйнованої інфраструктури.

Виділення невирішених раніше частин загальної проблеми. Водночас, попри зна-

чну теоретичну базу, існує дефіцит комплексних практико-орієнтованих досліджень, які б узагальнювали досвід українських підприємств в умовах повномасштабної війни. Це зумовлює потребу у подальшій науковій розробці проблеми, зокрема щодо впровадження ефективних систем управління ФЕБ в умовах високої турбулентності та нестабільності зовнішнього середовища.

Формулювання цілей статті (постановка завдання). Метою даного дослідження є всебічне обґрунтування та удосконалення підходів до менеджменту фінансово-економічної безпеки підприємства в умовах сучасних викликів, зокрема воєнного стану, цифрової трансформації та зростання системних ризиків, а також надання підприємствам методологічної й інструментальної основи для побудови адаптивної, стійкої та цифрово-орієнтованої системи управління ФЕБ, здатної ефективно функціонувати навіть в умовах кризових чи екстремальних ситуацій.

Виклад основного матеріалу дослідження. Фінансово-економічна безпека (ФЕБ) підприємства – це здатність суб'єкта господарювання захищати свої активи, ресурси, фінансові потоки та інтереси від зовнішніх і внутрішніх загроз, забезпечуючи стабільність та ефективність функціонування в умовах ризику та невизначеності.

Фінансово-економічна безпека підприємства в умовах сучасних викликів, зокрема повномасштабної війни, трансформації глобальних ланцюгів постачання, цифровізації та геополітичної напруги, перебуває під значним тиском. Стан ФЕБ визначається не лише фінансовою стабільністю, а й здатністю системи менеджменту забезпечувати стійкість до багатofакторних загроз.

На даний час однією з найгостріших загроз ефективній діяльності вітчизняних підприємств є слабкий захист інформаційної інфраструктури тобто інформаційна безпека підприємств. Як зазначають Атамас О. П. та Майстер Т. М. [2], недостатній рівень інформатизації, застаріле програмне забезпечення, відсутність чітких регламентів кіберзахисту та слабкий контроль за інформаційними потоками створюють передумови для: витоку конфіденційної інформації (комерційна таємниця, клієнтські бази, фінансові звіти); фішингових атак, зараження систем шкідливим ПЗ; паралізації бізнес-процесів у результаті DDoS-атак чи шифрування даних (ransomware).

У 2024 році зафіксовано різке зростання кібератак на українські компанії, зокрема у

фінансовому, логістичному та промисловому секторах. Зокрема, за 2024 рік CERT-UA (Державна служба спеціального зв'язку та захисту інформації України) зафіксувала 4315 інцидентів, що на 69,8 % більше, ніж у 2023 році, коли було зареєстровано 2541 інцидент. У другому півріччі 2024 року Україна зазнала 2 576 російських кібератак, що на 48% більше, ніж у першому півріччі. Проте, лише невеликий відсоток підприємств мають політику інформаційної безпеки, резервне копіювання та сценарії реагування на кіберінциденти.

Таким чином інформаційна вразливість вітчизняних підприємств на даний час є досить високою і несе ряд загроз, негативний вплив яких ліквідовується важко і тривалий час. До них, як правило відносять втрати даних, блокування фінансових операцій, репутаційні ризики.

Наступною серйозною загрозою для ФЕБ підприємства є те, що в умовах війни спостерігається дефіцит кваліфікованого персоналу через мобілізацію, евакуацію, релокацію підприємств і психологічне вигорання працівників. Шири Т. та Чупа Б. [3] наголошують на тому, що зниження мотивації та емоційне вигорання працівників суттєво впливають на зниження ефективності прийняття управлінських рішень, а відповідно і діяльності підприємства. Крім того, високий рівень плинності кадрів у сфері безпеки, ІТ та аналітики зменшує здатність підприємств своєчасно реагувати на загрози. Наявність знань і досвіду у сфері ФЕБ часто зосереджена в одиничних спеціалістів, що підвищує залежність від людського фактора.

На переважній більшості вітчизняних підприємств довоєнний період спостерігалася така загроза ФЕБ як відсутність системного підходу до організації та менеджменту ФЕБ. На даний час, на жаль, ситуація не змінилася. Орлик О. В. [1] відзначає, що значна частина українських підприємств продовжує використовувати фрагментарний, ситуативний підхід до менеджменту ФЕБ, замість розбудови комплексної системи ризик-менеджменту. Така реактивність виявляється у: відсутності чітких алгоритмів дій при фінансових чи інформаційних загрозах; нехтуванні побудовою моделей сценарного прогнозування; несумісності підсистем (фінансової, юридичної, кадрової, ІТ-безпеки). На підприємствах відсутні або слабо функціонують системи раннього попередження загроз: немає впроваджених ERM-систем (Enterprise Risk Management); моніторинг загроз часто

ведеться вручну або епізодично; недостатньо використовуються цифрові аналітичні інструменти (BI (Business Intelligence), Big Data, AI (Artificial intelligence)).

Це робить підприємства вразливими до навіть незначних змін у зовнішньому середовищі. Крім того, антикризові плани на багатьох підприємствах або застарілі, або відсутні взагалі. Вирішити проблему відсутності цілісної системи менеджменту ФЕБ можна шляхом впровадження ERM, GRC, адаптивного менеджменту.

В сучасних умовах у зв'язку із залежністю вітчизняної економіки від іноземного інвестування на діяльність підприємств посилюється вплив глобальних викликів які також можна розглядати як загрозу ФЕБ підприємства. Христенко Л. М. та ін. [4] зазначають, що сучасне середовище ведення бізнесу зазнає багаторівневого тиску: глобальна інфляція та коливання валют; енергетичні ризики та перебої в постачанні (знищення енергетичної інфраструктури); зміни у споживчому попиті та зменшення платоспроможності ринку; глобальні логістичні затримки, санкційні обмеження.

Ці чинники ускладнюють фінансове планування, зменшують інвестиційну привабливість і вимагають високої гнучкості. В умовах глобальної нестабільності безпека підприємства повинна бути адаптивною, а система менеджменту – побудована на багатосценарному прогнозуванні.

Рівень тінізації вітчизняної економіки є також серйозною загрозою для ФЕБ підприємства. Як не парадоксально, але за роки повномасштабного вторгнення не відбулося зниження сили тиску цієї загрози. У воєнний час активізувався тіньовий бізнес, схеми нелегального обігу коштів, зловживання на військових замовленнях, махінації з ПДВ, нелегальна логістика; почастишали випадки зниження рівня прозорості фінансової звітності у частини підприємств, набирає обертів фіктивна волонтерська діяльність.

Таким чином актуальні проблеми менеджменту ФЕБ вимагають глибокої трансформації погляду на безпеку – від захисної функції до інтегрованого стратегічного інструменту управління стійкістю підприємства. Ключ до вирішення ми вбачаємо у поєднанні цифрових технологій, системного мислення та людського потенціалу.

Менеджмент ФЕБ в Україні потребує негайного зміщення фокусу: від реактивного підходу до системної, ризик-орієнтованої моделі,

яка інтегрує стратегічне планування, сучасні цифрові інструменти та людський потенціал; змінити стратегію «виживання» на стратегію «трансформації».

Удосконалення системи управління фінансово-економічною безпекою (ФЕБ) вимагає комплексного підходу, що поєднує цифрові інструменти, ризик-орієнтоване мислення, кадрову стратегію та антикризове планування. На основі аналізу сучасних публікацій, нормативних документів і практичного досвіду функціонування українських і зарубіжних підприємств, можна виокремити п'ять ключових напрямків трансформації системи менеджменту ФЕБ:

1. Цифровізація та впровадження ERP-систем. Передбачає перетворення аналогових процесів на цифрові з метою підвищення ефективності, спрощення взаємодії та створення нових можливостей щодо запровадження в діяльність підприємства сучасних інформаційних систем управління ресурсами (ERP – Enterprise Resource Planning) які дають можливість централізовано, в режимі реального часу проводити моніторинг кадрових, виробничих, фінансових та логістичних показників. Такі системи забезпечують: автоматичне виявлення відхилень від критичних показників; побудову дашбордів для управлінського моніторингу; інтеграцію з CRM, логістичними та бухгалтерськими модулями; оперативне реагування на ризики завдяки сценарному моделюванню. ERP-платформи (як-от SAP, Oracle NetSuite) стають основою для прозорого фінансового контролю, запобігання помилкам і шахрайству.

2. Ризик-менеджмент на основі даних, сценарного аналізу та ШІ. Сучасний менеджмент ФЕБ потребує переходу до превентивного, аналітичного управління ризиками. Це передбачає: побудову систем управління ризиками (ERM); використання сценарного аналізу з моделюванням різних умов розвитку подій (best case / worst case); практичне використання інструментів Business Intelligence (BI) для візуалізації даних у процесі розробки та підтримки прийняття управлінських рішень; впровадження моделей прогнозування на основі AI/ML для виявлення фінансових ризиків, коливань попиту та різного роду аномалій. Такі підходи забезпечують проактивну політику безпеки, що дозволяє адаптувати стратегії до швидкозмінного середовища.

3. Формування маркетингової стратегії безпеки. Оригінальний підхід запропонував

Келманович О. [5], який розглядає маркетингову стратегію безпеки як один із компонентів ФЕБ. Цей підхід базується на позиціонуванні підприємства на стабільних ринках, що характеризуються: низьким рівнем макроекономічної турбулентності; прогнозованими змінами у споживчому попиті; стабільністю нормативно-правового регулювання. Окрім того, маркетингова стратегія безпеки передбачає активне управління репутаційними ризиками, прозорість комунікацій та сталу взаємодію з клієнтами, що сприяє підвищенню довіри та лояльності.

4. Інформаційна гігієна та кіберзахист. Інформаційна гігієна як підсистема ФЕБ передбачає формування політик з обробки, зберігання й передачі інформації, а також технічне забезпечення кіберзахисту. До основних інструментів відносять: перш за все регулярне навчання персоналу з основ кібергігієни та введення багаторівневої системи доступу до даних; дієвим та результативним є також запровадження: резервного копіювання на захищених серверах (on-premise або cloud); двофакторна автентифікація (2FA) та системи виявлення загроз (IDS/IPS). Інвестиції у кібербезпеку, особливо в умовах гібридної війни, стають не розкішшю, а необхідністю для стійкості бізнесу.

5. Інвестиції в людський капітал. Управління персоналом як фактором ФЕБ передбачає довгострокову політику утримання, навчання та захисту ключових працівників. Напрями удосконалення включають: запровадження мотиваційних програм в умовах воєнного ризику (гнучкий графік, компенсації, соціальні пакети); корпоративне навчання з питань кризового менеджменту, антикризового управління, кіберзахисту, що дозволяє швидко замінити втрачені позиції у критичних функціях. Людський капітал стає основною гарантією стабільності в нестабільному середовищі.

Висновки. У сучасних умовах соціально-економічної нестабільності, військових загроз, цифрових трансформацій та геополітичної турбулентності, фінансово-економічна безпека (ФЕБ) підприємства набуває системного, багатовимірного характеру. Традиційні підходи до забезпечення ФЕБ, що зосереджувалися виключно на фінансових показниках і бухгалтерському контролі, сьогодні виявляються недостатніми.

Удосконалення менеджменту ФЕБ має відбуватися за рахунок комплексної трансформації – цифрової, структурної та культур-

ної. Це включає гнучке управління ризиками, кіберзахист, підвищення прозорості, орієнтацію на дані та посилення людського потенціалу. Такий підхід формує адаптивну, антикрихку модель підприємства, здатну діяти ефективно в умовах невизначеності.

Українські підприємства можуть значно виграти від адаптації західних систем ERM, ESG, GRC, за умови врахування локальних ризиків – воєнних, енергетичних, інституційних. Комбінація кращих практик обох підходів дасть змогу створити ефективну гібридну модель управління ФЕБ, яка буде релевантною в умовах турбулентності, характерної для сучасної України. Зокрема, Kaplan & Mikes [6] у концепції Enterprise Risk Management (ERM) пропонують системну інтеграцію ФЕБ у стратегічне планування та управління ресурсами.

Ми вбачаємо формування ефективного менеджменту ФЕБ у переході до інтегрованої, гнучкої та ризик-орієнтованої моделі управління, яка включає такі ключові компоненти:

1) цифрова трансформація – комплексне запровадження в систему управління підприємством штучного інтелекту, ERP-систем, хмарних технологій; сучасного комплексу методів, інструментів і технологій для збору, обробки, аналізу та візуалізації даних (Business Intelligence (BI)), а також аналітики великих даних дозволяє підняти менеджмент на якісно новий рівень, забезпечуючи проактивне управління ризиками, оперативний моніторинг показників та автоматизацію фінансових процесів;

2) сучасний ризик-менеджмент – використання сценарного аналізу, індикативних моделей, оцінки ймовірностей та мультифакторного прогнозування дає змогу адаптуватися до нових загроз і запобігати системним втратам;

3) інформаційна безпека – з огляду на гібридну війну та кіберзагрози, підприємства мають створювати цілісну систему інформаційного захисту, включаючи кібергігієну, політику доступу, криптографічні засоби та систему реагування на інциденти;

4) кадровий аспект – розвиток людського капіталу, збереження експертного потенціалу, формування внутрішніх систем підвищення кваліфікації, утримання ключових працівників та впровадження гнучких форм мотивації є визначальними чинниками стійкості та гнучкості системи ФЕБ;

5) стратегічне позиціонування та маркетингова безпека – орієнтація на стабільні

ринки, репутаційна прозорість та комунікаційна стійкість формують довготривалу конкурентоспроможність підприємства.

У підсумку слід зазначити, що забезпечення фінансово-економічної безпеки підприємства – це не ізольована функція, а невід’ємна частина загальної стратегії управління підприємством, яка охоплює всі рівні – від оперативного до стратегічного. Ефективна система менеджменту ФЕБ має бути адап-

тивною, цифровізованою, антикризовою та орієнтованою на стале зростання.

Подальші дослідження доцільно спрямувати на поглиблення аналізу інструментів ESG, міжнародних стандартів GRC (Governance, Risk, Compliance), а також на оцінку ефективності впровадження моделі «антикрихкого підприємства» (антиризикова організація, за Н. Талебом) в умовах воєнного і поствоєнного періоду.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Орлик О. В. Механізм управління фінансово-економічною безпекою підприємства. *Financial and Credit Activity: Problems of Theory and Practice*. 2015, 2(19).
2. Атамас О. П., Майстер Т. М. Удосконалення системи управління інформаційною складовою фінансово-економічної безпеки підприємства. *Проблеми сучасних трансформацій. Серія: економіка та управління*. 2023. № 8. URL: <https://www.reicst.com.ua> (дата звернення: 14.09.2025).
3. Шира Т., Чупа Б. Менеджмент персоналом на підприємстві: виклики в системі забезпечення фінансово-економічної безпеки. *Економіка та суспільство*. 2024. Вип. 65. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4489> (дата звернення: 14.09.2025).
4. Христенко Л. М., Прохоровська С. А., Гречишкін С. А. Сучасні стратегії забезпечення фінансово-економічної безпеки підприємств у контексті глобальних викликів. *Актуальні питання економічних наук*. 2025. № 9. URL: <https://a-economics.com.ua> (дата звернення: 14.09.2025).
5. Келманович О. Сучасні аспекти формування маркетингової стратегії підвищення фінансово-економічної безпеки підприємства. *Modeling the development of the economic systems*. 2024. № 2. С. 333–339.
6. Kaplan R. S., Mikes A. Managing Risks: A New Framework. *Harvard Business Review*. 2012. URL: <https://www.ferma.eu/wp-content/uploads/2013/03/hbr-managing-risks-a-new-framework.pdf> (дата звернення: 14.09.2025).
7. Porter M. E., Kramer M. R. Creating Shared Value. *Harvard Business Review*. 2011. Vol. 89, No. 1, pp. 2–17. URL: <https://www.communitylivingbc.ca/wp-content/uploads/2018/05/Creating-Shared-Value.pdf> (дата звернення: 14.09.2025).
8. Taleb N. N. The Black Swan: The Impact of the Highly Improbable. Random House Publishing Group, 2010, p. 480.
9. Van Grembergen W., De Haes S. Enterprise Governance of IT: Achieving Strategic Alignment and Value,” Springer. 2009.
10. European Risk Management Council. URL: <https://riskcouncil.org/> (дата звернення: 12.09.2025).

REFERENCES:

1. Orlyk, O. V. (2015). Mekhanizm upravlinnia finansovo-ekonomichnoiu bezpekoiu pidpriemstva [Mechanism of managing the financial and economic security of the enterprise]. *Financial and Credit Activity: Problems of Theory and Practice*, vol. 2(19).
2. Atamas, O. P., Maister, T. M. (2023). Udoskonalennia systemy upravlinnia informatsiinoiu skladovoiu finansovo-ekonomichnoi bezpeky pidpriemstva [Improving the management system of the information component of financial and economic security of the enterprise]. *Problemy suchasnykh transformatsii. Seriya: Ekonomika ta upravlinnia*, vol. 8. Available at: <https://www.reicst.com.ua> (accessed September 14, 2025).
3. Shyra, T., Chupa, B. (2024). Menedzhment personalom na pidpriemstvi: vyklyky v systemi zabezpechennia finansovo-ekonomichnoi bezpeky [Personnel management at the enterprise: Challenges in the system of ensuring financial and economic security]. *Ekonomika ta suspilstvo*, vol. 65. Available at: <https://economyandsociety.in.ua/index.php/journal/article/view/4489> (accessed September 14, 2025).
4. Khrystenko, L. M., Prokhorovska, S. A., Hryshchyskin, S. A., (2025). Suchasni stratehii zabezpechennia finansovo-ekonomichnoi bezpeky pidpriemstv u konteksti hlobalnykh vyklykiv [Modern strategies for ensuring the financial and economic security of enterprises in the context of global challenges]. *Aktualni pytannia ekonomichnykh nauk*, vol. 9. Available at: <https://a-economics.com.ua> (accessed September 14, 2025).

5. Kelmanovych, O. (2024). Suchasni aspekty formuvannia marketynhovoï stratehii pidvyshchennia finansovo-ekonomichnoi bezpeky pidpriemstva [Modern aspects of forming a marketing strategy to increase the financial and economic security of the enterprise]. *Modeling the Development of the Economic Systems*, vol. 2, pp. 333–339.
6. Kaplan, R. S., Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review*. Available at: <https://www.ferma.eu/wp-content/uploads/2013/03/hbr-managing-risks-a-new-framework.pdf>. (accessed September 14, 2025).
7. Porter, M. E., Kramer, M. R. (2011). Creating shared value. *Harvard Business Review*. Vol. 89, no. 1, pp. 2–17. Available at: <https://www.communitylivingbc.ca/wp-content/uploads/2018/05/Creating-Shared-Value.pdf>. (accessed September 14, 2025).
8. Taleb N. N. (2010) The Black Swan: The Impact of the Highly Improbable. *Random House Publishing Group*, p. 480.
9. Van Grembergen W., De Haes S. (2009) Enterprise Governance of IT: Achieving Strategic Alignment and Value. *Springer*.
10. European Risk Management Council. Available at: <https://riskcouncil.org/> (accessed September 12, 2025).