Нові виклики та загрози цифрової трансформації економіки для системи фінансово-економічної безпеки підприємництва

Линда Іван Степанович[1]

Опубліковано	Секція	УДК
12.12.2025	Економіка	330.341.1:004:336.6

DOI: https://doi.org/10.5281/zenodo.17909029

Анотація. У статті досліджено новітні тенденції цифрової трансформації економіки України та їхній вплив на систему фінансово-економічної безпеки підприємництва в умовах війни та повоєнного відновлення. Обґрунтовано, що активне впровадження цифрових технологій, платформних бізнес-моделей і віддалених форм організації діяльності з одного боку підвищує стійкість та адаптивність підприємницького сектора, а з іншого – генерує нові виклики, пов'язані з кіберзагрозами, витоком комерційних даних, тіньовими електронними операціями та зовнішньою залежністю від цифрової інфраструктури. Визначено напрями адаптації механізмів забезпечення фінансово-економічної безпеки бізнесу через інтеграцію інструментів управління цифровими ризиками, удосконалення регуляторного середовища та розвиток партнерств держави і бізнесу у сфері захисту цифрового простору. Наголошено, що формування безпечного цифрового середовища є стратегічною передумовою посилення конкурентоспроможності, інвестиційної привабливості та прискорення економічного відновлення України в поствоєнний період.

Ключові слова: фінансово-економічна безпека, сектор підприємництва, бізнес, фінансові ризики і загрози, цифрова трансформація, виклики і загрози, державна політика і регулювання, інструменти зміцнення, фінансові ресурси.

New Challenges and Threats of Digital Transformation of the Economy for the System of Financial and Economic Security of Entrepreneurship

Abstract. The article examines the newest trends in the digital transformation of Ukraine's economy and their multidimensional impact on the system of financial and economic security of entrepreneurship in wartime conditions and throughout the post-war recovery phase. The study substantiates that the intensification of digitalization processes, the development of platform-based business models, the implementation of cloud services, remote work formats, and digital public services significantly transform the structure and dynamics of business processes, creating new opportunities for the resilience, adaptability, and innovation capacity of enterprises. However, it is emphasized that this transition simultaneously generates a wide spectrum of risks and threats to financial and economic security, including the rapid growth of cyberattacks, increased vulnerability of critical digital infrastructures, leakage of commercial and personal data, expansion of shadow digital markets, and heightened dependence on global technological providers.

[1] к.е.н., доцент, докторант Львівського торговельно-економічного університету, https://orcid.org/0009-0001-6325-7669

The research identifies the necessity of redesigning the mechanisms for protecting financial and economic security through a system-based integration of digital risk management, strengthening corporate cybersecurity standards, modernization of regulatory frameworks, and the institutionalization of public–private partnerships in the sphere of digital protection and information resilience. It is highlighted that enhancing digital literacy and cybersecurity culture among entrepreneurs is becoming a crucial factor for mitigating cyber threats and ensuring sustainable functioning in the digital economic environment. Special attention is devoted to the strategic importance of secure digital infrastructure for improving the investment climate, ensuring transparency of financial transactions, and strengthening the competitive position of domestic business in global markets.

The article concludes that creating a safe, resilient, and innovation-driven digital ecosystem is a key prerequisite for accelerating post-war economic recovery, attracting investments, and building long-term competitiveness of the national entrepreneurial sector. Strengthening the policy of financial and economic security in the context of digital transformation should evolve as a comprehensive and forward-looking process aligned with European standards and international best practices, thereby ensuring the integration of Ukraine into the global digital economy on principles of security, trust, and institutional maturity.

Key words: financial and economic security, entrepreneurial sector, business, financial risks and threats, digital transformation, challenges and threats, state policy and regulation, instruments for strengthening, financial resources.

Вступ

Сучасні тенденції цифрової трансформації економіки України набули особливої інтенсивності в умовах війни та вимушеної адаптації бізнесу до нової реальності. Масштабне впровадження цифрових платформ, дистанційних та хмарних сервісів, електронної комерції, онлайн-платіжних систем, мобільних фінансових застосунків формує якісно новий формат взаємодії суб'єктів господарювання, держави і споживачів. Оцифрування державних послуг, активне впровадження систем електронного документообігу, цифрова логістика, дистанційні моделі зайнятості зумовлюють перегляд усталених бізнес-процесів. У контексті воєнних ризиків ці тренди не лише забезпечують стійкість функціонування ринку, а й стають ключовими для економічної життєздатності держави, дозволяючи підтримувати комунікації, розрахунки, торгівлю та управління в умовах обмеженого фізичного доступу та руйнування інфраструктури.

Разом із тим цифровізація економіки України породжує нові виклики та загрози для системи фінансово-економічної безпеки підприємництва. Зростання залежності бізнесу від цифрових інструментів та електронних комунікацій підвищує його вразливість до кібератак, несанкціонованого доступу до інформації, фішингових схем, шахрайства та зовнішніх маніпуляцій. Розширення тіньового сегмента електронної економіки, ризики витоку персональних і комерційних даних, висока концентрація критичних сервісів у руках обмеженого кола провайдерів створюють додаткові фінансові та операційні небезпеки. Зміна структури зайнятості, заміщення робочих місць автоматизацією та посилення глобальної конкуренції у цифровому середовищі посилюють загрозу втрати конкурентних переваг суб'єктами малого та середнього бізнесу.

Забезпечення фінансово-економічної безпеки бізнесу в таких умовах потребує адаптації стратегій управління, модернізації захисних механізмів та впровадження інноваційних підходів як на рівні підприємств, так і в системі державної політики. Вітчизняні суб'єкти підприємництва повинні посилити кіберзахист, удосконалити внутрішній контроль, управління цифровими ризиками, інвестувати в кваліфікацію персоналу та захист комерційної інформації. Держава має розвивати сучасні регуляторні

інструменти цифрової безпеки, стимулювати інновації, формувати партнерські платформи держави та бізнесу, а також забезпечити інституційні умови для мінімізації цифрових загроз через стандартизацію, аудит безпеки та сучасну інфраструктуру кіберзахисту.

На етапі повоєнної відбудови перспективи посилення фінансово-економічної безпеки підприємництва тісно пов'язані з цифровою модернізацією економіки, інтеграцією до європейського цифрового ринку та формуванням національної системи стійкості бізнесу. Розвиток інноваційного та високотехнологічного підприємництва, цифрових фінансових сервісів, смарт-логістики, клауд-економіки та штучного інтелекту здатні прискорити відновлення економічної активності. Стратегічне значення матиме формування безпечного цифрового середовища, у якому підприємства зможуть ефективно залучати інвестиції, вести міжнародну торгівлю та конкурувати на глобальних ринках. Урешті, цифрова трансформація може стати фундаментом економічного відновлення, якщо її супроводжуватимуть системні механізми захисту фінансово-економічної безпеки вітчизняного бізнесу.

У працях В. Апалькової [1, с.9–18], С. Веретюка та В. Пілінського [4, с.51–58], О. Гудзя [6, с.4–12] і С. Коляденка [14, с.106–107] розкрито ключові напрями цифрової трансформації економіки та особливості впровадження цифрових технологій у світовій і вітчизняній практиці. Дослідники підкреслюють, що цифровізація бізнес-процесів, розбудова ІКТ і залучення України до європейських цифрових мереж формують передумови для зростання конкурентоспроможності підприємств та адаптації до нових економічних моделей.

Питання фінансово-економічної безпеки розглядаються у роботах Т. Бєлялова та І. Коріня [2], О. Квасової [13, с.70–73], І. Мойсеєнка і О. Марченка [15], Т. Васильціва [3, с.145–149], Ільчука та Садчикова [10, с.209–217], де визначено її зміст, загрози та підходи до підвищення стійкості бізнесу. Автори акцентують на необхідності комплексного управління ризиками, особливо в умовах нестабільності зовнішнього середовища та фінансових обмежень.

Дослідження В. Гловацького [5, с.13–16], В. Наконечного [9, с.10–15], О. Качана [11] і Т. Зубко [7, с.81–88] спрямовані на оцінку інформаційної безпеки підприємств, доводячи її вирішальний вплив на економічну стабільність і функціонування бізнесу в цифровому середовищі. Наголошується, що розвиток цифрової інфраструктури та система кіберзахисту є ключовими елементами забезпечення безпеки.

Науковці Г. Карчева, Д. Огородня і В. Опенько [12] аналізують вплив цифрової економіки на міжнародні та національні ринки, визначаючи нові можливості й ризики для підприємств, а В. Куцик і Р. Лупак [8, с.244–249] підкреслюють трансформацію конкурентних механізмів та необхідність стратегічного управління ризиками у цифровізованому середовищі. Узагальнення літератури демонструє інтеграційний зв'язок цифровізації з модернізацією системи фінансово-економічної безпеки, що передбачає управління ризиками, кіберзахист і вдосконалення технологічної платформи підприємств.

Водночас, сучасні виклики вимагають подальшого удосконалення методологічних та практичних засад зміцнення фінансово-економічної безпеки підприємництва в Україні, що передбачає систематизацію та впровадження якісного зарубіжного досвіду у відповідні механізми. Метою даної статті є ідентифікація Нових викликів та загроз цифрової трансформації економіки для системи фінансово-економічної безпеки підприємництва в Україні.

Результати

Цифрова трансформація економіки в останні роки перетворилася на ключовий чинник конкурентоспроможності національних економічних систем, формування нових

бізнес-моделей та прискорення соціально-економічного розвитку. В Україні ці процеси набули особливої інтенсивності в умовах війни, коли цифрові технології стали не лише інструментом оптимізації операційної діяльності, а й механізмом забезпечення економічної життєздатності держави та бізнесу. Масове поширення цифрової комунікації, онлайн-сервісів, електронного документообігу, цифрових фінансових трансакцій і платформних рішень докорінно змінюють природу економічної взаємодії, відкриваючи доступ до нових ринків та ресурсів, але водночас – створюючи додаткові ризики та залежності.

В умовах військових загроз, руйнування фізичної інфраструктури, релокації підприємств та людського капіталу цифровізація стала основою підтримання безперервності бізнес-процесів і логістичних ланцюгів. Проте активне перенесення критичних сервісів у цифрове середовище формує нові загрози для фінансово-економічної безпеки, пов'язані з кібернападами, шахрайством, несанкціонованим доступом до даних, технологічним шантажем та блокуванням цифрових сервісів. Ускладнення технологічного ландшафту вимагає від підприємств принципово нових підходів до управління ризиками, модернізації систем захисту та підвищення рівня організаційної стійкості.

Зростаюча цифрова залежність бізнесу від зовнішніх технологічних провайдерів, транснаціональних ІТ-корпорацій та глобальних хмарних інфраструктур підвищує вразливість українського підприємництва до зовнішніх маніпуляцій, санкційних обмежень і техногенних ризиків. Одночасно відбувається зміна структури витрат, трансформація зайнятості та необхідність інвестування в цифрові компетенції персоналу, що створює додаткове навантаження на фінансові ресурси підприємств, особливо малого та середнього бізнесу. У таких умовах питання забезпечення фінансово-економічної безпеки виступає стратегічним пріоритетом, який визначає стійкість функціонування бізнесу в короткостроковій перспективі та його конкурентний потенціал у післявоєнний період.

За ситуації, склалася, провідними викликами і загрозами для фінансово-економічної безпеки підприємництва доцільно визначити наведені на рис. 1.

Так, з розвитком цифрових платформ і хмарних сервісів підприємства стають вразливими до кібератак, включно з вірусними, DDoS-атаками та шкідливим ПЗ. Такі загрози можуть призвести до збоїв у роботі систем, порушення логістики, втрати даних та фінансових коштів, а також негативно вплинути на репутацію компанії. Недостатній рівень кіберзахисту може спричинити серйозні фінансові втрати і зниження довіри партнерів та клієнтів.

Іншим актуальним викликом слід вважати витік та компрометацію даних. Цифровізація передбачає накопичення та обробку великих обсягів комерційної та персональної інформації. Незахищені бази даних і слабкі протоколи доступу створюють ризик витоку інформації, що може стати причиною фінансових шахрайств, втрати конкурентних переваг та юридичних санкцій. Для бізнесу це означає зростання витрат на відновлення систем, компенсації клієнтам та репутаційні втрати.

При тому ведемо також мову і про техногенну залежність від зовнішніх провайдерів. Підприємства значною мірою залежать від глобальних хмарних сервісів та програмного забезпечення, контрольованого закордонними компаніями. Це підвищує ризик зовнішнього впливу, включно з блокуванням сервісів, зміною тарифів або санкційними обмеженнями. Негативні наслідки можуть включати перебої в роботі, фінансові збитки та необхідність пошуку альтернативних рішень, що потребує додаткових ресурсів.

Наступний виклик – це фінансові ризики та нестабільність. Зокрема, інвестиції в цифрову інфраструктуру, кіберзахист, автоматизацію процесів і навчання персоналу створюють суттєве навантаження на фінансові ресурси підприємств. Особливо це

стосується малого та середнього бізнесу, де обмежені бюджети можуть призводити до нестачі оборотних коштів. Наслідком є потенційне зниження фінансової стійкості, затримки в реалізації проєктів і зменшення інвестиційної привабливості.

Рис. 1. Виклики і загрози фінансово-економічній безпеці підприємництва в Україні в умовах цифрової трансформації національної економіки
Джерело: авторська розробка.

До наступної категорії викликів і загроз фінансово-економічній безпеці українського бізнесу в умовах цифровізації відносимо тінізацію електронної економіки. Швидке поширення незареєстрованих або напівлегальних цифрових операцій створює ризик втрати прозорості фінансових потоків, ускладнює контроль за податковими та

регуляторними вимогами. Для бізнесу це може призвести до юридичних проблем, штрафів і додаткових витрат на легалізацію діяльності, а також підривати довіру партнерів та інвесторів.

Окрім того, швидкі технологічні зміни та недостатня підготовка персоналу також підривають засади фінансово-економічної безпеки суб'єктів вітчизняного підприємницького сектору. Підприємства змушені швидко адаптуватися до нових цифрових інструментів, платформ і процесів. Недостатня кваліфікація співробітників може призвести до помилок у роботі систем, втрат даних або неефективного використання ресурсів. Наслідком стає зниження продуктивності, додаткові витрати на навчання та підвищення ризику фінансових втрат.

Врешті-решт цілковито закономірно вести мову й про посилення конкуренції та глобальні виклики. Цифровізація відкриває доступ до міжнародних ринків, одночасно підвищуючи конкуренцію. Підприємства, які не встигають впроваджувати сучасні цифрові стратегії, ризикують втратити частку ринку, доходи та конкурентні переваги. Для бізнесу це означає необхідність постійних інвестицій у технології, маркетинг і розвиток цифрових компетенцій для збереження фінансової стабільності.

Цілковито логічно, коли провідні рішення, які будуть напрацьовані та реалізовані в сенсі посилення фінансово-економічної безпеки підприємництва в Україні, будуть стосуватися впровадження інструментарію, який спрямований на послаблення визначених вище викликів та загроз (рис. 2).

У сучасних умовах цифровізації та зростаючих кіберзагроз питання забезпечення стійкості підприємств набуває особливої актуальності. Надзвичайно важливим є впровадження багаторівневих систем інформаційного захисту, які включають комплекс сучасних антивірусних рішень, фаєрволів, систем виявлення вторгнень (IDS/IPS) та інструментів моніторингу активності в мережі. Така інтегрована система дозволяє не лише ідентифікувати потенційні загрози на ранніх етапах, але й запобігати їхньому поширенню всередині корпоративної інфраструктури. Вкрай важливими є регулярне оновлення програмного забезпечення, тестування на вразливості, проведення аудитів безпеки та систематичне навчання персоналу правилам кібергігієни. Ці заходи сприяють мінімізації ризиків виникнення системних збоїв і фінансових втрат, забезпечуючи безперервність бізнес-процесів навіть у складних умовах, зокрема в умовах воєнних дій та інших надзвичайних ситуацій, що негативно впливають на роботу підприємств.

Захист даних і контроль доступу є критично важливими компонентами системи інформаційної безпеки. В умовах високого ризику витоку або компрометації корпоративної та персональної інформації необхідним є впровадження таких інструментів, як шифрування даних на всіх рівнях, політики доступу, які регламентують права користувачів залежно від їх ролі в організації, багатофакторна аутентифікація та регулярне резервне копіювання критичної інформації. Використання сертифікованих хмарних платформ для зберігання та обробки даних, а також побудова систем відновлення інформації після інцидентів дозволяє гарантувати збереження ключових ресурсів і підтримувати фінансово-економічну стабільність підприємства навіть у разі кібератак, техногенних аварій або системних збоїв. Крім того, застосування стандартів інформаційної безпеки, сертифікації систем та регулярний аудит зменшують ймовірність внутрішніх порушень і підвищують довіру партнерів і клієнтів.

Для мінімізації зовнішніх ризиків підприємства все частіше застосовують диверсифікацію постачальників цифрових та технологічних сервісів, укладають контракти з гарантіями безпеки та створюють локальні резервні рішення для критично важливих бізнес-процесів. Такий підхід дозволяє зменшити залежність від окремих провайдерів, уникати блокування сервісів, санкційних обмежень або непередбачуваних перебоїв у роботі, що є особливо важливим у нестабільних економічних умовах.

Диверсифікація постачальників і створення локальних резервів забезпечують більшу гнучкість у реагуванні на зовнішні загрози та підвищують стійкість бізнес-моделі до ризиків, пов'язаних з цифровою інфраструктурою.

Рис. 2. Інструментарій послаблення викликів та загроз фінансово-економічній безпеці підприємництва в Україні в умовах цифрової трансформації економіки

Джерело: авторська розробка.

Фінансове планування і оптимізація витрат у цифровій трансформації мають стратегічне значення для зменшення ризиків і забезпечення стабільності бізнесу. Підприємства формують резервні фонди для реалізації цифрових проєктів, здійснюють поетапне інвестування у розвиток цифрової інфраструктури та кіберзахист, а також активно використовують зовнішні джерела фінансування, такі як гранти, державні

програми або стратегічні інвестиції партнерів. Внутрішній фінансовий контроль дозволяє оцінювати ефективність витрат, оптимізувати ресурсне забезпечення та підтримувати фінансову стабільність у процесі цифрової трансформації. Така комплексна фінансова стратегія сприяє не лише захисту від можливих економічних втрат, а й підвищенню стійкості підприємства до непередбачуваних фінансових ризиків.

Прозорість фінансових операцій і відповідність законодавству виступають ключовими інструментами протидії тінізації електронної економіки та зловживанням у сфері цифрових розрахунків. Для цього використовуються легальні електронні платформи, здійснюється регулярний аудит фінансових потоків, дотримуються податкові та регуляторні вимоги, а також підвищується обізнаність бізнесу щодо правових аспектів цифрової діяльності. Забезпечення прозорості фінансових процесів дозволяє знизити юридичні ризики, уникнути штрафних санкцій, а також підтримувати довіру партнерів, інвесторів і державних органів, що є важливим для стабільного розвитку бізнесу.

Навчання персоналу та впровадження адаптивних систем управління знаннями є невід'ємною складовою підвищення ефективності діяльності підприємств у цифровому середовищі. Регулярні програми навчання, створення систем підтримки користувачів та поетапне впровадження нових технологій із попереднім тестуванням дозволяють мінімізувати людський фактор, зменшити кількість помилок і підвищити продуктивність роботи. Адаптивні системи управління знаннями забезпечують швидке реагування на технологічні зміни та підтримують стабільність бізнес-процесів навіть у динамічних умовах цифровізації.

Впровадження інновацій, стратегічне планування та адаптація до ринку сприяють зміцненню конкурентних переваг підприємств на глобальному рівні. Для цього застосовуються стратегії цифрового розвитку, інвестуються ресурси у створення інноваційних продуктів та послуг, розвиваються цифрові канали збуту, налагоджуються партнерські програми з технологічними компаніями та здійснюється постійний моніторинг ринкових трендів. Такий комплекс заходів дозволяє своєчасно коригувати бізнес-моделі, мінімізувати фінансові втрати, забезпечувати гнучкість підприємства і підтримувати його стабільність та конкурентоспроможність у процесі цифрової трансформації, що є критично важливим для довгострокового розвитку та ефективного функціонування на сучасних ринках.

Висновки

Цифрова трансформація економіки України, посилена викликами воєнного стану, стала ключовим чинником забезпечення стійкості та безперервності функціонування підприємницького середовища. Вона стимулює модернізацію бізнес-процесів, розширює можливості доступу до ринків та інноваційних сервісів, прискорює інтеграцію держави, бізнесу і споживачів у цифровому просторі.

Водночас цифровізація породжує низку нових ризиків і загроз, які безпосередньо впливають на фінансово-економічну безпеку підприємництва. Серед найбільш значущих – зростання кіберзлочинності, витік комерційних даних, тінізація електронних операцій та залежність від зовнішніх цифрових інфраструктур. Це вимагає трансформації системи захисту бізнесу та переорієнтації державної безпекової політики.

Ефективне забезпечення фінансово-економічної безпеки підприємницького сектора потребує впровадження інтегрованих механізмів управління цифровими ризиками, розвитку кіберкультури в бізнесі, удосконалення нормативного регулювання та створення інституційних передумов для безпечного функціонування цифрових сервісів. Спільні дії держави та підприємництва повинні бути спрямовані на підвищення цифрової стійкості та мінімізацію зовнішніх загроз.

Перспективи посилення фінансово-економічної безпеки бізнесу у повоєнний період пов'язані зі створенням комплексного, захищеного та конкурентоспроможного цифрового середовища, інтегрованого до європейського ринку. Цифрова трансформація може стати фундаментом економічного відновлення, проте її успішність визначатиметься здатністю держави та бізнесу забезпечити високий рівень безпеки, довіри та інституційної зрілості цифрової інфраструктури.

Подальші наукові дослідження в даній сфері мають бути спрямовані на стандартизацію публічно-приватної політики щодо забезпечення фінансово-економічної безпеки бізнесу в Україні.

Список використаних джерел

1. Апалькова В. В. Концепція розвитку цифрової економіки в Євросоюзі та перспективи України. Вісник Дніпропетровського університету. Серія «Менеджмент інновацій». 2015. Вип. 4. С. 9–18.
2. Бєлялов Т. Е., Корінь І. В. Фінансово-економічна безпека підприємства та напрями її підвищення. URL: https://chmnu.edu.ua/wp-content/uploads/2019/07/Byelyalov-T.E.-Korin-I.-V..pdf.
3. Васильців Т. Г. Удосконалення державного регулювання підприємницької діяльності в Україні. Стратегічні пріоритети. 2009. № 1 (10). С. 145-149.
4. Веретюк С. М., Пілінський В. В. Визначення пріоритетних напрямків розвитку цифрової економіки в Україні. Наукові записки Українського науково-дослідного інституту зв'язку. 2016. № 2. С. 51–58.
5. Гловацький В. В. Методи оцінювання стану безпеки та загроз інформаційних ресурсів. Зв'язок. 2016. № 5. С. 13–16.
6. Гудзь О. Є. Цифрова економіки: зміна цінностей та орієнтирів в управлінні підприємством. Економіка. Менеджмент. Бізнес. 2018. № 2(24). С. 4–12.
7. Зубко Т. Л. Оцінка рівня економічної безпеки підприємства галузі зв'язку. Економіка. Менеджмент. Бізнес. 2016. Вип. 3. С. 81-88.
8. Куцик В. І., Лупак Р. Л. Моделювання конкурентних позицій підприємств реального сектора економіки на внутрішньому ринку. Бізнес Інформ. 2017. № 12 (479). С. 244-249.
9. Наконечний В. С. Стан розвитку управління інформаційною безпекою в світовій прак-тиці та її вплив на економічний розвиток України. Сучасний захист інформації. 2015. № 4. С. 10–15. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/419/387.
10. Ільчук В., Садчиков В. Шляхи підвищення фінансово-економічної безпеки підприємств аграрного бізнесу. Вісник Чернігівського державного технологічного університету. 2013. № 2(66). С. 209–217.
11. Качан О. І. Інформаційна безпека підприємства в умовах глобалізації. URL: https://conf.ztu.edu.ua/wp-content/uploads/2017/09/234.pdf.
12. Карчева Г. Т., Огородня Д. В., Опенько В. А. Цифрова економіка та її вплив на розвиток національної та міжнародної економіки. URL: http://dspace.ubs.edu.ua/jspui/bitstream/123456789/901/1/Karcheva_Digital_ecoNºmy.pdf.
13. Квасова О. П. Фінансово-економічна безпека як система. Інтернаука. 2016. № 12 (22). С. 70–73.
14. Коляденко С. В. Цифрова економіка: передумови та етапи становлення в Україні і у світі. Економіка. Фінанси. Менеджмент. 2016. № 6. С. 106–107.
15. Мойсеєнко І. П., Марченко О. М. Управління фінансово-економічною безпекою підприємства. Львів, 2011. 380 с.