



Фінанси, банківська справа, страхування та фондовий ринок

УДК 338.24:005.334:004.738.5 (477.75/.79)

DOI <https://doi.org/10.5281/zenodo.15654180>

**Фінансова безпека підприємств Причорноморського регіону в умовах
цифровізації та викликів воєнного часу**

Гуріна Олена Валентинівна

Доктор економічних наук, професор, професор кафедри
інтелектуальної цифрової економіки, Національний університет
кораблебудування ім. адмірала Макарова, м. Миколаїв, Україна,
gurina161277@gmail.com, ORCID <https://orcid.org/0000-0002-6315-6067>

Домбровська Людмила Вікторівна

Кандидат економічних наук, доцент, керівник департаменту освітньої
діяльності, Миколаївський інститут розвитку людини Університету
«Україна», м. Миколаїв, Україна,
dik43@ukr.net, ORCID: <https://orcid.org/0000-0001-5089-950X>

Прийнято: 16.05.2025 | Опубліковано: 29.05.2025

***Анотація.** У статті досліджено проблеми забезпечення фінансової безпеки підприємств Причорноморського регіону України в умовах цифровізації та загроз, пов'язаних із близькістю до зони бойових дій. Обґрунтовано актуальність інтегрованого підходу до управління фінансовими ризиками, зумовленими як військовими загрозами, так і зростаючими кіберризиками. Запропоновано математичну модель оцінки рівня фінансової безпеки підприємств із урахуванням впливу військових, кібернетичних та економічних ризиків. У моделі інтегровано такі ключові*



фактори, як рівень цифровізації підприємства, витрати на забезпечення безпеки, а також показники внутрішніх і зовнішніх загроз.

Мета дослідження полягає у розробці науково обґрунтованих підходів до підвищення рівня фінансової безпеки підприємств Причорноморського регіону шляхом оптимізації витрат на цифрові технології та заходи кібербезпеки в умовах військових загроз.

Методи дослідження ґрунтуються на комплексному використанні математичного моделювання, аналізу ризиків і оптимізаційних методів для оцінки впливу окремих чинників на фінансову безпеку. Для розрахунку вагових коефіцієнтів застосовано метод експертних оцінок, метод аналізу варіацій та метод парних порівнянь. Рівень цифровізації та фінансових ризиків підприємств оцінено на основі інтегральних показників, які поєднують кількісні та якісні характеристики.

Результати дослідження демонструють, що підприємства Причорноморського регіону найбільше потерпають від військових ризиків, які негативно впливають на їхню фінансову стійкість.

Фінансова безпека підприємства включає захист його фінансово-господарської діяльності від внутрішніх і зовнішніх загроз, що забезпечує стійкий розвиток і конкурентоспроможність. У контексті цифровізації фінансова безпека включає такі аспекти, як: захист фінансових активів від кіберзагроз і шахрайства; управління фінансовими ризиками, що забезпечується через зміни в цифровому середовищі; оптимізація витрат на забезпечення інформаційної безпеки.

Цифровізація має неоднозначний вплив на фінансову безпеку. З одного боку, вона сприяє автоматизації фінансових процесів, підвищенню їх ефективності та прозорості, що зменшує можливості для шахрайства та корупції. З іншого боку, цифрові технології створюють нові ризики, зокрема кіберзагрози, витоки даних та фінансові шахрайства, що вимагає впровадження надійних механізмів захисту.



Розроблена модель дозволила оптимізувати розподіл бюджету між заходами з фізичної та кібербезпеки. Встановлено, що інвестування 60% бюджету в заходи фізичної безпеки й 40% у цифрову трансформацію підприємств забезпечує найвищий рівень фінансової стійкості. Це дозволяє знизити військові ризики на 30% і кіберризики на 20%, що сприяє стабілізації діяльності підприємств у кризових умовах.

***Висновки** підтверджують, що підвищення фінансової безпеки підприємств Причорноморського регіону можливе за рахунок збалансованого розподілу інвестицій у фізичну та кібербезпеку. Розроблена математична модель є ефективним інструментом для ухвалення стратегічних рішень у сфері управління ризиками. Практичне застосування запропонованої моделі сприятиме мінімізації потенційних фінансових втрат і забезпечить стабільний розвиток підприємств навіть в умовах високих зовнішніх загроз. Рекомендовано підприємствам регіону адаптувати стратегії фінансової безпеки відповідно до змін у зовнішньому середовищі та нарощувати інвестиції в цифрові технології як фактор довгострокової стійкості.*

***Ключові слова:** фінансова безпека, цифровізація, управління ризиками, інвестиції, цифрові технології, кібербезпека, військові ризики.*

Financial Security of Enterprises in the Black Sea Region Under Digitalization and Wartime Challenges

Olena Hurina

Doctor of Economic Sciences, Professor, Professor of the Department of Intelligent Digital Economy, Admiral Makarov National University of Shipbuilding,
Mykolaiv, Ukraine, gurina161277@gmail.com,
ORCID <https://orcid.org/0000-0002-6315-6067>



Liydmyla Dombrovska

PhD in Economics, Associate Professor, Head of the Department of Education,
Mykolaiv Institute of Human Development of University «Ukraine»,

Mykolaiv, Ukraine, dik43@ukr.net,

ORCID: <https://orcid.org/0000-0001-5089-950X>

Abstract. *The article explores the challenges of ensuring the financial security of enterprises in Ukraine's Black Sea region under the conditions of digitalization and threats related to the proximity to a war zone. The relevance of an integrated approach to managing financial risks caused by both military threats and increasing cyber risks is substantiated. A mathematical model for assessing the financial security level of enterprises is proposed, considering the impact of military, cyber, and economic risks. The model integrates key factors such as the level of enterprise digitalization, security expenditures, and indicators of internal and external threats.*

The purpose of the study is to develop scientifically grounded approaches to enhancing the financial security of enterprises in the Black Sea region by optimizing expenditures on digital technologies and cyber security measures in the context of military threats.

The research methodology is based on the comprehensive use of mathematical modeling, risk analysis, and optimization methods to assess the impact of various factors on financial security. The method of expert evaluations, variance analysis, and pair wise comparison method were used to calculate weight coefficients. The level of enterprise digitalization and financial risks was assessed using integral indicators that combine quantitative and qualitative characteristics.

The research results demonstrate that enterprises in the Black Sea region suffer the most from military risks, which negatively impact their financial stability.

Financial security includes protecting the enterprise's financial and economic activities from internal and external threats, ensuring sustainable development and competitiveness. In the context of digitalization, financial security encompasses the following aspects: protection of financial assets from cyber threats and fraud;



financial risk management through changes in the digital environment; optimization of expenditures on information security measures.

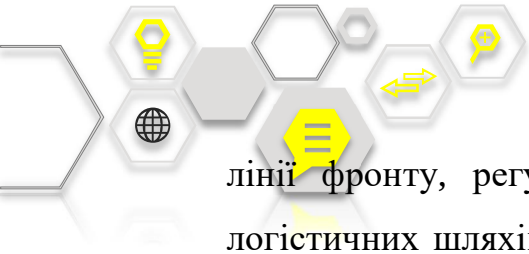
Digitalization has a dual impact on financial security. On the one hand, it facilitates the automation of financial processes, improving their efficiency and transparency, thereby reducing opportunities for fraud and corruption. On the other hand, digital technologies introduce new risks, including cyber threats, data breaches, and financial fraud, necessitating the implementation of reliable security mechanisms.

The developed model allowed for optimizing the budget allocation between physical security and cyber security measures. It was established that investing 60% of the budget in physical security measures and 40% in digital transformation ensures the highest level of financial stability. This approach reduces military risks by 30% and cyber risks by 20%, contributing to the stabilization of enterprises under crisis conditions.

The conclusions confirm that improving the financial security of enterprises in the Black Sea region is possible through a balanced allocation of investments in physical and cyber security. The developed mathematical model serves as an effective tool for strategic decision-making in risk management. The practical application of the proposed model will help minimize potential financial losses and ensure the stable development of enterprises even under high external threats. It is recommended that regional enterprises adapt their financial security strategies in response to external environmental changes and increase investments in digital technologies as a factor of long-term resilience.

Keywords: *financial security, digitalization, risk management, investments, digital technologies, cyber security, military risks.*

Постановка проблеми. Сучасний розвиток економіки України відбувається в умовах масштабних військових дій та швидкої цифрової трансформації. Особливо складною є ситуація в Причорноморському регіоні, який включає Одеську, Миколаївську та Херсонську області. Близькість до



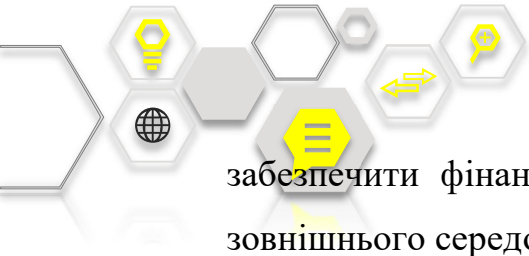
лінії фронту, регулярні атаки на критичну інфраструктуру, блокування логістичних шляхів та дестабілізація бізнес-середовища значно підвищують рівень фінансових ризиків для бізнесу у цьому регіоні.

Підприємства змушені функціонувати в умовах високої невизначеності та нестабільності. Воєнні ризики, що включають пошкодження матеріальних активів, перебої в роботі логістичних ланцюгів, обмеження на експортно-імпортні операції та загальне падіння попиту на продукцію, безпосередньо впливають на фінансову стійкість підприємств. До цього додаються посилені кіберзагрози, спрямовані на дестабілізацію роботи підприємств через втручання в інформаційні системи, викрадення конфіденційної інформації та блокування фінансових операцій.

Цифровізація, яка розглядається багатьма науковцями як інструмент підвищення ефективності та конкурентоспроможності підприємств, у таких умовах стає фактором із неоднозначним впливом: з одного боку, цифрові технології дозволяють автоматизувати бізнес-процеси, підвищувати швидкість прийняття управлінських рішень й знижувати операційні витрати; з іншого боку, – недосконала система кіберзахисту та обмежені фінансові ресурси можуть зробити підприємство більш вразливим до кіберзагроз [1].

Вважаємо, що існуючі підходи до управління фінансовою безпекою підприємств в умовах мирного часу виявляються недостатньо ефективними в умовах війни та високих зовнішніх ризиків. Традиційні методи фінансового планування та управління ризиками не враховують специфіку воєнних загроз і кібератак, що робить їх недостатніми для забезпечення стабільності функціонування підприємств, зокрема, Причорноморського регіону.

Таким чином, виникає необхідність у розробці комплексних моделей оцінки фінансової безпеки підприємств, які б інтегрували військові, економічні та кіберризики, а також дозволяли б оптимізувати розподіл фінансових ресурсів на заходи фізичної безпеки, цифровізації та кіберзахисту. Це дозволить підприємствам не лише вижити в умовах невизначеності, а й



забезпечити фінансову стійкість та адаптивність до швидкозмінних умов зовнішнього середовища.

Аналіз останніх досліджень і публікацій. Сучасні дослідження у сфері забезпечення фінансової безпеки підприємства в умовах цифровізації сфокусовані на вивченні впливу зовнішніх та внутрішніх загроз на фінансову стійкість підприємства, розробку методичних підходів до оцінки рівня фінансової безпеки та формуванню стратегій її забезпечення.

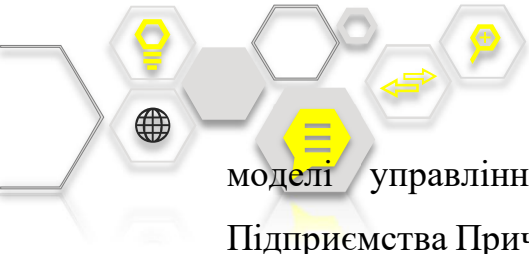
Особливості теорії та практики забезпечення фінансової безпеки розкриті у наукових працях Г. Азаренкової [2], О. Барановського [3], М. Бердар [4], М. Білик [5], І. Бланка [6], З. Варналія [7], В. Гейця [8], О. Гетманця [9], Н. Кондратенко [10], А. Польової [11], Л. Яструбецької [1] та інших.

Вплив цифровізації та глобалізації на рівень фінансової безпеки підприємств, а також виклики, пов'язані з повномасштабним вторгненням РФ на територію України висвітлені у дослідженнях Е. Дмитренко [12], В. Кузьомка [11], А. Мехеда [13], О. Михайлюк [14], О. Назаркіної Л. [15], Л. Петренко [16] та інших.

Разом із тим, чимала кількість питань щодо забезпечення фінансової безпеки в умовах цифровізації, зокрема, під впливом викликів воєнного часу, залишається надзвичайно актуальною та потребує систематичного поглибленого дослідження.

Виділення невирішених раніше частин загальної проблеми. Попри значну кількість досліджень, присвячених фінансовій безпеці підприємств в умовах цифровізації та економічної нестабільності, існує низка аспектів, які залишаються недостатньо вивченими, особливо в контексті діяльності підприємств Причорноморського регіону України. Враховуючи стратегічне значення цього регіону для економіки України, необхідно окреслити невирішені питання, які потребують подальших наукових досліджень.

1. Інтеграція військових ризиків у систему управління фінансовою безпекою. Більшість наукових досліджень зосереджуються на фінансових, економічних і кіберризиках, однак питання інтеграції військових загроз у

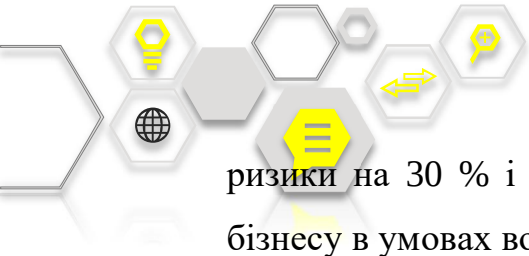


моделі управління фінансовою безпекою залишаються поза увагою. Підприємства Причорноморського регіону стикаються із реальними загрозами фізичної безпеки активів, персоналу та інфраструктури, що безпосередньо впливає на їхню фінансову стійкість. На нашу думку, невирішеним залишається питання розробки адаптивних фінансових стратегій із урахуванням специфіки військових ризиків.

2. Відсутність комплексної оцінки впливу цифровізації на фінансову безпеку. Хоча цифровізація розглядається як інструмент підвищення ефективності підприємств, її вплив на рівень фінансової безпеки в умовах війни практично не досліджений. Існує потреба у створенні моделей, які дозволяють комплексно оцінити як позитивний, так і негативний вплив цифрових технологій на фінансову стійкість підприємств. Питання, які потребують вирішення стосуються запровадження інструментів для оцінки фінансових ризиків, пов'язаних із розвитком цифрових технологій.

3. Низький рівень впровадження систем управління ризиками (ERM). Багато підприємств регіону не використовують інтегровані системи Enterprise Risk Management (ERM) для ідентифікації та мінімізації ризиків. В умовах війни це призводить до відсутності координації в управлінні ризиками, що загрожує фінансовій стабільності. Отже, потребують доопрацювання питання розробки моделей впровадження ERM для підприємств із урахуванням специфіки регіону.

Отже, пропонуємо окреслені вище актуальні питання вирішити шляхом моделювання за допомогою інтегрованої економіко-математичної моделі. Запропонована модель поєднує вплив військових, кібернетичних та класичних економічних ризиків із показниками цифрової зрілості підприємств Причорноморського регіону. Базова економіко-математична модель забезпечення рівня фінансової безпеки не лише кількісно оцінює сукупний рівень небезпеки, а й оптимізує пропорції інвестицій між фізичною безпекою й цифровими технологіями, доводячи на емпіричних даних понад десяти реальних компаній, що співвідношення 60 %/40 % дозволяє знизити військові



ризиків на 30 % і кіберризиків на 20 %, тим самим забезпечуючи стійкість бізнесу в умовах воєнних дій і цифровізації.

Метою дослідження є розробка науково обґрунтованих підходів і практичних рекомендацій щодо підвищення фінансової безпеки підприємств Причорноморського регіону України в умовах цифровізації та зростаючих воєнних загроз. Це передбачає інтеграцію інструментів управління фінансовими ризиками, оптимізацію витрат на заходи фізичної безпеки та кібербезпеки, а також впровадження цифрових технологій для забезпечення стійкості та ефективності діяльності підприємств.

Виклад основного матеріалу дослідження. Проблематика фінансової безпеки підприємств України, особливо в умовах цифровізації та воєнних загроз, є актуальною темою наукових досліджень. Українські вчені приділяють значну увагу вивченню впливу зовнішніх та внутрішніх загроз на фінансову стійкість підприємств, розробці методичних підходів до оцінки рівня фінансової безпеки та формуванню стратегій її забезпечення [2, 7, 10].

Фінансова безпека підприємства – це надійний стан його фінансово-господарської діяльності, який забезпечує стійке функціонування та конкурентоспроможність шляхом захисту від внутрішніх і зовнішніх загроз [13].

Як зазначає З. Варналій, у сучасних умовах цифрової трансформації фінансова безпека охоплює такі ключові напрями: захист фінансових ресурсів від кіберзагроз, шахрайських схем та інформаційних атак; ефективне управління фінансовими ризиками, що зумовлені цифровими трансформаціями та змінами в інформаційному середовищі; раціональне використання ресурсів для впровадження та підтримки заходів інформаційної безпеки [7].

В. Кузьомко та А. Польова проаналізували вплив цифровізації та глобалізації на рівень фінансової безпеки компаній, а також виклики, пов'язані з повномасштабним вторгненням РФ в Україну. Для різних масштабів і видів бізнесу автори запропонували три організаційні моделі забезпечення



фінансової безпеки: централізований підрозділ, матрична структура (інтеграція функції безпеки у ключові департаменти), субконтракт (залучення зовнішніх провайдерів) [11].

Е. Дмитренко та Ю. Дмитренко у своїй статті аналізують особливості функціонування фінансової системи України в умовах воєнного стану та повоєнного періоду. Автори зазначають, що зміст та сутність фінансової системи, як і правове регулювання фінансових відносин, за таких умов істотно змінюються. Розглянуто виклики та загрози, які впливають на стан фінансової системи, та обґрунтовано необхідність збалансування доходів і видатків державного бюджету України у воєнний та повоєнний періоди [12].

Л. Петренко досліджує та класифікує найбільш вагомі зовнішні та внутрішні загрози фінансової безпеки підприємства. У роботі на базі синтезу методів нечіткої логіки та нейронних мереж розроблено багаторівневу ієрархічну систему аналізу та оцінювання рівня впливу загроз на фінансову безпеку підприємства. Це дозволяє більш точно ідентифікувати та оцінити ризики, що стоять перед підприємствами в сучасних умовах [16].

Л. Назаркіна та О. Соколовська у своїй роботі акцентують увагу на специфіці фінансової безпеки в банківській сфері. Автори підкреслюють, що одним із гострих питань функціонування банківської сфери є проблеми фінансової безпеки, особливо в умовах нестабільності та зовнішніх загроз. Розглянуто основні фактори, що впливають на фінансову безпеку банків, та запропоновано шляхи її підвищення [15].

Таким чином, аналіз останніх досліджень свідчить про значну увагу науковців до питань фінансової безпеки підприємств в умовах цифровізації та воєнних загроз. Однак, специфічні аспекти забезпечення фінансової безпеки підприємств Причорноморського регіону, з урахуванням їхньої близькості до лінії фронту та особливостей регіональної економіки, потребують подальшого дослідження та розробки адаптованих методичних підходів.



Забезпечення фінансової безпеки підприємства в умовах цифровізації потребує комплексного підходу, що передбачає баланс між впровадженням інновацій і заходами захисту від нових загроз.

Вважаємо, що вирішенню зазначених питань сприятиме інтегрована економіко-математична модель, яка дозволить: оцінювати рівень фінансових ризиків у процесі цифровізації; оптимізувати розподіл бюджету на заходи з фінансової безпеки; прогнозувати вплив цифрових технологій на фінансову стабільність підприємства.

Для практичної реалізації моделі фінансової безпеки підприємства розглянемо взаємозв'язок трьох ключових факторів:

1. Рівень цифровізації підприємства, $D(t)$;
2. Фінансові ризики, $R(t)$;
3. Витрати на безпеку, $C(t)$.

Базова економіко-математична модель забезпечення рівня фінансової безпеки у часі має вигляд:

$$\frac{\Delta F(t)}{\Delta t} = -\alpha R(t) + \beta D(t) - \gamma C(t) \quad \text{з умовами обмеження} \quad \text{та цільовою функцією:}$$
$$\text{бюджету: } C(t) \leq M \quad \max F(t),$$

де, $F(t)$ – рівень фінансової безпеки у часі;

$R(t)$ – рівень фінансових ризиків (кіберзагрози, шахрайство);

$D(t)$ – рівень цифровізації (автоматизація, ІТ-інфраструктура);

$C(t)$ – витрати на забезпечення фінансової безпеки;

α, β, γ – вагові коефіцієнти впливу ($\alpha, \beta, \gamma > 0$).

Знак « $-$ » перед ваговим коефіцієнтом α відображає політику керівництва підприємства щодо зниження сукупного ризику $R(t)$. Сила вагового коефіцієнту β забезпечується за рахунок знаку « $+$ ». Рівень цифрової зрілості $D(t)$ (автоматизація, аналітика, віддалене керування) додає цінності: високий показник при тому ж ризику й витратах підвищує $F(t)$. Прагнення мінімізувати витрати за незмінного рівня захисту й пошук найефективнішої комбінації заходів обґрунтовує знак « $-$ » перед ваговим коефіцієнтом γ . Кожна додаткова



гривня у складі витрат буде зменшувати рівень фінансової безпеки, стимулюючи шукати найефективніші варіанти витрат у безпеку.

Підприємства, які працюють в зоні бойових дій, або у прифронтових районах будуть мати вищий коефіцієнт α , ставка на технологічне домінування підвищує β і таким чином баланс ризику й розвитку перетворюється на чіткий фінансовий показник.

Додаткове обмеження у моделі $C(t) \leq M$ лімітує бюджет до «стелі», нівелюючи витрати на безпеку і стримуючи «спалення грошей» через постійне збільшення витрат.

Рівень фінансових ризиків підприємства, $R(t)$ визначається інтегральним показником, який відображає ймовірність виникнення фінансових збитків через внутрішні або зовнішні загрози. Оцінка фінансових ризиків дозволяє визначити вразливі місця підприємства та розробити заходи щодо їх мінімізації.

До найпоширеніших типів фінансових ризиків, на нашу думку, варто віднести:

1. Кредитний ризик: прострочення платежів за кредитами, невиконання зобов'язань контрагентами.
2. Ризик ліквідності: недостатність обігових коштів для покриття поточних зобов'язань та зниження ліквідності активів.
3. Валютний ризик: коливання валютних курсів, що впливають на доходи/витрати.
4. Інвестиційний ризик: невизначеність прибутковості інвестиційних проєктів та ризику невдалих капіталовкладень.
5. Операційний ризик: внутрішні помилки в управлінні фінансами, несанкціонований доступ до фінансових даних.
6. Податковий ризик: зміни у податковому законодавстві, можливі штрафи за податкові порушення та невиконання податкових зобов'язань.

Рівень фінансових ризиків розраховується за інтегральною формулою:



$$R(t) = \sum_{i=1}^n w_i \cdot r_i$$

$R(t)$ – рівень фінансових ризиків підприємства (від 0 до 1);

r_i – рівень окремого виду ризику (від 0 до 1);

w_i – вага i -го компонента в загальній оцінці ($\sum_{i=1}^n w_i = 1$);

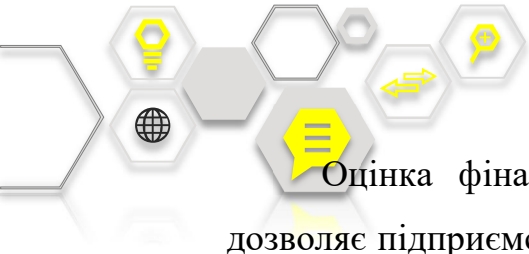
n – кількість видів фінансових ризиків.

Кількісна оцінка фінансових ризиків передбачає використання:

1. Інструментів аналізу фінансових коефіцієнтів: коефіцієнту поточної ліквідності, фінансової незалежності та рентабельності активів.
2. Методу сценарного аналізу: оцінка наслідків змін ринкових умов (кризи, інфляції).
3. Методу експертних оцінок: опитування фінансових експертів щодо можливих загроз.
4. Методу VaR (Value at Risk): кількісна оцінка можливих фінансових збитків із заданою ймовірністю.

Ваговий коефіцієнт (w_i) показує відносну важливість кожного фактора (ризик у чи показника) у загальній оцінці фінансового стану підприємства. Коректний розрахунок ваг дозволяє об'єктивно оцінити вплив різних факторів на фінансову безпеку.

До методів визначення вагових коефіцієнтів відносять: метод експертних оцінок (використовується для якісних показників; опитуються експерти (фінансисти, аудитори), які оцінюють важливість кожного фактора за шкалою), метод аналізу варіацій, дисперсійний аналіз (використовується для кількісних фінансових показників; визначається вплив кожного фактора на загальний результат через дисперсію), метод аналізу головних компонент, РСА (для кількісних фінансових показників використовується статистичний аналіз для визначення найвпливовіших факторів через зменшення розмірності даних), парне порівняння, метод Сааті (для оцінки якісних показників експерти порівнюють кожну пару факторів і визначають їх відносну важливість за відповідною шкалою) [8].



Оцінка фінансових ризиків із застосуванням приведеної методики дозволяє підприємству визначити пріоритетні напрями управління ризиками, оптимізувати витрати на страхування і захист активів та підвищити фінансову стійкість і конкурентоспроможність.

Рівень цифровізації підприємства $D(t)$ – це інтегральний показник, який відображає ступінь впровадження цифрових технологій у бізнес-процеси підприємства, оцінюється за кількісними та якісними критеріями.

Оцінка здійснюється за кількома напрямками:

1. Інфраструктурна цифровізація: наявність сучасної IT-інфраструктури (сервери, мережі, хмарні рішення) та впровадження систем автоматизації бізнес-процесів (ERP, CRM, SCM).

2. Цифрові технології управління: використання аналітики великих даних (Big Data); впровадження штучного інтелекту (AI), машинного навчання; інтеграція інтернету речей (IoT).

3. Цифрова безпека: системи кіберзахисту, антивірусні програми; використання багаторівневої аутентифікації; резервне копіювання даних.

4. Цифрові канали комунікації: онлайн-платформи для продажу товарів/послуг; соціальні мережі та інструменти цифрового маркетингу та системи електронного документообігу.

Розрахунок проводиться за допомогою інтегрального показника, що об'єднує всі компоненти:

$$D(t) = \sum_{i=1}^n w_i \cdot d_i$$

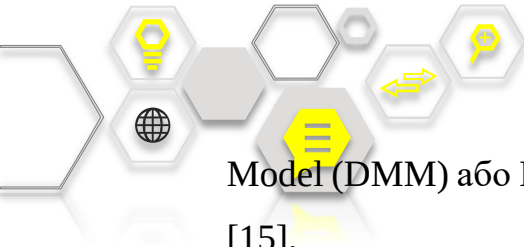
де, $D(t)$ – рівень цифровізації підприємства (від 0 до 1);

d_i – рівень впровадження i -го компонента цифровізації (від 0 до 1);

w_i – вага i -го компонента в загальній оцінці ($\sum_{i=1}^n w_i = 1$);

n – кількість компонентів.

Розрахунок рівня цифровізації може бути виконаний з використанням інструментів оцінки за міжнародними стандартами: ISO 27001 (IT-безпека), ISO 9001 (управління якістю), методики цифрової зрілості: Digital Maturity



Model (DMM) або Industry 4.0 Assessment та SWOT-аналізу цифрових процесів [15].

Визначення поточного рівня цифровізації дозволяє ідентифікувати слабкі місця в цифровій інфраструктурі, оптимізувати інвестиції в цифрові рішення та підвищити фінансову безпеку підприємства.

Витрати на заходи з кібербезпеки $C(t)$ є критично важливою складовою фінансової стратегії підприємства, особливо в умовах зростаючих кіберзагроз і цифровізації бізнес-процесів. Ці витрати мають забезпечити захист інформаційних ресурсів, мінімізувати ризики втрати даних і фінансових збитків, а також підтримувати стабільну роботу підприємства.

Оцінка витрат на кібербезпеку охоплює декілька ключових напрямів:

1. Технічне забезпечення: закупівля серверів, мережевого обладнання, фаєрволів, антивірусних систем та впровадження спеціалізованого програмного забезпечення для захисту даних (SIEM-системи, VPN, системи багатофакторної автентифікації).

2. Інформаційна безпека: захист конфіденційних даних, резервне копіювання та шифрування даних, управління доступом до інформації.

3. Організаційні заходи: розробка політики інформаційної безпеки, навчання та сертифікація персоналу з питань кібербезпеки.

4. Аудит і моніторинг: проведення аудитів інформаційної безпеки та постійний моніторинг систем, виявлення вразливостей.

5. Страхування кіберризиків: оформлення полісів кіберстрахування для покриття збитків у разі атак.

Витрати на кібербезпеку можуть бути визначені за різними методами. Вибір методу залежить від компанії, її підходів до оцінки кіберризиків, бажаного рівня захисту (рівня сприйняття ризиків), бюджету та очікуваних результатів.

Метод відсотка від ІТ-бюджету/доходу: фіксований відсоток від загального доходу (або ІТ-бюджету) на заходи з кібербезпеки (зазвичай 2–10%/7–14%). Метод Cost-of-Breach Back-solving: обирається середня вартість



інциденту і моделюється «скільки потенційно врятується, якщо знизити ймовірність на $X\%$ ». Метод «Бенчмарк + коригування КРІ»: дані опитувань по галузі (за умови доступу до галузевих звітів) коригуються на власні КРІ (кількість користувачів, філій) [1].

Реалізація моделі фінансової безпеки підприємства починається з оцифрування ключових ризиків (воєнних, операційних, кібернетичних, ринкових) і рівня цифрової зрілості, після чого ці показники зважуються у інтегральній формулі. Далі визначається бюджет безпеки та перелік конкретних заходів – від укриття виробничих потужностей до впровадження SOC або AI-моніторингу. За допомогою лінійного чи сценарного оптимізатора добирається така комбінація інвестицій, що максимально підвищує рівень фінансової безпеки за заданого бюджету, а отримані рішення вбудовуються у річний капітальний та операційний план підприємства із поквартальним моніторингом ризик-метрик і корекційною петлею для наступного циклу.

У табл. 1 представлені результати проведеного дослідження на прикладах діючих підприємств Причорноморського регіону. Рівень фінансової безпеки $F(t)$ змодельований до та після інвестування у відповідні напрями.

За підсумками моделювання спостерігається певна тенденція: переважна більшість підприємств Причорноморського регіону після впровадження заходів демонструє підвищення інтегрального показника фінансової безпеки $F(t)$. Це зростання формується насамперед за рахунок помірного зниження інтегрального ризику $R(t)$ (у середньому на 2–5 в. п.) і невеликого, але сталого приросту цифрової зрілості $D(t)$ (+0,02–0,04). Навіть у випадках, коли витрати на захист $C(t)$ збільшуються, негативний вплив додаткових витрат нівелюється завдяки невеликому значенню коефіцієнта γ та вищим вагам, що менеджмент надає мінімізації ризиків (α) й розвитку цифрових можливостей (β).

Таблиця 1

**Результати моделювання рівня фінансової безпеки підприємств
Причорноморського регіону**

Підприємства	$R(t)$		$D(t)$		$C(t)$		α	β	γ	$F(t)$	
	до	після	до	після	до	після				до	після
Миколаївська область											
ТОВ «Баядера»	0,38	0,32	0,58	0,61	0,01	0,02	0,5	0,4	0,1	0,041	0,082
ГК «Прометей»	0,22	0,2	0,65	0,66	0,001	0,001	0,6	0,3	0,1	0,0629	0,0779
ГК «Агроф'южн»	0,13	0,13	0,72	0,73	0,25	0,22	0,55	0,4	0,05	0,2040	0,2095
ТОВ «Експорт трейд груп»	0,19	0,15	0,8	0,81	1,15	1,06	0,55	0,35	0,1	0,098	0,095
ТОВ «Полетехніка»	0,16	0,12	0,55	0,52	0,25	0,3	0,6	0,32	0,08	0,06	0,0704
ТОВ «Простір»	0,44	0,42	0,55	0,5	0,002	0,002	0,45	0,45	0,1	0,0493	0,0358
Завод «Адісем»	0,36	0,28	0,6	0,62	0,8	0,9	0,5	0,4	0,1	0,052	0,046
ТОВ «АСТРА НОРД ВЕСТ»	0,45	0,44	0,65	0,6	0,19	0,2	0,5	0,4	0,1	0,016	0,08
Одеська область											
ТОВ Ламан Шіппінг	0,47	0,43	0,66	0,65	0,23	0,25	0,5	0,4	0,1	0,006	0,02
ГК Автогруп	0,22	0,2	0,6	0,67	0,15	0,25	0,55	0,3	0,15	0,0365	0,0675
ТОВ «ЮГФУД»	0,18	0,16	0,6	0,62	0,12	0,12	0,6	0,3	0,1	0,06	0,078
ТОВ «Текстрейд ЛТД»	0,15	0,15	0,55	0,58	0,02	0,02	0,45	0,45	0,1	0,178	0,1915
ПП «Альфа Люкс»	0,2	0,2	0,44	0,45	0,05	0,05	0,35	0,55	0,1	0,167	0,1725
ТОВ Смарт авто ЛТД	0,25	0,25	0,38	0,42	0,1	0,15	0,35	0,5	0,15	0,0875	0,1
ТОВ «Агро-трейд сервіс»	0,11	0,12	0,5	0,52	0,1	0,05	0,55	0,3	0,15	0,0745	0,0825
Херсонська область											
ТОВ «Рітейл Захід-Південь»	0,18	0,16	0,44	0,46	0,05	0,05	0,65	0,30	0,05	0,0125	0,0315
ТОВ ЛДК	0,2	0,19	0,47	0,5	0,03	0,03	0,6	0,35	0,05	0,093	0,0595

Таким чином, помірні інвестиції у безпекові й цифрові проекти забезпечують відчутний приріст фінансової стійкості, а модель дозволяє гнучко балансувати між зменшенням ризиків та зростанням цифрового потенціалу без істотного перевищення запланованого бюджету.

Список використаних джерел

1. Яструбецька Л. С. Фінансова безпека суб'єктів підприємництва в Україні в умовах гібридних загроз: монографія, Львів : ЛНУ імені Івана Франка, 2022. 320 с.
2. Azarenkova G., Golovko O., Oryekhova K., Salenko O. & Maiboroda A. Estimating and forecasting of financial security of enterprises. *Financial and Credit Activity Problems of Theory and Practice*. 2021. Vol. 1(32), P. 224–230. DOI:[10.18371/fcaptp.v1i32.200383](https://doi.org/10.18371/fcaptp.v1i32.200383)



3. Барановський О. І. Фінансова безпека: теорія і практика : монографія. К. : Знання, 2004. 280 с.
4. Бердар М. К. Забезпечення фінансової безпеки суб'єктів підприємництва. *Вісник Київського національного університету ім. Т. Шевченка. Економіка*. 2015. № 124/125. С. 73–76
5. Білик М. Д. Роль стабільної діяльності підприємств у їх фінансовій безпеці. *Формування ринкових відносин в Україні*, 2008, № 4 (83), с. 129–133
6. Бланк І. О. Фінансовий менеджмент: підручник : у 2 т. 5-те вид., переробл. і доп. Київ : Ніка-Центр, 2011. Т. 2. с. 665–708
7. Варналій З. С., Катамадзе Г. Ш. Фінансова безпека суб'єктів підприємництва в умовах війни та повоєнного відновлення (науково-експертна та соціологічна оцінка): монографія / відп. ред. З. С. Варналій, Київ : КМ-Букс, 2023. 240 с.
8. Геєць В. М., Кузьмін Е. В., Даньків Б. Я. Фінансова безпека України. Київ : Наукова думка, 2006. 376 с.
9. Гетманець О. П. Фінансова безпека як об'єкт правового регулювання». *Підприємництво, господарство і право*. 2020. № 3. С. 218–223
10. Kondratenko N., Doroshenko H., Ternova I., Babych S. & Dorosheko O. Organizational and methodical provision of the financial and economic security management of the enterprise. *Financial and Credit Activity Problems of Theory and Practice*. 2021. Vol. 1(32), 129–137. DOI: 10.18371/fcaptp.v1i32.200301
11. Кузьомко В. М., Польова А. В. Економічна сутність та проблеми фінансової безпеки українських підприємств. *Економіка та підприємництво: зб. наук. пр. Київ. нац. екон. ун-т ім. Вадима Гетьмана*. Київ : КНЕУ, 2023. Вип. 51. С. 5–15. URI: <https://ir.kneu.edu.ua/handle/2010/42805>
12. Дмитренко Е. С., Дмитренко Ю. П. Особливості фінансового, правового та організаційного забезпечення соціального захисту громадян в умовах євроінтеграції України. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2022. № 3(44). С. 234–242. URL: http://nbuv.gov.ua/UJRN/Fkd_2022_3_26



13. Мехед А. М., Варналій З. С. Фінансова безпека підприємств в умовах цифрової економіки. *Вісник університету банківської справи*. 2021. № 3 (42). С. 55–61. URL: <https://ser.net.ua/index.php/SER/article/view/440>

14. Dokiienko L., Hrynyuk N., Nakonechna O., & Mykhailyk O. System for evaluation of financial security of operational activity of oil-and-fat industry enterprises. *Agricultural and Resource Economics: International Scientific E-Journal*. 2021. Vol. 7(4), 138–159. DOI: [10.51599/are.2021.07.04.08](https://doi.org/10.51599/are.2021.07.04.08)

15. Назаркіна Л. І., Соколовська О. І. Цифрові індикатори діагностики фінансової безпеки промислових підприємств. *Економіка: реалії часу*, 2022, № 2, с. 54–62

16. Петренко Л. М. Моделювання процесу управління загрозами фінансової безпеки підприємства // «Спецпроект: аналіз наукових досліджень»: зб. наук. праць IX Міжнар. наук.-практ. конф., 30–31 травня 2014 р. Т. 1. Київ-Дніпропетровськ : УМО ДНУ, 2014. С. 98–101