

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова праця
на правах рукопису

ЛЕСУН СЕРГІЙ МИКОЛАЙОВИЧ

УДК 658.14/.17:[338.46:004]:330.341(043.5)

ДИСЕРТАЦІЯ

**ФОРМУВАННЯ СИСТЕМИ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВ
ІТ-СФЕРИ В УМОВАХ СТАНОВЛЕННЯ ЦИФРОВОЇ ЕКОНОМІКИ**

Галузь науки: 07 «Управління та адміністрування»

Спеціальність: 072 «Фінанси, банківська справа та страхування»

Подається на здобуття наукового ступеня доктора філософії.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

 — С. М. Лесун

Науковий керівник: Панченко Олена Іванівна, кандидат економічних наук,
доцент

АНОТАЦІЯ

Лесун С. М. Формування системи фінансової безпеки підприємств ІТ-сфери в умовах становлення цифрової економіки. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 072 «Фінанси, банківська справа та страхування» (07 «Управління та адміністрування»). – Національний університет «Чернігівська політехніка». – Чернігів, 2026.

У дисертаційній роботі поглиблено теоретико-методичні засади та розроблено науково-практичні рекомендації щодо формування системи фінансової безпеки підприємств ІТ-сфери в умовах становлення цифрової економіки.

Стабільне функціонування підприємств ІТ-сфери є важливою передумовою розвитку цифрової економіки, інноваційної трансформації національного господарства та зміцнення фінансової стійкості держави. Підприємства цієї сфери забезпечують створення інтелектуальних продуктів, розвиток цифрових сервісів, підтримку технологічної модернізації бізнес-процесів тощо. В умовах високої динамічності зовнішнього середовища, цифрової трансформації економічних процесів та ускладнення доступу до фінансових ресурсів такі суб'єкти господарювання стикаються з необхідністю забезпечення безперервності діяльності, збереження фінансової стійкості, підтримання інвестиційної привабливості та адаптації до нових викликів і загроз. За таких умов особливого значення набуває формування цілісної системи фінансової безпеки підприємств ІТ-сфери, здатної забезпечити своєчасне виявлення ризиків, захист фінансових ресурсів і цифрових активів, а також створення передумов для їхнього довгострокового розвитку.

У роботі поглиблено категоріальний апарат фінансової науки в частині уточнення змісту поняття «фінансова безпека ІТ-підприємства». На основі

узагальнення підходів до трактування сутності фінансової безпеки, фінансової безпеки підприємства та врахування специфічних рис господарської діяльності ІТ-підприємств запропоновано розглядати фінансову безпеку таких суб'єктів господарювання як динамічний стан захищеності фінансових ресурсів, цифрових активів, інформаційних систем і бізнес-процесів, що забезпечує фінансову стійкість, ліквідність, платоспроможність, адаптивність і безперервність функціонування.

Значну увагу приділено дослідженню впливу цифрової економіки на функціонування системи фінансової безпеки підприємств ІТ-сфери. Такий вплив систематизовано за технологічним, інформаційним, організаційним, ризиковим, інфраструктурним та інституційним напрямками, що дозволило виокремити конструктивні й деструктивні наслідки цифровізації діяльності ІТ-підприємств, визначити роль інформаційних технологій у формуванні їхньої фінансової стійкості та обґрунтувати вектори інтеграції цифрових технологій у систему фінансового менеджменту зазначених підприємств.

Також у дисертації набули подальшого розвитку наукові положення щодо обґрунтування впливу стабільності фінансової діяльності ІТ-підприємств на рівень фінансової безпеки ІТ-галузі та національного господарства. Виокремлено ключові канали такого впливу та конкретизовано його наслідки для забезпечення стійкого розвитку фінансової системи держави. Доведено, що фінансова безпека ІТ-підприємств має не лише мікроекономічне, а й галузеве та макрофінансове значення, оскільки стабільність їх функціонування впливає на експортний потенціал, інвестиційну привабливість, податкові надходження та загальну фінансову стійкість національної економіки.

У дисертації обґрунтовано концептуальні положення формування системи фінансової безпеки підприємств ІТ-сфери. На основі системного підходу, дослідження особливостей фінансової діяльності ІТ-підприємств та аналізу ендегенних і екзогенних чинників, що впливають на ефективність їх функціонування, конкретизовано структурні компоненти цієї системи,

визначено джерела виникнення потенційних загроз та виокремлено прикладні напрями забезпечення фінансової безпеки ІТ-підприємств з урахуванням можливостей і викликів цифрової економіки. Систему фінансової безпеки ІТ-підприємства розглянуто як відкриту, динамічну та адаптивну сукупність взаємопов'язаних елементів, функціонування яких спрямоване на підтримання фінансової рівноваги, захист фінансових, інформаційних і технологічних ресурсів, забезпечення безперервності діяльності та здатності підприємства своєчасно реагувати на зміни внутрішнього й зовнішнього середовища в умовах цифрової економіки.

Також у роботі удосконалено методичний інструментарій оцінювання рівня фінансової безпеки підприємств ІТ-сфери. Запропонований підхід ґрунтується на розрахунку інтегрального показника стану фінансової безпеки з конкретизацією його ключових складових: фінансової стійкості, ліквідності, прибутковості, майнового стану, рівня ділової активності та інвестиційної привабливості. Це забезпечило можливість комплексного оцінювання рівня фінансової безпеки ІТ-підприємств з урахуванням галузевої специфіки, виявлення зміни її рівня та формування аналітичної основи для вибору відповідних стратегій забезпечення фінансової безпеки.

У дисертації здійснено систематизацію деструктивних чинників та потенційних загроз фінансовій безпеці підприємств ІТ-сфери. На основі поєднання результатів PEST- та SWOT-аналізу, а також дослідження поточного фінансового стану ІТ-підприємств такі загрози розподілено на воєнно-політичні, фінансово-економічні, регуляторні, кадрові, технологічні та кібербезпекові. Це дозволило врахувати їхній потенційний вплив на фінансову безпеку підприємств ІТ-сфери у процесі обґрунтування стратегій її забезпечення та формування відповідних управлінських рішень.

Прикладні положення дисертації спрямовано на обґрунтування механізму забезпечення фінансової безпеки підприємств ІТ-сфери та визначення напрямів його практичної реалізації в умовах цифрової економіки. На основі результатів інтегрального оцінювання, систематизації ризиків і

загроз та сценарного підходу обґрунтовано доцільність застосування диференційованих стратегій підвищення фінансової безпеки підприємств ІТ-сфери, орієнтованих на своєчасне реагування на зміну їхнього фінансового стану, підтримання фінансової стійкості та адаптацію до дестабілізуючих чинників.

У роботі розкрито науково-практичні аспекти державної та інституційної підтримки підвищення фінансової безпеки підприємств ІТ-сфери. На основі результатів кореляційно-регресійного аналізу обґрунтовано напрями такої підтримки, що орієнтовані на формування сприятливого економічного середовища, підвищення стійкості ІТ-підприємств до зовнішніх ризиків та зміцнення їх фінансової безпеки в умовах становлення цифрової економіки.

Практичне значення отриманих результатів полягає в можливості використання запропонованих теоретико-методичних положень, висновків і науково-практичних рекомендацій у діяльності підприємств ІТ-сфери, зокрема для проведення внутрішньої фінансової діагностики, моніторингу фінансових показників, ідентифікації загроз і ризиків, обґрунтування стратегій забезпечення фінансової безпеки та прийняття фінансових управлінських рішень. Окремі положення дисертаційної роботи можуть бути використані в освітньому процесі під час викладання навчальних дисциплін фінансового спрямування, а також у подальших наукових дослідженнях проблематики фінансової безпеки підприємств в умовах цифрової економіки.

Ключові слова: *фінансова безпека, фінансова безпека підприємства, ІТ-підприємство, ІТ-сфера, цифрова економіка, система фінансової безпеки, цифрові технології, фінансове управління, фінансова стійкість, ризики, загрози, цифровізація, інвестиційна привабливість, державна підтримка, фінансова безпека держави.*

ABSTRACT

Lesun S. M. Formation of a Financial Security System for IT Enterprises under the Conditions of the Emerging Digital Economy. - Qualification scientific work submitted as a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 072 “Finance, Banking and Insurance” (07 “Management and Administration”). Chernihiv Polytechnic National University. Chernihiv, 2026.

The dissertation deepens the theoretical and methodological foundations and develops scientific and practical recommendations for forming a financial security system for IT enterprises under the conditions of the emerging digital economy.

The stable functioning of IT enterprises is an important prerequisite for the development of the digital economy, the innovative transformation of the national economy, and the strengthening of the financial stability of the state. Enterprises in this sector ensure the creation of intellectual products, the development of digital services, and support for the technological modernization of business processes. Under conditions of high dynamism of the external environment, the digital transformation of economic processes, and limited access to financial resources, such business entities face the need to ensure business continuity, preserve financial stability, maintain investment attractiveness, and adapt to new challenges and threats. Under these conditions, the formation of an integrated financial security system for IT enterprises becomes particularly important, as it is capable of ensuring the timely identification of risks, the protection of financial resources and digital assets, and the creation of prerequisites for their long-term development.

The dissertation deepens the categorical apparatus of financial science in terms of clarifying the content of the concept of “financial security of an IT enterprise.” Based on the generalization of approaches to interpreting the essence of financial security and enterprise financial security, as well as taking into account the specific features of the economic activity of IT enterprises, it is proposed to consider the financial security of such business entities as a dynamic state of protection of

financial resources, digital assets, information systems, and business processes, which ensures financial stability, liquidity, solvency, adaptability, and continuity of functioning.

Considerable attention is paid to studying the impact of the digital economy on the functioning of the financial security system of IT enterprises. This impact is systematized according to technological, informational, organizational, risk-related, infrastructural, and institutional directions, which made it possible to identify the constructive and destructive consequences of the digitalization of IT enterprises, determine the role of information technologies in shaping their financial stability, and substantiate the vectors for integrating digital technologies into the financial management system of these enterprises.

The dissertation also further develops scientific provisions concerning the substantiation of the impact of the stability of financial activity of IT enterprises on the level of financial security of the IT industry and the national economy. The key channels of such influence are identified, and its consequences for ensuring the sustainable development of the state's financial system are specified. It is proved that the financial security of IT enterprises has not only microeconomic but also sectoral and macrofinancial significance, since the stability of their functioning affects export potential, investment attractiveness, tax revenues, and the overall financial stability of the national economy.

The dissertation substantiates the conceptual provisions for forming a financial security system for IT enterprises. Based on a systems approach, the study of the specific features of the financial activity of IT enterprises, and the analysis of endogenous and exogenous factors affecting the efficiency of their functioning, the structural components of this system are specified, the sources of potential threats are identified, and applied directions for ensuring the financial security of IT enterprises are outlined, taking into account the opportunities and challenges of the digital economy. The financial security system of an IT enterprise is considered as an open, dynamic, and adaptive set of interconnected elements whose functioning is aimed at maintaining financial equilibrium, protecting financial, informational, and

technological resources, ensuring business continuity, and enabling the enterprise to respond promptly to changes in the internal and external environment under the conditions of the digital economy.

The dissertation also improves the methodological toolkit for assessing the level of financial security of IT enterprises. The proposed approach is based on the calculation of an integral indicator of the state of financial security with the specification of its key components: financial stability, liquidity, profitability, property condition, business activity level, and investment attractiveness. This made it possible to comprehensively assess the level of financial security of IT enterprises, taking into account industry-specific characteristics, identify changes in its level, and form an analytical basis for selecting appropriate financial security strategies.

The dissertation systematizes destructive factors and potential threats to the financial security of IT enterprises. Based on a combination of PEST and SWOT analysis results, as well as the study of the current financial condition of IT enterprises, such threats are classified into military-political, financial-economic, regulatory, personnel-related, technological, and cybersecurity threats. This made it possible to take into account their potential impact on the financial security of IT enterprises in the process of substantiating strategies for ensuring it and forming appropriate managerial decisions.

The applied provisions of the dissertation are aimed at substantiating the mechanism for ensuring the financial security of IT enterprises and determining the directions of its practical implementation under the conditions of the digital economy. Based on the results of integral assessment, the systematization of risks and threats, and the scenario-based approach, the expediency of applying differentiated strategies for enhancing the financial security of IT enterprises is substantiated. These strategies are focused on timely response to changes in their financial condition, maintaining financial stability, and adapting to destabilizing factors.

The dissertation reveals the scientific and practical aspects of state and institutional support for enhancing the financial security of IT enterprises. Based on

the results of correlation and regression analysis, the directions of such support are substantiated, oriented toward the formation of a favorable economic environment, increasing the resilience of IT enterprises to external risks, and strengthening their financial security under the conditions of the emerging digital economy.

The practical significance of the obtained results lies in the possibility of using the proposed theoretical and methodological provisions, conclusions, and scientific and practical recommendations in the activities of IT enterprises, in particular for conducting internal financial diagnostics, monitoring financial indicators, identifying threats and risks, substantiating financial security strategies, and making financial managerial decisions. Certain provisions of the dissertation may be used in the educational process when teaching finance-related academic disciplines, as well as in further scientific research on the issues of enterprise financial security under the conditions of the digital economy.

Keywords: *financial security, enterprise financial security, IT enterprise, IT sector, digital economy, financial security system, digital technologies, financial management, financial stability, risks, threats, digitalization, investment attractiveness, state support, financial security of the state.*

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

статті в закордонних наукових виданнях,

включених до міжнародних наукометричних баз:

1. Yevtushenko Y., Bilyi, M., **Lesun S.**, Fedoriv, Y., Kravchenko A., & Akinchyts O. (2025). Customization of Financial Services: Digitalization, Transformation, Trust, Emphasizing the Role of Education in Processes. *Cadernos De Educação Tecnologia E Sociedade*, 18(se3), 239–249. DOI: <https://doi.org/10.14571/brajets.v18.nse3.239-249> (1,3 ум. друк. арк.). Особистий внесок: розглянуто роль цифрових технологій у трансформації фінансових послуг та формуванні довіри між фінансовими установами і споживачами (0,22 ум. друк. арк.).

2. Bilyi M., Kravchenko A., **Lesun S.**, Fedoriv Y., Penteleichuk M., & Akinchyts O. (2026). Formation of competitive advantages of financial institutions in the conditions of digitization and instability of the national economy. *Financial and Credit Activity Problems of Theory and Practice*, 1(66), 123–137. DOI: <https://doi.org/10.55643/fcaptp.1.66.2026.5024> (0,9 ум. друк. арк.). Особистий внесок: визначено роль цифрових технологій у формуванні конкурентних переваг фінансових установ в умовах нестабільності (0,16 ум. друк. арк.).

статті в наукових фахових виданнях України:

3. Лесун С. М. Фінансова безпека підприємств та її особливості в умовах цифрової економіки. *Проблеми і перспективи економіки та управління*. 2024. № 3(39). С. 341-352. URL: <http://ppeu.stu.cn.ua/article/view/319324> (0,61 ум. друк. арк.).

4. Кальченко О. М., Зеленська О. О., **Лесун С. М.** Фінансова поведінка домогосподарств у контексті розвитку поведінкових фінансів. *Проблеми і перспективи економіки та управління*. 2023. № 4(36). С. 280-290. URL: <http://ppeu.stu.cn.ua/article/view/299261> (0,69 ум. друк. арк.). Особистий внесок: узагальнено поведінкові чинники прийняття фінансових рішень в умовах ризику та невизначеності, що впливають на фінансову стійкість економічних суб'єктів (0,1 ум. друк. арк.).

5. Кальченко О. М., Лесун С. М. Економіко-статистичне дослідження ефективності використання фінансових ресурсів підприємств ІТ-сфери. *Проблеми і перспективи економіки та управління*. 2025. № 1(41). С. 422-436. URL: <http://ppeu.stu.cn.ua/issue/view/19295/12492> (0,68 ум. друк. арк.)
Особистий внесок: проведено аналіз структури фінансових ресурсів, активів і фінансових результатів підприємств ІТ-сфери та визначено їх вплив на фінансову стійкість ІТ-компаній (0,4 ум. друк. арк.).

6. Панченко О. І., Лесун С. М. Методичні підходи до оцінки рівня фінансової безпеки підприємств ІТ-сфери. *Проблеми і перспективи економіки та управління*. 2025. № 3(43). С. 347-358 URL: <http://ppeu.stu.cn.ua/article/view/344079> (0,75 ум. друк. арк.). Особистий внесок: систематизовано методичні підходи до оцінки фінансової безпеки підприємств ІТ-сфери, обґрунтовано доцільність використання інтегрального підходу та запропоновано етапи комплексного оцінювання її рівня з урахуванням галузових особливостей (0,45 ум. друк. арк.).

7. Дубина М. В., Кальченко О. М., Лесун С. М. Фінансове забезпечення розвитку ІТ-компаній в Україні. *Проблеми системного підходу в економіці*. 2025. Вип. 5 (102). С. 72-86. URL: http://www.psae-jrnl.nau.in.ua/journal/5_102_2025_ukr/11.pdf (1,06 ум. друк. арк.). Особистий внесок: визначено сутність, види та особливості функціонування ІТ-компаній, що впливають на формування їх фінансової стійкості та безпеки (0,45 ум. друк. арк.).

8. Кальченко О. М., Лесун С. М., Кальченко М. В. Фінансовий інструментарій забезпечення фінансової безпеки ІТ-підприємств в умовах цифрової економіки. *Успіхи і досягнення у науці*. 2026. № 4(26). С. 1356–1372 (1,07 ум. друк. арк.). Особистий внесок: узагальнено фінансовий інструментарій забезпечення фінансової безпеки ІТ-підприємств та визначено роль цифрових технологій у його реалізації (0,45 ум. друк. арк.).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

9. Панченко О. І., Лесун С. М. Особливості страхування фінансових ризиків банківських установ. *Фінансове та інформаційно-аналітичне забезпечення безпеки бізнесу в умовах воєнної економіки та повоєнного відновлення* : матеріали XII Міжнар. наук.-практ. конф., Харків, 22–23 листопада 2023 р. Харків : ХНУМГ ім. О. М. Бекетова, 2023. С. 220-222. URL: https://eprints.kname.edu.ua/64334/1/%D0%9A%D0%9E%D0%9D%D0%A4%D0%95%D0%A0%D0%95%D0%9D%D0%A6%D0%98%D0%AF%20%D0%A2%D0%B5%D0%B7%D0%B8%D1%81%D0%B8_2023_2.pdf (0,13 ум. друк. арк.).
Особистий внесок: розглянуто страховий механізм як інструмент мінімізації фінансових ризиків та забезпечення фінансової стійкості суб'єктів господарювання (0,05 ум. друк. арк.).

10. Панченко О. І., Кальченко О. М., Лесун С. М. Банкострахування як основа стабільності фінансового ринку. *Юність науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства* : збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 26-27 квітня 2023 р.). Чернігів : НУ «Чернігівська політехніка», 2023. С. 117-118. URL: <https://stu.cn.ua/wp-content/uploads/2023/11/zbirnyk-tez-yunist-nauky-2023.pdf> (0,15 ум. друк. арк.).
Особистий внесок: розглянуто страхові інструменти як засіб мінімізації фінансових ризиків і підтримання фінансової стійкості економічних суб'єктів (0,05 ум. друк. арк.).

11. Панченко О. І., Кальченко О. М., Лесун С. М. Проблеми розвитку сучасної системи ризик-менеджменту в банківських установах. *Юність науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства* : збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 26-27 квітня 2023 р.). Чернігів: НУ «Чернігівська політехніка», 2023. С. 118-120. URL: <https://stu.cn.ua/wp-content/uploads/2023/11/zbirnyk-tez-yunist-nauky-2023.pdf>

(0,18 ум. друк. арк.). Особистий внесок: узагальнено проблеми розвитку системи ризик-менеджменту та визначено його роль у забезпеченні фінансової стійкості суб'єктів господарювання (0,06 ум. друк. арк.).

12. **Лесун С. М.** Фінансова безпека підприємств в умовах становлення цифрової економіки. *Сучасні критерії оцінки ефективності господарських процесів в нестабільних економічних умовах* : матеріали Всеукр. наук.-практ. конф. (Чернігів, 12 листопада 2024 р.). Чернігів : Коледж транспорту та комп'ютерних технологій НУ «Чернігівська політехніка», 2024. С. 220-222 (0,12 ум. друк. арк.).

13. **Лесун С. М.** Соціально-філософський контекст управління фінансовими ризиками. *Юність науки – 2024: соціально-економічні та гуманітарні аспекти розвитку суспільства* : збірник тез доповідей XIV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 24-26 квітня 2024 р.). Чернігів : НУ «Чернігівська політехніка», 2024. С. 635-638. URL: <https://ir.stu.cn.ua/handle/123456789/30262> (0,2 ум. друк. арк.).

14. Панченко О. І., **Лесун С. М.** Специфіка підприємств ІТ-сфери як об'єкта фінансового управління. *Юність науки – 2025: збірник тез доповідей XV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених* (м. Чернігів, 23-25 квітня 2025 р.). Чернігів : НУ «Чернігівська політехніка», 2025. С. 78–80. URL: <https://ir.stu.cn.ua/items/7024c8b0-86f3-4ff4-baa0-3548f8c61574> (0,2 ум. друк. арк.). Особистий внесок: узагальнено специфіку підприємств ІТ-сфери як об'єкта фінансового управління та визначено її вплив на формування фінансової стійкості й безпеки (0,1 ум. друк. арк.).

15. **Лесун С. М.** Цифрова економіка та фінансова безпека: роль інформаційних технологій. *Фінансово-управлінські інновації як драйвер сталого розвитку в умовах сучасних викликів* : матеріали Міжнародної науково-практичної конференції (м. Хмельницький, 7 листопада 2025 року). Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2025. Ч. 1. С. 360-363 (0,2 ум. друк. арк.).

ЗМІСТ

ВСТУП	16
РОЗДІЛ 1. Теоретичні положення формування системи фінансової безпеки підприємств ІТ-сфери	25
1.1. Сутність фінансової безпеки та особливості її забезпечення в умовах становлення цифрової економіки.....	25
1.2. Концептуально-змістовні характеристики особливостей функціонування підприємств ІТ-сфери в цифровій економіці	49
1.3. Теоретичні засади формування системи фінансової безпеки підприємств ІТ-сфери	77
Висновки до першого розділу.....	104
РОЗДІЛ 2. Дослідження сучасного стану фінансової безпеки підприємств ІТ-сфери	107
2.1. Сучасний стан та тенденцій розвитку підприємств ІТ-сфери України.....	107
2.2. Комплексна оцінка фінансового стану підприємств ІТ-сфери України.....	133
2.3. Методологічні засади оцінки фінансової безпеки підприємств ІТ-сфери в умовах цифрової економіки	157
Висновки до другого розділу	181
РОЗДІЛ 3. Концептуальні засади розвитку системи фінансової безпеки ІТ-підприємств в умовах становлення цифрової економіки	184
3.1. Оцінка та характеристика загроз формування системи фінансової безпеки підприємств ІТ-сфери	184
3.2. Формування механізму забезпечення фінансової безпеки підприємств ІТ-сфери	210
3.3. Державна та інституційна підтримка підвищення фінансової безпеки ІТ-підприємств в умовах цифрової економіки.....	245

Висновки до третього розділу	274
ВИСНОВКИ	277
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	281
ДОДАТКИ	313

ВСТУП

Сучасний розвиток підприємств ІТ-сфери відбувається в умовах становлення цифрової економіки, прискорення технологічних змін, зростання нестабільності зовнішнього середовища та ускладнення фінансово-економічних процесів. Для України ці виклики набувають особливої гостроти в умовах воєнного стану, що супроводжується підвищеними ризиками, обмеженням доступу до фінансових та інвестиційних ресурсів, зміною умов ведення бізнесу й потребою у зміцненні стійкості підприємств до внутрішніх і зовнішніх загроз.

Питання забезпечення фінансової безпеки підприємств ІТ-сфери за таких умов набувають особливої актуальності, оскільки виступають важливою передумовою їх стабільного функціонування, здатності протидіяти негативним впливам, зберігати фінансову рівновагу та реалізовувати наявний потенціал розвитку.

Водночас в умовах цифрової економіки змінюються не лише технологічні засади функціонування підприємств ІТ-сфери, а й підходи до організації фінансового управління, оцінювання та мінімізації ризиків, забезпечення платоспроможності, фінансової стійкості та фінансової результативності в довгостроковій перспективі. У цьому контексті зростає значення своєчасного фінансового аналізу, прогнозування можливих загроз, ефективного використання ресурсів, вибору відповідних інструментів управління та застосування можливостей сучасних цифрових технологій для підтримки стабільної діяльності підприємств у динамічному середовищі.

Функціонування та розвиток підприємств в умовах цифрової економіки досліджували у своїх наукових доробках такі вчені, як: О. Виноградова, О. Гудзь, О. Гусева, Т. Гринько, С. Коляденко, Н. Краус, К. Краус, О. Голобородько, І. Струтинська, С. Тульчинська, М. Верескун, Г. Карчева, З. Живко, Н. Подольчак, О. Птащенко, М. Портер, Д. Тапскотт та ін.

Питанням забезпечення фінансової безпеки присвячено багато праць таких науковців, як: О. Ареф'єва, О. Барановський, О. Василик, В. Геєць, М. Ермошенко, К. Горячева, О. Ілляшенко, Г. Козаченко, Т. Кузенко, Н. Краснокутська, І. Манцуров, С. Мельник, О. Мініна, В. Мунтіян, О. Панченко, Н. Пойда-Носик, О. Терещенко, О. Шишкіна, С. Шкарлет та ін.

Особливості розвитку ІТ-підприємств у сучасних умовах становлення цифрової економіки розглядають у своїх наукових роботах О. Ананьєва, Б. Луговець, І. Кораблінова, О. Лаговська, Г. Лоскоріх, Ю. Ковтуненко, М. Кужелєв, М. Мельник, Н. Тимошенко, В. Міщенко, О. Пащенко, О. Базик та ін. Окремі питання фінансової безпеки, фінансового управління та аналізу діяльності ІТ-компаній досліджували Н. Виговська, Н. Демчишак, В. Дранус, В. Ільчук, О. Костюнік, А. Полчанов, І. Литвинчук, І. Чуй, О. Мицак, В. Панченко, А. Семенов, В. Чижов, М. Дубина та ін.

Попри наявність значної кількості наукових праць, присвячених фінансовій безпеці підприємств, фінансовій стійкості, антикризовому управлінню, цифровізації економіки та розвитку ІТ-сфери, питання формування системи фінансової безпеки саме ІТ-підприємств в умовах становлення цифрової економіки залишаються недостатньо розкритими. Це зумовлює необхідність подальшого теоретичного обґрунтування, методичного забезпечення та прикладного розроблення підходів до формування такої системи.

Таким чином, актуальність дисертаційного дослідження визначається потребою у розробці науково обґрунтованих підходів до формування сучасної, комплексної та адаптивної системи фінансової безпеки підприємств ІТ-сфери, яка враховує особливості їх функціонування в умовах становлення цифрової економіки. Формування такої системи є важливою передумовою зміцнення фінансової стійкості, підтримання фінансової рівноваги, підвищення конкурентоспроможності та забезпечення довгострокового розвитку ІТ-підприємств у динамічному зовнішньому середовищі.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційну роботу виконано в рамках планів науково-дослідних робіт Національного університету «Чернігівська політехніка» за темою «Розробка механізму фінансування інноваційного відновлення стратегічно важливих секторів економіки України у післявоєнний період» (державний реєстраційний номер 0123U104318), де автором обґрунтовано теоретичні положення щодо змісту та особливостей фінансової безпеки підприємств в умовах становлення цифрової економіки; «Розвиток фінансової системи в умовах турбулентності та становлення цифрової економіки» (державний реєстраційний номер 0125U000298), у межах якої автором поглиблено методичні підходи до оцінювання рівня фінансової безпеки підприємств ІТ-сфери.

Мета і завдання дослідження. Метою дисертаційної роботи є поглиблення теоретико-методичних засад та обґрунтування практичних рекомендацій щодо формування системи фінансової безпеки підприємств ІТ-сфери в умовах становлення цифрової економіки.

Для досягнення мети в роботі поставлено такі завдання:

- розкрити сутність фінансової безпеки та особливості її забезпечення в умовах становлення цифрової економіки;
- визначити концептуально-змістовні характеристики особливостей функціонування підприємств ІТ-сфери в цифровій економіці;
- обґрунтувати теоретичні засади формування системи фінансової безпеки підприємств ІТ-сфери та визначити її структурно-логічну побудову і функціональне призначення у забезпеченні їх фінансової стійкості;
- проаналізувати тенденції розвитку підприємств ІТ-сфери та оцінити їх фінансовий стан в контексті забезпечення фінансової безпеки;
- удосконалити науково-методичний підхід та провести комплексне оцінювання рівня фінансової безпеки підприємств ІТ-сектору з урахуванням галузевих особливостей;
- систематизувати ризики та загрози фінансової безпеки підприємств ІТ-сфери в умовах становлення цифрової економіки;

- обґрунтувати концептуальні засади розробки та практичної реалізації механізму забезпечення фінансової безпеки ІТ-підприємств в умовах цифрової економіки;

- сформувати науково-практичні рекомендації щодо підвищення фінансової безпеки підприємств ІТ-сектору у системі державної та інституційної підтримки.

Об'єктом дослідження є процес формування та забезпечення фінансової безпеки підприємств.

Предметом дослідження є теоретико-методичні підходи щодо формування системи фінансової безпеки підприємств ІТ-сфери в умовах становлення цифрової економіки.

Методи дослідження. У дисертаційній роботі використано сукупність загальнонаукових і спеціальних методів, що забезпечили комплексність і наукову обґрунтованість отриманих результатів. Зокрема, методи наукового аналізу, синтезу та узагальнення застосовано для розкриття сутності фінансової безпеки підприємств ІТ-сфери та визначення особливостей їх функціонування в умовах становлення цифрової економіки; системний підхід і структурно-логічний аналіз використано для дослідження системи фінансової безпеки ІТ-підприємств, визначення її елементів, функцій та взаємозв'язків між складовими, а також для розробки механізму забезпечення фінансової безпеки підприємств ІТ-сфери; методи статистичного, порівняльного та коефіцієнтного аналізу застосовано для дослідження тенденцій розвитку ІТ-сектору, оцінювання фінансового стану підприємств галузі та визначення його впливу на фінансову безпеку; інтегральний метод та метод нормування показників використано для комплексного оцінювання рівня фінансової безпеки підприємств ІТ-сектору з урахуванням галузевих особливостей. PEST-аналіз застосовано для систематизації зовнішніх загроз, SWOT-аналіз - для узагальнення внутрішніх і зовнішніх чинників формування системи фінансової безпеки ІТ-підприємств; кореляційно-регресійний аналіз використано для оцінювання впливу макроекономічних і галузевих чинників

на рівень фінансової безпеки підприємств ІТ-сфери; метод сценарного аналізу застосовано для визначення варіантів управлінського реагування залежно від рівня фінансової безпеки ІТ-підприємства; табличний і графічний методи – для систематизації, візуалізації та наочного подання результатів дослідження.

Інформаційною базою дослідження є законодавчі та нормативно-правові акти України, офіційні статистичні дані Державної служби статистики України, Національного банку України, Міністерства цифрової трансформації України, Міністерства економіки України, Державної податкової служби України, аналітичні матеріали IT Ukraine Association, Lviv IT Cluster, DOU, Дія.City, Українського фонду стартапів, міжнародних організацій, фінансова звітність підприємств ІТ-сфери України, наукові праці вітчизняних і зарубіжних учених, матеріали науково-практичних конференцій, інформаційні ресурси мережі Internet, а також результати власних розрахунків і узагальнень автора.

Наукова новизна одержаних результатів полягає у поглибленні теоретико-методичних засад і розробленні науково-практичних рекомендацій щодо формування системи фінансової безпеки підприємств ІТ-сфери з урахуванням особливостей їх функціонування в умовах становлення цифрової економіки. Найбільш суттєві результати, що характеризують наукову новизну дисертаційної роботи та відображають особистий внесок автора, полягають у такому:

удосконалено:

– методичний інструментарій оцінювання рівня фінансової безпеки підприємств ІТ-сфери, який, на відміну від існуючих, сформульований на основі розрахунку інтегрального показника стану такої безпеки із конкретизацією його ключових параметрів (фінансова стійкість, ліквідність, прибутковість, майновий стан, рівень ділової активності та інвестиційна привабливість). Це забезпечило можливість обґрунтувати різні стратегії забезпечення фінансової безпеки підприємств цієї сфери з урахуванням сукупності фінансових ризиків і загроз;

– концептуальні положення обґрунтування сутності системи фінансової безпеки підприємств у ІТ-сфері, що реалізовано через використання методології системного підходу і, на відміну від існуючих положень, базуються на пізнанні та аналізі особливостей фінансової діяльності таких підприємств, дослідженні основних ендогенних та екзогенних чинників, які впливають на її ефективність. Це дало можливість конкретизувати структурні компоненти такої системи, визначити джерела виникнення потенційних загроз для її стабільності та виокремити прикладні напрями забезпечення її стабільного розвитку з урахуванням можливостей і викликів цифрової економіки;

– прикладні аспекти підвищення ефективності державної підтримки забезпечення фінансової безпеки підприємств ІТ-сфери, які, на відміну від уже сформованих підходів, конкретизовано через використання результатів кореляційно-регресійного аналізу впливу макроекономічних чинників на їхній фінансовий стан. Це дало можливість обґрунтувати основні напрями впливу органів державної влади на функціонування таких підприємств з метою формування сприятливого економічного середовища для зміцнення рівня їхньої фінансової безпеки.

– наукові підходи до визначення результатів впливу цифрової економіки на функціонування системи фінансової безпеки підприємств ІТ-сфери, які, на відміну від існуючих, реалізовано через систематизацію та розподіл можливих наслідків такого впливу за такими напрямками: технологічним, інформаційним, організаційним, ризиковим, інфраструктурним та інституційним. Це забезпечило можливість виокремити конструктивні та деструктивні наслідки цифровізації діяльності ІТ-підприємств, визначити вплив інформаційних технологій на формування їхнього фінансового стану та обґрунтувати вектори інтеграції цифрових технологій у систему фінансового менеджменту зазначених підприємств.

набуло подальшого розвитку

– поглиблення категоріального апарату фінансової науки у частині уточнення змісту поняття «фінансова безпека ІТ-підприємства», що реалізовано через обґрунтування сутності категорій «фінансова безпека»,

«фінансова безпека підприємства», конкретизацію специфічних рис господарської діяльності ІТ-підприємств. Запропоновано розглядати фінансову безпеку ІТ-підприємства як динамічний стан захищеності фінансових ресурсів, цифрових активів, інформаційних систем і бізнес-процесів, що забезпечує фінансову стійкість, ліквідність, платоспроможність, адаптивність і безперервність функціонування підприємств, основним видом діяльності яких є створення інтелектуальних продуктів, пов'язаних з інформаційними технологіями;

– систематизація деструктивних чинників та потенційних загроз фінансовій безпеці підприємств ІТ-сфери, які, на відміну від існуючих підходів, виокремлено на основі поєднання результатів застосування PEST- та SWOT-аналізу, дослідження їхнього поточного фінансового стану, та розподілено у наступні групи: воєнно-політичні, фінансово-економічні, регуляторні, кадрові, технологічні та кібербезпекові. Це дало можливість враховувати їхній потенційний вплив на фінансову безпеку зазначених підприємств у процесі розробки стратегій її підвищення;

– наукові положення щодо обґрунтування впливу стабільності фінансової діяльності ІТ-підприємств на рівень фінансової безпеки ІТ-галузі та національного господарства, що реалізовано через виокремлення ключових каналів здійснення такого впливу та конкретизацію його наслідків для забезпечення стійкого розвитку фінансової системи держави.

Практичне значення отриманих результатів полягає в тому, що результати наукових положень, висновків та науково-практичних рекомендацій, які сформульовані в дисертаційній роботі, можуть бути використані у практичній діяльності підприємств ІТ-сфери, навчальному процесі та науково-дослідній роботі. Зокрема, положення щодо комплексного оцінювання рівня фінансової безпеки ІТ-підприємства на основі інтегрального показника використані у практичній діяльності SendPulse Inc. під час проведення внутрішньої фінансової діагностики, моніторингу фінансових показників, виявлення негативних тенденцій у фінансово-господарській

діяльності для зміцнення фінансової стійкості підприємства (довідка № 02-15/11 від 12.05.2026р.); ФОП Базилевич В.М. прийняті до використання рекомендації щодо ідентифікації зовнішніх загроз і внутрішніх ризиків фінансової безпеки ІТ-підприємств, їх систематизації та застосування сценарного підходу до реагування на дестабілізаційні чинники цифрового середовища (довідка № 03/05-26 від 11.05.2026р.); ТОВ «Айті-Солюшнс» враховано пропозиції щодо використання цифрових інструментів у системі забезпечення фінансової безпеки підприємства (довідка про впровадження результатів дослідження від 5.05.2026р.). Окремі теоретичні та методичні положення і висновки щодо формування системи фінансової безпеки підприємств ІТ-сфери в умовах становлення цифрової економіки використані в освітньому процесі кафедри фінансів, банківської справи та страхування Національного університету «Чернігівська політехніка» при розробці методичних матеріалів, а також під час проведення лекційних і практичних занять з навчальних дисциплін «Фінансовий аналіз», «Фінансове планування у бізнесі», «Фінанси підприємств», «Фінансовий менеджмент» (довідка № 202/08-835 від 12.05.2026р.).

Особистий внесок здобувача. Дисертаційна робота є самостійно виконаним завершеним науковим дослідженням. Наукові положення, теоретичні підходи, висновки та рекомендації, що виносяться на захист, сформульовані автором самостійно та відображають результати власних досліджень щодо формування системи фінансової безпеки підприємств ІТ-сфери в умовах становлення цифрової економіки. З наукових праць, опублікованих у співавторстві, у дисертації використано лише ті положення, які є результатом особистого внеску здобувача.

Апробація результатів дисертації. Основні теоретичні та методичні результати дисертаційного дослідження оприлюднено автором на міжнародних та всеукраїнських науково-практичних конференціях: Міжнародній науково-практичній конференції «Фінансове та інформаційно-аналітичне забезпечення безпеки бізнесу в умовах воєнної економіки та

повоєнного відновлення» (м. Харків, 22–23 листопада 2023 р.); XIII Міжнародній науково-практичній конференції студентів, аспірантів і молодих вчених «Юність науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства» (м. Чернігів, 26-27 квітня 2023 р.); Всеукраїнській науково-практичній конференції «Сучасні критерії оцінки ефективності господарських процесів в нестабільних економічних умовах» (м. Чернігів, 12 листопада 2024 р.); XIV Міжнародній науково-практичній конференції студентів, аспірантів і молодих вчених «Юність науки – 2024: соціально-економічні та гуманітарні аспекти розвитку суспільства» (м. Чернігів, 24-26 квітня 2024 р.); «Юність науки – 2025» (м. Чернігів, 23-25 квітня 2025 р.); Міжнародній науково-практичній конференції «Фінансово-управлінські інновації як драйвер сталого розвитку в умовах сучасних викликів» (м. Хмельницький, 7 листопада 2025 року).

Публікації. За результатами дослідження опубліковано 15 наукових праць, загальним обсягом 8,24 д.а., з яких 3,62 д.а. належить автору особисто. Зокрема, 2 статті у періодичних наукових виданнях іншої держави, одне з яких індексується в наукометричній базі Web of Science, 6 статей – у наукових фахових виданнях України, 7 публікацій апробаційного характеру.

Структура та обсяг дисертації. Дисертаційна робота складається з анотації, вступу, трьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертаційної роботи становить 331 сторінку, з них основний зміст викладено на 264 сторінках, перелік використаних джерел розміщений на 31 сторінках і налічує 276 найменувань. У дисертації розміщено 24 таблиці, 49 рисунків та 6 додатків, що займають 19 сторінок.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ПОЛОЖЕННЯ ФОРМУВАННЯ СИСТЕМИ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ІТ-СФЕРИ

1.1. Сутність фінансової безпеки та особливості її забезпечення в умовах становлення цифрової економіки

На сьогодні фінансова безпека в науково-прикладних дослідженнях розглядається як багаторівнева система, яка характеризується складною внутрішньою структурою та специфічними механізмами формування і забезпечення на кожному рівні господарювання. В умовах формування цифрової економіки ця економічна категорія набуває принципово нового змістового наповнення як у межах національної економіки, так і в діяльності окремих галузей або підприємств.

Сучасний розвиток цифрової економіки характеризується високим рівнем технологічної взаємодії між суб'єктами господарювання різних рівнів, широким застосуванням інформаційно-комунікаційних технологій та інформатизацією практично всіх галузей національного господарства, цифровізацією фінансової сфери та бізнес-процесів підприємств, що з одного боку дозволяє удосконалювати та розширювати можливості ведення господарської діяльності, але з іншого – супроводжується появою нових викликів та загроз, пов'язаних із ризиками втрати даних, кіберзагрозами, уразливістю інформаційних систем та цифрової інфраструктури тощо.

Такі зміни зумовлюють необхідність пристосування суб'єктів економіки до нових умов господарювання, забезпечення комплексного захисту їх фінансово-економічної діяльності від негативного впливу зовнішніх та внутрішніх загроз, що формуються в реаліях цифрової економіки.

У зв'язку з цим у професійному та науковому середовищі здійснюється перегляд традиційних підходів до розуміння сутності категорії фінансової безпеки на всіх рівнях господарювання, а також механізмів її забезпечення.

Умови сьогодення вимагають переходу від класичних моделей запобігання фінансовим ризикам до нових, більш технологічно орієнтованих, що передбачають інтеграцію цифрових технологій у систему фінансового менеджменту суб'єктів господарювання.

Розглянемо на початку нашого дослідження трактування поняття «безпека». У результаті узагальнення та порівняльного аналізу наукових підходів до визначення сутності категорії «безпека» можна зробити певні висновки. Незалежно від авторської інтерпретації, у всіх визначеннях простежується спільна суть – захищеність об'єкта (особистості, суспільства, держави, суб'єкта господарювання та ін.) від загроз, збереження життєво важливих функцій та запобігання негативним наслідкам.

Основна відмінність між підходами до визначення цього поняття полягає в різниці акцентів та цілей проваджуваних досліджень. Так, В. І. Франчук, Ю. С. Шемшученко та ін. [160; 213] розглядають безпеку переважно як активний процес виявлення, запобігання та нейтралізації загроз, що передбачає певну стабільну управлінську динаміку.

Інші автори [71; 80] акцентують увагу на безпеці як досягненні стану захищеності, тобто розглядають її в більш статичному контексті.

Медведева І. Б., Погосова М. Ю. безпеку загалом трактують як здатність суб'єкта (держави, галузі, підприємства) зберігати стійкість і цілісність функціонування, нейтралізувати загрози та забезпечувати досягнення стратегічних цілей [116].

Влучним є визначення С. Марової [112], яка пропонує розглядати безпеку як «стан, при якому сума впливів на систему зовнішніх та внутрішніх енергетичних та інформаційних потоків не перевищує допустимого значення, яке може призвести до руйнації самої системи безпеки», оскільки воно відображає системну природу безпеки як багатофакторного та динамічного явища. Такий підхід є особливо актуальним у контексті цифрової трансформації економіки.

Передусім варто зазначити, що в процесі становлення і розвитку теорії безпеки як самостійного наукового напрямку сформувалося розуміння

національної безпеки як багатофакторної категорії та цілісної системи, що охоплює різні сфери життєдіяльності держави та суспільства [226].

При цьому особливе місце у структурі національної безпеки належить економічній безпеці, яка виступає її ключовим компонентом та включає систему економічних, правових, організаційних та політичних заходів для забезпечення захисту національних інтересів, стабільності фінансової системи, інвестиційної привабливості економіки та спроможності держави ефективно виконувати свої функції і своєчасно реагувати на кризові явища й дестабілізаційні фактори [216].

Водночас економічна безпека включає низку складових, серед яких центральне місце посідає фінансова безпека. При цьому важливо підкреслити, що фінансова безпека в сучасних дослідженнях розглядається на трьох взаємопов'язаних рівнях: макро-, мезо- та мікрорівні, які перебувають у тісному взаємозв'язку й утворюють єдину, цілісну систему. Підприємства як ключові суб'єкти господарської діяльності формують фінансову стійкість на мікрорівні, забезпечуючи ефективне управління фінансово-господарськими процесами та протидію різноманітним ризикам і загрозам.

На мезорівні фінансова стійкість підприємств у межах окремої галузі або регіону консолідується, формуючи загальний рівень фінансової безпеки цієї ланки економіки. Своєю чергою стабільність провідних секторів і галузей економіки загалом забезпечує надійність і міцність фінансової безпеки держави на макрорівні. Така інтегративна структура системи фінансової безпеки свідчить про те, що зміни або виникнення загроз на одному із зазначених рівнів неминуче позначаються на функціонуванні інших рівнів системи фінансової безпеки.

На основі дослідження наукової літератури [16; 197; 211], можна констатувати, що сутність фінансової безпеки галузі полягає у збалансованості та захищеності фінансових відносин, достатності фінансових ресурсів, рівня ліквідності, платоспроможності, фінансової стійкості та ефективності використання капіталу підприємств, що входять до складу галузі чи сектору економіки.

З іншого боку, фінансову безпеку галузі можна охарактеризувати як здатність її суб'єктів ефективно протидіяти як зовнішнім, так і внутрішнім загрозам, підтримувати фінансову рівновагу, інвестиційну привабливість і здатність до самофінансування, забезпечувати технологічний розвиток та оперативно реагувати на зміни бізнес-середовища.

Очевидним є той факт, що фінансова стійкість і належний рівень фінансової безпеки підприємств будь-якого сектору економіки здійснюють позитивний вплив на стабільність розвитку національної економіки загалом. Отже, формування та забезпечення фінансової безпеки окремих галузей слід розглядати як один із ключових чинників не лише гарантування стабільності фінансово-економічних відносин та підвищення конкурентоспроможності галузі, а й забезпечення загальної фінансово-економічної стабільності держави.

Далі, у межах нашої дисертаційної роботи особливу увагу приділимо такій науковій категорії, як «фінансова безпека підприємства» (рис. 1.1). При цьому зауважимо, що хоча фінансова безпека підприємства і розглядається як складова економічної безпеки, але функціонально це автономна система, що має власні об'єкти, інструменти та механізми забезпечення.

Проведений аналіз наукових праць з цієї тематики дозволив виділити наукові підходи до визначення сутності фінансової безпеки підприємства (рис. 1.2), що ґрунтуються на різних концепціях, економічних школах та парадигмах фінансового менеджменту [103; 223].

У межах *ресурсного підходу* фінансова безпека розглядається як «стан найбільш ефективного використання корпоративних ресурсів підприємства, виражене в кращих значеннях фінансових показників прибутковості та рентабельності бізнесу, якості управління, використання основних і оборотних коштів підприємства, структури його капіталу, а також курсової вартості його цінних паперів як синтетичного індикатора поточного фінансово-господарського стану підприємства і перспектив його технологічного і фінансового розвитку» [5] або як «захищеність його фінансових інтересів та наявність фінансових ресурсів для задоволення своїх потреб та виконанням існуючих зобов'язань» [114].

Сутність поняття «Фінансова безпека підприємств»	
І. Д'яконова [49]	Фінансову безпеку слід визначати як такий стан економічних відносин, що виникають між суб'єктами корпоративного управління, який забезпечує досягнення довгострокових цілей діяльності підприємства, шляхом узгодження їх фінансових інтересів
А. Крутова, Т. Ставерська, І. Шевчук [90]	Складова економічної безпеки підприємства, яка відображається через систему критеріїв і динамічних показників його стану, що дозволяє підтримувати фінансову стабільність у поточній та стратегічній перспективі, а також ступінь захищеності фінансових інтересів на усіх рівнях фінансових відносин за рахунок ефективного використання економічного потенціалу підприємства з метою протистояння зовнішнім і внутрішнім загрозам – як реальним, так і потенційним
Н. Пойда-Носик [158]	Фінансова безпека - складний багаторівневий процес забезпечення захищеності суб'єкта від негативного впливу зовнішніх і внутрішніх фінансових загроз та формування його фінансової рівноваги в поточній і стратегічній перспективі за рахунок ефективного використання його фінансового потенціалу з метою збільшення ринкової вартості
О. Арєф'єва, Т. Кузенко [6]	Стан найбільш ефективного використання корпоративних ресурсів підприємства, виражене в кращих значеннях фінансових показників прибутковості та рентабельності бізнесу, якості управління, використання основних і оборотних коштів підприємства, структури його капіталу, норми дивідендних виплат з цінних паперів підприємства, а також курсової вартості його цінних паперів як синтетичного індикатора поточного фінансово-господарського стану підприємства і перспектив його технологічного і фінансового розвитку
Н. Правдюк, Я. Мулик, Т. Мулик [165]	Фінансова безпека підприємства – це стан захищеності фінансових інтересів підприємства на всіх рівнях його фінансових відносин від впливу внутрішніх і зовнішніх загроз, який забезпечує його самозбереження та розвиток у поточній та стратегічній перспективах
І. Кононова [82]	Фінансова безпека як самостійний об'єкт у системі управління фінансами підприємства покликана підтримувати підприємство у стійкому фінансовому стані – це головна передумова його стабільного розвитку
Т. Мисник [122]	Фінансова безпека є категорією, яка відображає захищеність суб'єктів господарювання на всіх рівнях. Тобто це захищеність діяльності підприємства від негативних впливів зовнішнього середовища, а також здатність швидко усунути різноманітні загрози або пристосуватися до наявних умов, що не позначаються негативно на його діяльність та виявлення загроз і небезпек, що несе в собі внутрішнє середовище суб'єкта господарювання

Рис. 1.1. Наукова категорія «Фінансова безпека підприємства»

Джерело: складено автором.

Характеристика підходів до визначення поняття «Фінансова безпека підприємств»		
	Основні положення	Автори
Ресурсний підхід	<ul style="list-style-type: none"> - найбільш ефективне використання корпоративних ресурсів; - достатність фінансових ресурсів для задоволення своїх потреб і виконання зобов'язань; - ефективна та стабільна діяльність підприємства. 	Реверчук Н. [179], Марченко О. [114], Ареф'єва О., Кузенко Т. [5], Мунтіян В. [130], Загородній А., Вознюк Г. [56], Мельник І. [50] та ін.
Ризико-орієнтований підхід	<ul style="list-style-type: none"> - діяльність з управління ризиками; - захист від зовнішніх та внутрішніх загроз та мінімізація їх наслідків; - стабільність розвитку підприємства 	Куцик В., Бартиш А. [96], Сукрушева Г., Коляда К. [196], Шиназі Г. [94], Вівчар О. [26] та ін.
Стратегічний підхід	<ul style="list-style-type: none"> - впровадження та реалізація фінансової стратегії в умовах невизначеності та ризику; - захищеність підприємства в стратегічній перспективі. 	Кракос Ю., Разгон Р. [87], Гукова А., Анікіна І. [193], Пойда-Носик Н. [158], Руцишин Н., Ніконенко У., Костак З. [259] та ін.
Комплексний підхід	<ul style="list-style-type: none"> - складова економічної безпеки підприємства; - захищеність від внутрішніх та зовнішніх загроз; - система кількісних та якісних параметрів фінансового стану, що відображає рівень його захищеності; - збалансованість та якість фінансових інструментів, технологій, послуг. 	Судакова О. [195], Крутова А., Ставерська Т., Шевчук І. [90], Блакита Г., Галушак Т. [236], Бондарчук Н., Гуменчук Н. [15], Могилина Л. [127], Івашина Є., Чібісова І. [220] та ін.
Інноваційний підхід	<ul style="list-style-type: none"> - цифрові активи та інформаційні системи як об'єкти фінансового захисту; - інтеграція цифрових технологій у фінансове управління; - наявність кіберризиків та цифрових загроз. 	Захаркіна О. О., Бойко А. В., Сокол Л. В. [57], Демчишак Н., Шевчук Р., Гоменюк К. [38], та ін.

Рис. 1.2. Систематизація та характеристика підходів до визначення поняття «фінансова безпека підприємства»

Джерело: складено автором.

У межах *ризикоорієнтованого підходу* увага зосереджується на ідентифікації, оцінці та управлінні фінансовими ризиками, а фінансова безпека розглядається через призму антикризового управління та механізмів мінімізації негативних наслідків таких ризиків. Основною метою при цьому є забезпечення такого рівня захисту фінансових ресурсів, який дозволяє уникати або мінімізувати вплив негативних факторів зовнішнього та внутрішнього середовища [102].

Стратегічний підхід до визначення фінансової безпеки підприємств полягає у розгляді фінансової безпеки не лише як механізму захисту від ризиків та загроз, а і як системи довгострокового цілепокладання, головною метою якої стає забезпечення конкурентоспроможності, фінансової стійкості та рівноваги суб'єкта господарювання в перспективі.

Ми погоджуємось із думкою багатьох науковців, які вважають, що найбільш повним для розкриття сутності фінансової безпеки є *комплексний підхід*, який інтегрує теоретико-методологічні положення, що дозволяють врахувати специфіку діяльності підприємства, особливості зовнішнього середовища та фінансові цілі й завдання. Важливість комплексного підходу також полягає в інтеграції різних аспектів діяльності підприємства (фінансових, економічних, виробничих) для мінімізації впливу зовнішніх та внутрішніх загроз на його фінансову стійкість. У межах цього підходу фінансова безпека розглядається як одна з головних складових загальної системи економічної безпеки суб'єкта господарювання, а підприємство аналізується як складна система, що перебуває в постійній взаємодії із зовнішнім середовищем [102].

Таким чином, на основі проведеного дослідження наукових підходів можна виокремити низку спільних рис, характерних для тлумачення поняття «фінансова безпека підприємства». Насамперед більшість авторів розглядають фінансову безпеку як стан захищеності підприємства від внутрішніх і зовнішніх загроз, що негативно впливають на його фінансову стійкість і рівновагу. Водночас науковцями наголошується на важливості

ідентифікації, аналізу та мінімізації загроз і ризиків, оцінці їх впливу на оперативні та стратегічні фінансові цілі підприємства, а також на тісному взаємозв'язку рівня фінансової безпеки з результативністю діяльності, фінансовою стійкістю та ефективністю управління фінансовими ресурсами суб'єкта господарювання.

Разом з тим в ряді визначень акцент робиться виключно на підтриманні внутрішньої фінансової стійкості та платоспроможності. Такий підхід є обмеженим у сучасних умовах цифрової трансформації економіки, оскільки не враховує зростання ролі цифрових чинників, поширення кіберризиків та появу нових загроз, пов'язаних із диджиталізацією та динамічним технологічним розвитком усіх сфер економіки, що істотно змінюють ризикове середовище функціонування суб'єктів господарювання та робить його більш залежним від зовнішніх впливів.

У зв'язку з цим фінансова безпека вже не може обмежуватися класичним трактуванням: виключно як стан фінансової стійкості та рівноваги, що забезпечує протидію традиційним загрозам (зниження ліквідності, платоспроможності, погіршення інвестиційної привабливості тощо). В умовах цифрової економіки її зміст істотно розширюється та охоплює технологічні, інформаційні та інноваційні чинники, які формують нову логіку виникнення ризиків в діяльності підприємств та зумовлюють потребу у формуванні принципово нових механізмів забезпечення фінансової стійкості та рівноваги суб'єктів господарювання.

За таких умов виникає об'єктивна потреба в оновленні традиційних наукових підходів до вивчення фінансової безпеки підприємств з урахуванням процесів цифрової трансформації економіки. Хоча класичні аспекти в характеристиці фінансової безпеки й залишаються актуальними, їхнє змістовне наповнення зазнає суттєвих змін: акценти поступово зміщуються від вузько фінансових параметрів до комплексного врахування фінансових, інформаційних, технологічних та управлінських компонентів.

Подібні підходи дедалі частіше простежуються в сучасних дослідженнях [57; 38; 256], де цифрові технології розглядаються як важливий чинник досягнення належного рівня фінансової безпеки, удосконалення управління фінансовими ризиками та забезпечення ефективності управлінських та фінансових процесів.

Узагальнення наведених підходів дозволяє констатувати, що в сучасних наукових дослідженнях формується *інноваційний підхід* до розуміння сутності фінансової безпеки, який ґрунтується на концепції інтеграції цифрових технологій у систему її формування та забезпечення. В рамках цього підходу суттєво розширюється класичне розуміння змісту категорії «фінансова безпека підприємств», де підкреслюється важливість її адаптації до умов сучасних процесів диджиталізації економіки й підвищення внаслідок цього вимог до забезпечення фінансової стійкості суб'єктів господарювання. При цьому фінансова безпека розглядається як динамічна, ризикоорієнтована й технологічно інтегрована система, що здатна ефективно функціонувати у високотехнологічному цифровому середовищі та забезпечувати фінансову стійкість підприємства в умовах зростання рівня інформаційно-технологічних загроз.

На нашу думку, у межах інноваційного підходу цифрові технології виступають важливим елементом системи фінансової безпеки, оскільки дозволяють підвищити точність фінансової діагностики, посилити надійність фінансового контролю, удосконалити механізми реагування на ризики. Їх використання дозволяє формувати більш проактивні механізми управління фінансовою безпекою та підвищувати спроможність підприємств протистояти технічним і інформаційним загрозам, що можуть призводити до значних фінансових втрат.

Зазначена позиція узгоджується з висновками Мехеда А. М. та Варналія З. С., які підкреслюють, що цифрові технології суттєво підвищують рівень фінансової безпеки підприємства, а їх використання сприяє не лише оптимізації управлінських фінансових рішень, але й формуванню проактивного механізму забезпечення фінансової безпеки, здатного швидко

ідентифікувати потенційні загрози, адаптуватися до змін цифрового середовища та оперативно реагувати на внутрішні та зовнішні виклики [121].

Узагальнення наведених положень дозволяє зробити висновок, що в умовах цифрової економіки фінансова безпека набуває багаторівневого та комплексного характеру. Вона дедалі більше визначається рівнем технологічної готовності підприємства, його інноваційною гнучкістю, здатністю адаптації до технологічних змін та спроможністю забезпечувати належний рівень захисту як фінансових, так і інформаційних ресурсів.

На основі узагальнення існуючих підходів, фінансову безпеку підприємства в умовах цифрової економіки слід розуміти як динамічний стан захищеності фінансових ресурсів, інформаційних систем та бізнес-процесів від внутрішніх і зовнішніх загроз, який забезпечується ефективним управлінням фінансовими ризиками, підтримкою фінансової стійкості, ліквідності і платоспроможності, у тому числі й з використанням інноваційних цифрових технологій, а також здатністю підприємства адаптуватись до викликів цифрової трансформації з метою досягнення стратегічних та оперативних фінансових цілей.

Таким чином, зміна умов господарювання підприємств, ускладнення структури ризиків та цифровізація фінансово-економічних процесів зумовлюють необхідність переосмислення традиційних підходів до формування системи фінансової безпеки підприємств. Подальший аналіз таких трансформацій потребує звернення до сутності категорії «цифрова економіка», як нової парадигми розвитку, що формує якісно інші умови функціонування підприємств.

За прогнозами науковців, у найближче десятиліття близько 70 % створюваної вартості буде засновано на цифрових продуктах [2]. Наразі цифрова трансформація супроводжується зміною пріоритетів, ресурсів і моделей взаємодії між різними стейкхолдерами економічних процесів. Від традиційної економіки, що базується переважно на матеріальних активах і фізичній

інфраструктурі, цифрова економіка відрізняється створенням цінностей через дані, знання, цифрові платформи, алгоритми та інші ІТ-рішення.

Цифрова економіка нині виступає драйвером інноваційного розвитку та глобалізації для підприємств усіх галузей, водночас висуваючи нові вимоги до їхньої безпеки, конкурентоспроможності та спроможності адаптуватись до динамічних умов сучасності.

Формування теоретичних засад процесів цифровізації суспільства бере початок у 1994–1995 роках із фундаментальних праць Д. Тапскотта та Н. Негропонта [262], які вперше системно окреслили поняття цифрової економіки й цифрових трансформацій. З того часу термін «цифрова економіка» став широко використовуватися, відзначаючи новий етап активного розвитку інформаційно-комунікаційних технологій, сучасної ІТ-інфраструктури та зростаючу роль інтернету як основного каналу доступу до інформації [115; 55].

Загальновідомо, що в основі цифрової економіки лежить четверта промислова революція (Індустрія 4.0), яка ґрунтується на масштабному впровадженні інформаційно-комунікаційних технологій, автоматизації та інтеграції інтелектуальних ІТ-рішень у виробничі й управлінські процеси. Такі трансформації радикально змінюють структуру ринків, бізнес-моделі та управлінські практики як на рівні держави, так і в діяльності окремих секторів економіки та підприємств.

Під цифровою економікою, на думку Д. Тапскотта, треба розуміти «економічну діяльність, яка, на відміну від традиційної економіки, визначається мережевою свідомістю та залежністю від віртуальних технологій» [262]. Дослідження інших науковців сутності цифрової економіки представлені на рис. 1.3.

Аналіз наведених визначень демонструє, що всі автори наголошують на ключовій ролі в цифровій економіці інформаційно-комунікаційних технологій, які істотно змінюють суспільно-економічні відносини. Разом з тим, у науковому дискурсі можна виділити ряд основних підходів до визначення цієї

наукової категорії, кожен з яких має певні особливості та акценти, залежно від мети та предмета наукового дослідження.

Перший – *техніко-технологічний підхід* [173; 88; 134], переважає в наукових дослідженнях і в межах якого цифрова економіка розглядається з погляду активного впровадження інноваційних цифрових технологій у всі сфери господарської діяльності на макро- та мікрорівнях. Тобто, ключовими факторами в зазначеному контексті виступають цифрові дані, ресурси та платформи, а також відбувається створення нового кіберпростору, який сприяє змінам суспільних економічних відносин.

У межах *трансформаційного підходу*, або *структурно-секторального*, який також широко розповсюджений серед науковців, цифрова економіка розглядається як процес структурної трансформації економічної системи країни з перенесенням знань та інформації у цифрове середовище. Тобто йдеться про перехід від товарної моделі економіки до інформаційно-цифрової [24; 134].

Еволюційний підхід передбачає акцент на еволюційному характері цифрової економіки, яка розглядається як новий етап економічного розвитку, що формує нові інститути, бізнес-моделі та форми взаємодії економічних суб'єктів на основі цифрових технологій, які змінюють структуру традиційної економіки. Тобто підкреслюється незворотність цифрової трансформації всіх аспектів суспільно-економічної діяльності й перетин цифрової та традиційної економік [55; 177].

На нашу думку, найбільш комплексним є визначення цифрової економіки з погляду *системного підходу*, відповідно до якого цифрова економіка розглядається як інтегрована економічна система, де цифрові технології виступають ключовим драйвером створення, розподілу та споживання економічних благ, а взаємодія між державою, суб'єктами господарювання, суспільством і технологіями розглядається як єдина системна структура, що забезпечує узгоджений розвиток і адаптацію всіх її елементів до умов цифрової трансформації [4; 42].

Сутність поняття «цифрова економіка»	
Концепція розвитку цифрової економіки та суспільства України на 2018-2020 рр. [173]	Діяльність, у якій основними засобами (факторами) виробництва є цифрові (електронні, віртуальні) дані як числові, так і текстові.
С. Веретюк, В. Пілінський [24]	Ще нереалізована трансформація всіх галузей економіки завдяки перенесенню всіх інформаційних ресурсів і знань на комп'ютерну платформу
Г. Карчева, Д. Огородня, В. Опенько [70]	Цифрова економіка – це інноваційна динамічна економіка, що базується на активному впровадженні інновацій та інформаційно-комунікаційних технологій у всі види економічної діяльності та сфери життєдіяльності суспільства, що дозволяє підвищити ефективність та конкурентоспроможність окремих компаній, економіки та рівень життя населення
Н. Дєєва, В. Делейчук [42]	Цифрова економіка – це економічна діяльність, яка виникає на основі мільярдів повсякденних онлайн зв'язків між процесами, організаціями, громадянами, даними, пристроями
Н. Подольчак, О. Білик, В. Левицька [156]	Цифрова економіка – різновид ринку суб'єктів економічної системи на якому один, декілька або всі етапи господарських процесів здійснюються через комп'ютерні мережі; один із проявів економічної свободи, інноваційності та рівня розвитку економіки
О. Марченко [115]	Цифрова економіка – доповнення до традиційної економіки, що передбачає виготовлення та реалізацію традиційних товарів і послуг із використанням комп'ютерного обладнання та цифрових систем, зокрема мережі інтернет
Н. Краус, О. Голобородько, К. Краус [88]	Економіка, заснована на цифрових технологіях: конвергенції інформаційно-комунікативних технологій, знань, ресурсів
З. Живко, С. Родченко, Н. Лелюк [55]	Цифровізація економіки – процес еволюції економічних, соціальних, виробничих, організаційних, управлінських і суспільних відносин унаслідок розвитку інформаційно-цифрових технологій і комунікацій

Рис. 1.3. Наукові підходи до розуміння сутності категорії «цифрова економіка»

Джерело: складено автором.

Отже, цифрова економіка – це нова форма організації економічної діяльності, в основі якої лежить широке використання ряду ключових цифрових компонентів, які об'єднуються в єдину екосистему, що стимулює економічне зростання, підвищує конкурентоспроможність галузей економіки й формує нові моделі господарювання.

Ключові характеристики цифрової економіки, що формують якісно нові умови фінансово-економічної діяльності на всіх рівнях визначимо так:

- в умовах цифрової економіки відбувається трансформація природи економічних благ, оскільки поряд з традиційними матеріальними продуктами зростає роль продуктів і послуг нематеріального характеру, що забезпечує їх масове тиражування та поширення;

- широке застосування інформаційно-комунікаційних технологій у роботі підприємств відкриває нові перспективи для автоматизації бізнес-процесів, оптимізації виробництва та зниження операційних витрат, впливаючи на зміну підходів до організації фінансово-економічної діяльності суб'єктів господарювання;

- головним активом цифрової економіки є інформація та інновації, де цифрові дані, знання та програмні продукти набувають статусу стратегічного ресурсу, який має практично невичерпний характер та визначає ефективність виробництва, розподілу і споживання, формуючи при цьому нові підходи до управління економічними процесами;

- сучасна цифрова економіка ґрунтується на розвитку цифрових платформ та екосистем, які виступають новими центрами економічної координації та забезпечують мережеву взаємодію між різними групами користувачів, створюючи ефекти масштабу та змінюючи характер конкурентної боротьби, у якій визначальним стає рівень інтеграції цифрових сервісів;

- цифрова економіка носить глобальний та транскордонний характер, оскільки цифрові технології усувають територіальні бар'єри, створюють

умови для формування глобальних ринків, розширення міжнародної кооперації, інтеграції у світові цифрові ланцюги доданої вартості та появи нових форм транскордонної економічної діяльності;

- цифрова економіка сприяє появі нових спеціальностей і компетентностей, поширенню дистанційних форм зайнятості та розвитку гіг-економіки, що зумовлює зміну вимог до кваліфікації працівників, підвищує значення цифрових навичок та формує нові моделі зайнятості у різних секторах економіки;

- в умовах цифрової економіки особливо зростає значення кібербезпеки та відповідного нормативно-правового регулювання в питаннях захисту інформаційних систем, персональних даних та інтелектуальної власності для забезпечення довіри учасників цифрового простору [4; 42; 101; 177; 125].

Отже, можна констатувати, що цифрова економіка сьогодні суттєво трансформує традиційні підходи до ведення бізнесу та організації фінансово-економічних процесів як на макро-, так і на мікрорівнях. Розвиток цифрової економіки веде до змін характеру фінансової поведінки її суб'єктів, зрушень у всіх сферах підприємницької діяльності, змінюючи як внутрішні бізнес-процеси, так і характер зовнішньої взаємодії між суб'єктами ринку. Вона змінює логіку прийняття фінансових рішень економічного розвитку, акцентуючи увагу на інноваційності, динамічності та гнучкості в усіх сферах суспільно-господарських відносин [64].

Не менш суттєвим є вплив цифрової економіки й на фінансову безпеку суб'єктів господарювання. Тому, далі в роботі доцільним вважаємо уточнення змістовних характеристик фінансової безпеки підприємства саме в контексті цифрової економіки. Серед них виділимо такі:

- фінансова безпека є ключовим компонентом системи економічної безпеки підприємства, що забезпечує його фінансову стійкість, у тому числі в цифровому середовищі. Тому вона характеризується також здатністю суб'єктів

господарювання протистояти зростаючим кіберзагрозам і підвищеній невизначеності зовнішнього середовища;

- належний рівень фінансової безпеки досягається завдяки ефективному фінансовому управлінню та контролю за грошовими потоками, ліквідністю, прибутковістю і фінансовою стійкістю, враховуючи як традиційні фінансові ресурси, так і цифрові активи (дані, ІТ-інфраструктуру, інтелектуальну власність);

- фінансова безпека включає також цифрову безпеку фінансово-інформаційних систем, що передбачає захист інформаційних потоків та фінансових даних від кіберзагроз, несанкціонованого доступу та інформаційних маніпуляцій, а також забезпечення довіри контрагентів до цифрових каналів взаємодії;

- забезпечення фінансової безпеки передбачає використання сучасних цифрових технологій (автоматизації, аналітики даних, штучного інтелекту та ін.) для підвищення ефективності фінансового аналізу, контролю, точності фінансового планування та прогнозування і оперативності управлінських рішень;

- фінансова безпека проявляється через здатність підприємства реагувати на зовнішні та внутрішні фінансово-економічні виклики, зумовлені цифровими трансформаціями та високими темпами розвитку технологічних інновацій;

- забезпечення фінансової безпеки передбачає формування та реалізацію комплексної фінансової стратегії, що включає управління ризиками із використанням цифрових інструментів для захисту фінансових даних, підвищення прозорості та контролю за фінансовими операціями;

- фінансова безпека в умовах цифрової економіки вимагає забезпечення надійності інформаційних систем, захисту цифрових каналів фінансових операцій та контролю за використанням цифрових активів у процесі господарської діяльності підприємства;

- фінансова безпека визначається рівнем відповідності регуляторним та інституційним вимогам, дотриманням стандартів фінансової прозорості та захисту даних, а також здатністю підприємства адаптуватися до змін нормативно-правового регулювання в цифровій сфері [4; 95; 121; 223].

Таким чином, цифрова економіка створює принципово нові умови функціонування підприємств. Цифровізація проникає у всі сфери їх господарської діяльності та трансформує виробничі, фінансові, організаційно-управлінські та комунікаційні процеси, у результаті чого формуються специфічні канали впливу, через які процеси диджиталізації визначають рівень фінансової безпеки підприємства. Виокремлення таких аспектів впливу (рис. 1.4) дозволить сформувати теоретико-аналітичну основу для формування ефективної системи фінансової безпеки суб'єктів господарювання.

Процеси цифровізації, з одного боку, мають позитивний вплив на функціонування підприємств та рівень фінансової безпеки, з іншого – створюють нові виклики та загрози, які не були притаманні традиційній економіці (рис. 1.5).

Отже, розвиток цифрової економіки обумовлює необхідність переосмислення традиційних підходів до формування системи фінансової безпеки підприємства. Розглянемо більш детально основні аспекти таких змін.

Так, однією з ключових трансформацій, що відбувається в умовах розвитку цифрової економіки, є зміна та розширення об'єктів фінансового захисту. Якщо у традиційній економіці при забезпеченні фінансової безпеки основна увага зосереджувалась на збереження майна, капіталу, грошових коштів та інших фінансових ресурсів, то в цифровому середовищі зростає значення цифрових активів (інформаційних ресурсів, програмних продуктів, баз даних, IT-інфраструктури тощо). Проте природа цифрових активів суттєво відрізняється від матеріальних. Їхня технологічна складність, швидкі темпи оновлення та підвищена вразливість до кіберзагроз вимагають застосування спеціальних інструментів захисту з метою мінімізації фінансових втрат.

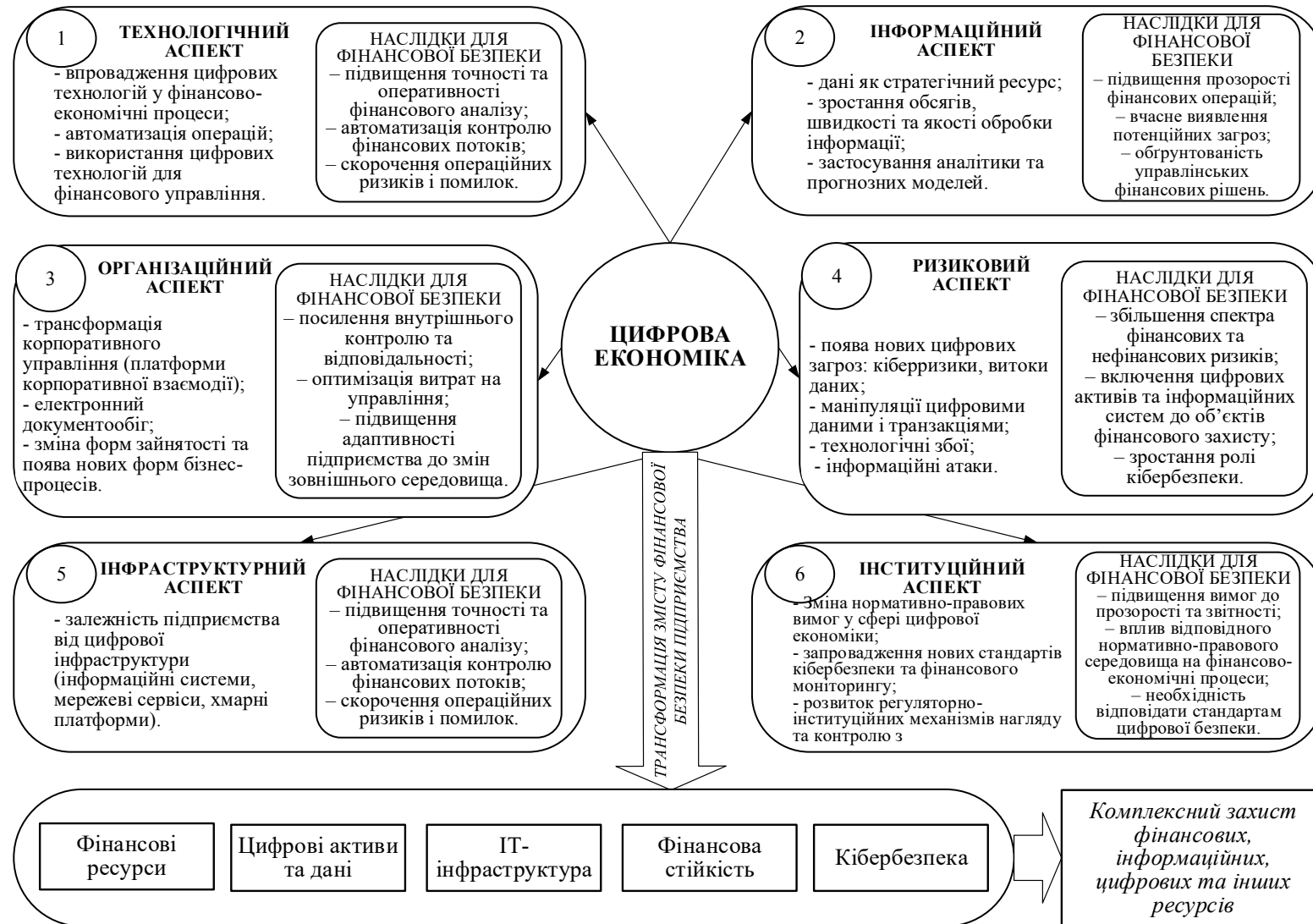
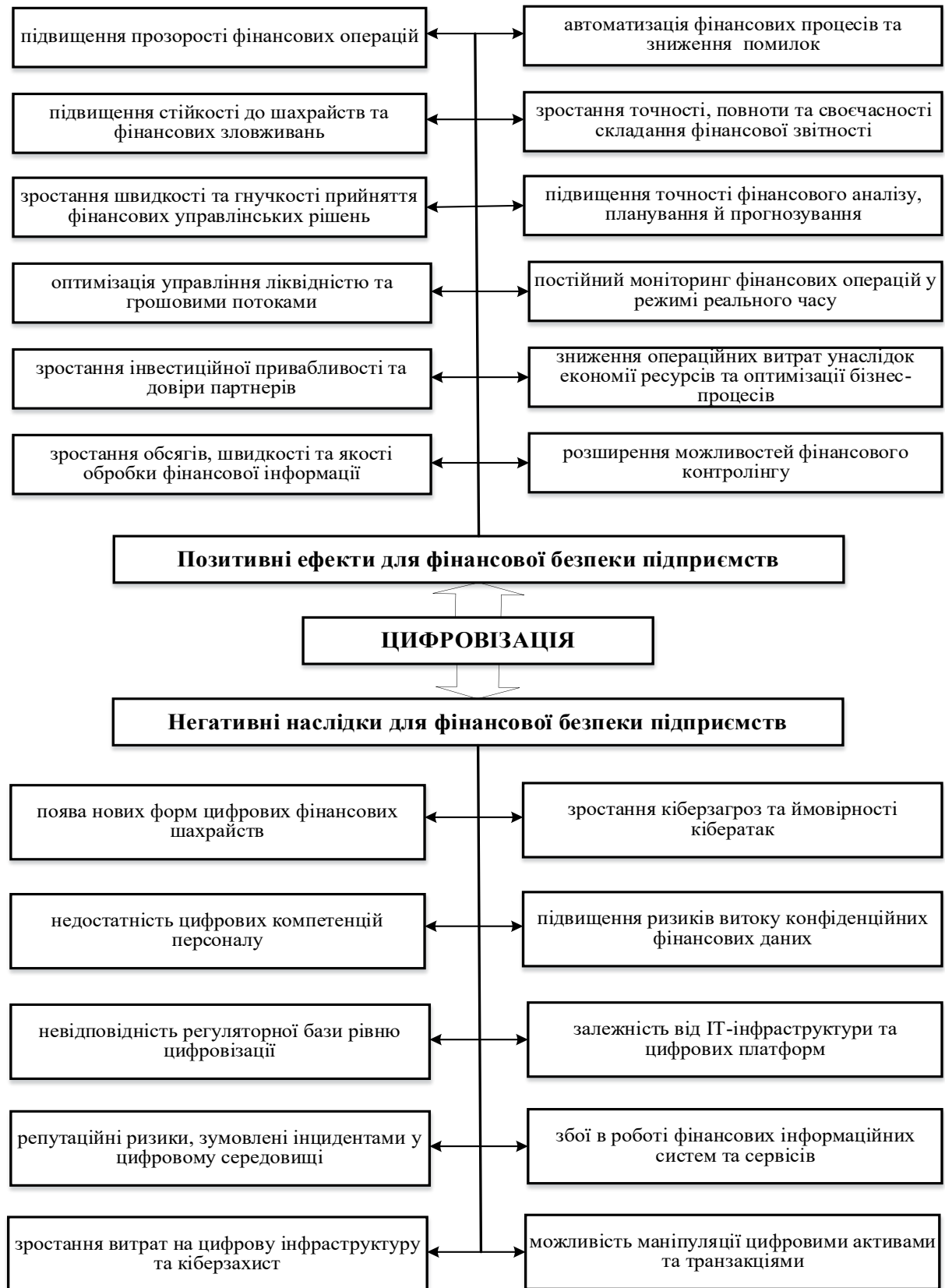


Рис. 1.4 Основні аспекти впливу цифрової економіки на фінансову безпеку підприємства

Джерело: складено автором на основі [26; 38; 57; 95; 134].



**Рис. 1.5. Позитивні ефекти та ризики цифровізації
для фінансової безпеки підприємств**

Джерело: узагальнено автором на основі [57; 68; 115; 210].

Також акцентуємо увагу на тому, що в сучасних умовах цифрової економіки суттєво змінюється спектр і характер ризиків, з якими стикаються підприємства. Поряд із традиційними ризиками (кредитними, ринковими, валютними, ризиками ліквідності) виникають специфічні цифрові виклики: кіберзагрози, ризики витоку даних, маніпуляції з цифровими активами, кібератаки на фінансові інформаційні системи, порушення роботи цифрових платформ тощо. Зростаючі темпи автоматизації внутрішніх бізнес-процесів також посилюють залежність підприємства від стабільності IT-інфраструктури та захищеності інформаційних ресурсів, що робить кібербезпеку одним із центральних чинників забезпечення його фінансової стійкості.

В умовах цифрової економіки фінансова безпека підприємства дедалі тісніше інтегрується з кібербезпекою, оскільки фінансові ресурси, грошові потоки та управлінські рішення все частіше реалізуються через цифрові канали та інформаційні системи. Інтеграція фінансової та кібербезпеки зумовлює необхідність переосмислення традиційних підходів до управління ризиками та доповнення їх інноваційними методами та інструментами, спрямованими на протидію кіберзагрозам, забезпечення ефективного реагування на виклики цифрового середовища та мінімізацію фінансових втрат, що спричинені кібератаками, шахрайськими діями та іншими формами несанкціонованого втручання в фінансову сферу суб'єктів господарювання.

Водночас цифрова економіка суттєво впливає і на механізми забезпечення фінансової безпеки, які стають дедалі більш залежними від процесів цифровізації. Тому розширення інструментарію фінансового управління, удосконалення системи фінансового моніторингу та контролю, а також побудова ефективної системи антикризового управління суб'єктів підприємницької діяльності повинні відбуватись з урахуванням сучасних цифрових реалій.

У новітньому цифровому середовищі на перший план виходять інноваційні методи та інструменти, що ґрунтуються на використанні цифрових даних, автоматизованих систем обробки інформації, засобів кіберзахисту та інших новітніх технологій. При цьому спектр таких технологій

стрімко розширюється, впливаючи на формування нової архітектури фінансової безпеки суб'єктів господарювання (рис. 1.6).



Рис. 1.6. Напрями цифрової трансформації у формуванні фінансової безпеки підприємства

Джерело: складено автором на основі [38; 68; 82; 256].

Так, значний потенціал для нейтралізації фінансових ризиків та загроз і зміцнення фінансової безпеки несуть можливості розвитку цифрових платформ і хмарних сервісів, блокчейн-рішень, а також технологій штучного інтелекту та аналітики великих даних тощо. Їх широке застосування розширює можливості фінансового планування та прогнозування, підвищує якість фінансової аналітики, швидкість прийняття управлінських рішень та ефективність фінансового менеджменту загалом [210].

Також важливо зазначити, що цифровізація змінює не лише об'єкти фінансового захисту та інструменти забезпечення фінансової безпеки, а й коло

її суб'єктів. У діяльності суб'єктів господарювання істотно зростає роль ІТ-підрозділів та фахівців, які стають важливим учасниками управління цифровими ризиками, забезпечуючи недопущення їх виникнення або мінімізацію впливу на фінансовий стан підприємства.

Цифрова економіка кардинально змінює підходи до фінансового управління загалом, трансформуючи процеси фінансового планування, контролю, внутрішнього аудиту, управління ліквідністю, платоспроможністю та фінансовою стійкістю. Перелічені функції дедалі більше ґрунтуються на цифрових технологіях, що забезпечує вищу точність фінансових розрахунків і аналітичних процедур.

Узагальнення наведених положень дозволяє запропонувати модель впливу цифрової економіки на фінансову безпеку підприємств, у межах якої цифрова економіка розглядається не лише як сукупність технологій, а як інтегроване середовище, що змінює умови функціонування підприємства, розширює об'єкти фінансового захисту, трансформує структуру ризиків і загроз, змінює коло суб'єктів забезпечення та зумовлює оновлення інструментів управління фінансовою безпекою (рис. 1.7).

Таким чином, можемо констатувати, що система фінансової безпеки підприємства в умовах цифрової економіки набуває нового змісту та може бути більш дієвою за умови переходу до нової логіки її формування. Ефективність такої системи визначається здатністю інтегрувати традиційні фінансові механізми із сучасними цифровими технологіями, активним використанням інноваційних технологічних рішень в системі фінансового менеджменту та посиленням ролі кібербезпеки для забезпечення фінансової стійкості підприємства. Саме поєднання окреслених підходів створює підґрунтя для формування динамічної, технологічно орієнтованої системи фінансової безпеки, що здатна забезпечувати фінансову стійкість підприємства у швидкозмінному цифровому середовищі як на макро-, так і на мікрорівні.

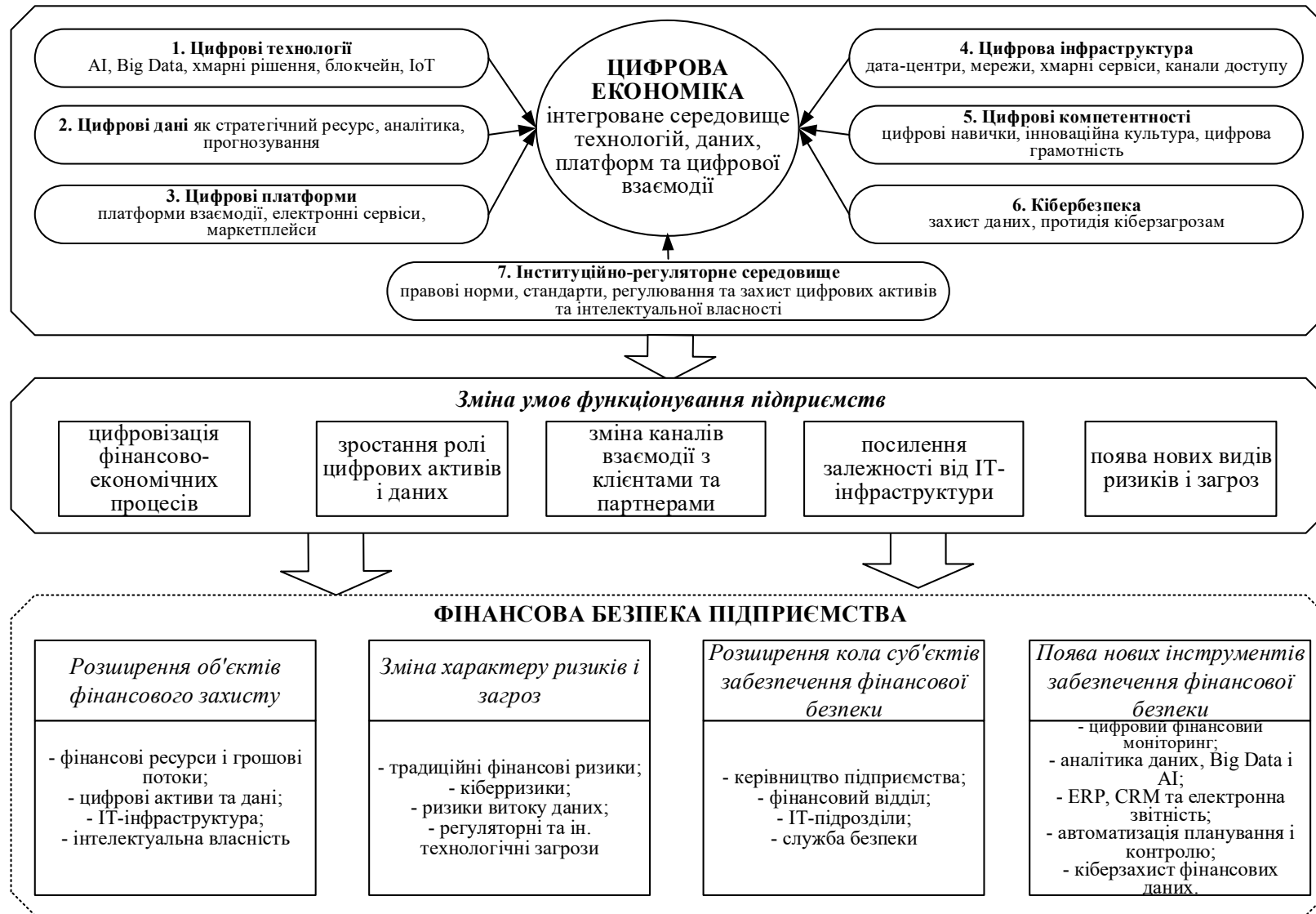


Рис. 1.7. Модель впливу цифрової економіки на фінансову безпеку підприємств

Джерело: складено автором на основі [26; 68; 121; 256].

Таким чином, у підрозділі 1.1 проведено комплексне дослідження сутності фінансової безпеки підприємств в умовах цифрової економіки. Розглянуто зміст категорії «безпека» та обґрунтовано роль фінансової безпеки як ключового елемента економічної безпеки на макро-, мезо- та мікрорівнях у межах єдиної ієрархічної системи.

Детально проаналізовано наукові підходи вчених до трактування дефініції «фінансова безпека підприємства» та встановлено, що у результаті розвитку цифрової економіки формується інноваційний підхід до її розуміння, у межах якого фінансова безпека розглядається як динамічна категорія, чутлива до впливу технологічних та інформаційних чинників.

Дослідження теоретичних підходів до визначення сутності цифрової економіки та виявлення її ключових характеристик дозволило встановити, що процеси цифрової трансформації істотно змінюють умови функціонування підприємств, структуру фінансових ризиків та справляють суттєвий вплив на фінансову безпеку корпоративного сектору. На цій основі визначено змістовні характеристики фінансової безпеки підприємств у цифровій економіці та окреслено основні особливості впливу цифровізації на формування системи фінансової безпеки суб'єктів господарювання. У результаті такого впливу фінансова безпека підприємства набуває нового змістового наповнення та характеризується новою логікою забезпечення, що поєднує традиційні фінансові механізми з сучасними цифровими технологіями. У цьому контексті особливе значення в процесах цифровізації економіки належить підприємствам ІТ-сфери, які виступають не лише провайдерами цифрових технологій, а й активними учасниками трансформації фінансово-економічних процесів.

Отже, отримані результати створюють теоретичне підґрунтя для подальшого аналізу галузевих аспектів формування системи фінансової безпеки суб'єктів господарювання ІТ-сфери, що буде розглянуто в наступних підрозділах дисертаційної роботи.

1.2. Концептуально-змістовні характеристики особливостей функціонування підприємств ІТ-сфери в цифровій економіці

На сучасному етапі розвитку суспільства цифрові технології стають ключовим рушієм структурних зрушень в економіці, впливаючи на трансформацію якісного складу факторів виробництва та традиційних моделей господарювання. У таких умовах переходу економіки до цифрової моделі розвитку зростає роль секторів, які забезпечують розробку та впровадження цифрових технологічних рішень.

Сьогодні ІТ-галузь стає драйвером інновацій та технологічного оновлення, і розглядається не лише як окремий сектор економіки, а і як інфраструктурна основа цифрової трансформації всіх сфер господарської діяльності. Широке застосування цифрових рішень обумовлює зростання ролі ІТ-сектору як структуроутворювального елементу сучасної економіки.

Підприємства, які працюють у сфері інформаційно-комунікаційних технологій, характеризуються певними унікальними особливостями функціонування та розвитку. Тому для формування цілісного бачення проблематики формування системи фінансової безпеки підприємств ІТ-сфери, необхідним є попередній аналіз їхнього видового складу, функціональних характеристик, ролі в структурі цифрової економіки, а також особливостей економічної діяльності та фінансового управління в умовах зростаючої нестабільності фінансово-економічного та цифрового середовища.

У науковій літературі під підприємствами ІТ-сфери розуміють організації, що здійснюють діяльність, пов'язану з інформаційними технологіями. Вони залучені до розробки, підтримки та впровадження ІТ-продуктів і послуг. Такі підприємства можуть спеціалізуватися на розробці програмного забезпечення (програмні продукти, мобільні додатки, корпоративні системи), наданні консалтингових послуг у сфері інформаційних систем та технологій, створенні та підтримці вебсайтів, цифрових маркетингових послуг, кібербезпеці, реалізації інфраструктурних рішень (мережеві технології, серверні та хмарні платформи) тощо [62; 84].

Узагальнено ІТ-підприємства можна охарактеризувати як суб'єкти господарювання, які функціонують у сфері ІКТ, яка включає весь комплекс процесів та засобів, що забезпечують збір, обробку, збереження, передачу й використання інформації засобами обчислювальної техніки та програмного забезпечення [47].

Варто зазначити, що згідно з результатами аналізу наукових джерел, терміни «ІТ-сфера», «ІТ-галузь», «ІТ-сектор» та «ІТ-індустрія» здебільшого використовуються як синоніми в академічному та прикладному дискурсі.

ІТ-сфера, що досліджується в межах цієї роботи, трактується як сукупність видів економічної діяльності, пов'язаних з розробкою, впровадженням, супроводом та комерціалізацією інформаційних технологій, програмного забезпечення, цифрових сервісів і засобів інформаційно-комунікаційної взаємодії. У такому розумінні ІТ-сфера охоплює як підприємства, що здійснюють безпосередню розробку програмного забезпечення, так і компанії, що спеціалізуються на обробці даних, хмарних послугах, кібербезпеці, ІТ-консалтингу, адмініструванні вебпорталів та ін.

Для конкретизації меж функціонування вітчизняних ІТ-підприємств доцільно звернутися до національної системи класифікації видів економічної діяльності (КВЕД). Слід зауважити, що в наукових дослідженнях немає єдиного підходу до визначення меж галузі інформаційних технологій. Згідно з національною класифікацією видів економічної діяльності, до ІТ-галузі належать підприємства за кодами 62 (комп'ютерне програмування, консультування з питань інформатизації тощо), 63 (оброблення даних, розміщення інформації тощо), а також окремі види діяльності, пов'язані з електронною комерцією, вебпорталами та хостингом [43].

Так, у працях [100; 209] до ІТ-сфери включено групу 62 «Комп'ютерне програмування, консультування та пов'язана з ними діяльність» за КВЕД.

Як зазначено в [25], ІТ-асоціація України зараховує до ІТ-галузі також такі види діяльності: 58.21 Видання комп'ютерних ігор; 58.29 Видання іншого програмного забезпечення; 63.11 Оброблення даних, розміщення інформації на вебвузлах і пов'язана з ними діяльність; 63.12 Вебпортали [246].

Проте, на нашу думку, спираючись на [72; 247] також доцільно віднести до ІТ-сфери й такий вид діяльності, як 63.99 «Надання інших інформаційних послуг, н.в.і.у.» (рис. 1.8), що охоплює різноманітні види діяльності, пов'язані з обробкою, пошуком і наданням інформації, яка не віднесена до інших категорій. Це можуть бути як традиційні інформаційні послуги, так і сучасні цифрові сервіси. Такі послуги можуть надавати аналітичні компанії, які збирають і обробляють великий обсяг інформації за запитом клієнтів. Цією діяльністю також займаються підприємства у сфері бізнес-аналітики та моніторингу. Сюди також відносяться довідкові та інформаційні служби, що надають послуги 24/7 підтримки клієнтів у банківській сфері, послуги чат-ботів та віртуальних помічників для компаній, віртуальні помічники та персоналізовані інформаційні сервіси, інформаційна підтримка в e-commerce, вебдослідження та аналіз трафіку тощо.

Доцільність включення виду діяльності за кодом 63.99 «Надання інших інформаційних послуг, н.в.і.у.» до складу ІТ-сфери зумовлена низкою аргументів. По-перше, в умовах цифрової трансформації бізнесу спостерігається розширення спектра інформаційних сервісів, що виходять за межі традиційного програмування або хостингу.

По-друге, значна частина підприємств, що позиціонуються як ІТ-компанії, фактично здійснюють діяльність саме у межах цього коду, надаючи послуги з бізнес-аналітики, обробки великих масивів даних, інформаційної підтримки, автоматизованих консультаційних сервісів, моніторингу та інтерпретації даних у сфері e-commerce, маркетингу, логістики тощо. Такі функції тісно інтегровані з інформаційними технологіями, використовують ІТ-інфраструктуру та персонал з відповідними цифровими компетентностями.

НАЗВА КЛАСУ	ХАРАКТЕРИСТИКА
62.01 Комп'ютерне програмування	Розроблення, модифікація, тестування й технічна підтримка програмного продукту (розроблення структури та контенту та/або розроблення системи команд, необхідних для створення та виконання системного програмного забезпечення, прикладних програм, баз даних, веб-сайтів; налаштування програмного забезпечення, тобто модифікація та конфігурація існуючих програмних додатків таким чином, щоб воно функціонувало в межах інформаційної системи клієнта)
62.02 Консультування з питань інформатизації	Планування та проектування інтегрованих комп'ютерних систем, які поєднують апаратні засоби, програмне забезпечення та комунікаційні технології; ці послуги можуть також включати навчання користувачів цих систем
62.03 Діяльність із керування комп'ютерним устаткуванням	Керування й експлуатація комп'ютерних систем клієнтів та/або засобів оброблення даних таким чином, щоб вони функціонували в межах інформаційної системи клієнта
62.09 Інша діяльність у сфері інформаційних технологій і комп'ютерних систем	Включає послуги, не віднесені до інших категорій, такі як відновлення комп'ютерів після пошкодження, встановлення та налаштування персональних комп'ютерів, інсталяція програмного забезпечення, не пов'язаного з торгівлею комп'ютерною технікою
63.11 Обробка даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність	Надання інфраструктури для хостингу, обробка даних і пов'язана з цим діяльність; надання спеціалізованих послуг з розміщення (хостингу), таких як вебхостинг, потокові послуги, надання простору для розміщення програмних додатків та інші пов'язані послуги
63.12 Веб-портали	Керування вебсайтами, які використовують пошукові механізми для створення та підтримки великих таз даних інтернет-адрес і контенту в зручному для пошуку форматі; керування іншими вебсайтами, що функціонують як портали в Інтернеті, таких як медійні сайти, що періодично поновлюють інформаційний контент
63.99 Надання ін. інформаційних послуг, н.в.і.у.	Інформаційне обслуговування, не включене до інших категорій, із застосуванням комп'ютерних технологій
58.21 Видання комп'ютерних ігор	Видання комп'ютерних ігор для всіх платформ
58.29 Видання ін. програмного забезпечення	Видання стандартного програмного забезпечення, включаючи операційні системи та бізнес-додатки, а також їх переклад та адаптацію

Рис. 1.8. Види економічної діяльності у сфері інформаційних технологій за КВЕД України

Джерело: [72; 74; 105; 221].

У межах нашого дослідження для формування системного уявлення про ІТ-галузь необхідно провести класифікацію суб'єктів, що її формують, адже різні типи підприємств мають різну структуру активів та капіталу, рівень капіталізації, темпи обороту фінансових ресурсів, залежність від зовнішніх ринків тощо [47]. Типологізація ІТ-підприємств також виступає передумовою ухвалення обґрунтованих управлінських рішень у сфері формування системи фінансової безпеки, а також визначення інструментів ідентифікації та нейтралізації ризиків, які можуть становити загрозу для суб'єктів господарювання ІТ-сектору.

Для класифікації ІТ-підприємства в [25] колектив авторів наводить розподіл підприємств ІТ-сфери за типом бізнес-моделі та організаційно-правовими формами.

І. А. Кораблінова та Н. М. Кульбацька надають поділ ІТ-компаній за ознаками блоку управлінських та фінансово-економічних характеристик, виділяючи наступні класифікаційні ознаки: за кількістю працівників, за типом бізнес-моделі, за джерелами фінансування, за формою організації бізнесу, за ринковою орієнтацією компаній та іншими типами характеристик [84].

Лаговська О.А., Лоскоріх Г.Л., з огляду на вимоги до організації бухгалтерського обліку в ІТ-компаніях, наводить їх класифікацію за такими ознаками як: система оподаткування, види проєктів, що виконуються, та замовник [97].

Для кращого розуміння джерел ризиків та загроз, що безпосередньо впливають на формування системи фінансової безпеки ІТ-підприємств ми пропонуємо розглядати класифікацію ІТ-компаній за типом бізнес-моделі, чисельністю працюючих, технологічною спеціалізацією, юридичною формою, джерелами фінансування, географією обслуговування клієнтів та структурою власності (рис. 1.9). Така класифікація дає змогу виявити специфіку формування ризиків в окремих типах ІТ-компаній та визначити рівень їх адаптивності до змін зовнішнього та внутрішнього середовища, а також розробити диференційовані підходи до підвищення рівня фінансової безпеки, враховуючи вид ІТ-компанії [47].

Класифікація підприємств ІТ-сфери	
За типом бізнес-моделі	<ul style="list-style-type: none"> - аутсорсингові компанії – займаються розробленням програмного забезпечення для зовнішнього замовника; - аутстафінгові компанії – надають клієнтам спеціалістів на тимчасовий чи тривалий період; - продуктові компанії – займаються розробленням та продажем власних ІТ-продуктів; - сервісно-продуктові компанії – займаються як розробкою власних продуктів, так і отримують замовлення від зовнішніх контрагентів; - стартап-компанії – нові компанії, які працюють над інноваційними ІТ-рішеннями; - консалтингові компанії – допомагають бізнесу з технологічними рішеннями.
За чисельністю працюючих	<ul style="list-style-type: none"> - мікро підприємства; - малі підприємства; - середні підприємства; - великі підприємства.
За технологічною спеціалізацією	<ul style="list-style-type: none"> - підприємства, що спеціалізуються на штучному інтелекті та машинному навчанні; - підприємства, що працюють у сфері фінансових технологій і блокчейн-розробок; - компанії з кібербезпеки та інформаційного захисту; - підприємства, що працюють з великими даними та аналітичними системами; - компанії, орієнтовані на Інтернет речей (IoT); - постачальники хмарних рішень та сервісів; - розробники розважального програмного забезпечення, ігор, віртуальної та доповненої реальності
За юридичною формою	<ul style="list-style-type: none"> - приватні підприємства; - товариства з обмеженою відповідальністю; - акціонерні товариства.
За джерелами фінансування	<ul style="list-style-type: none"> - підприємства, що фінансуються переважно за рахунок власних коштів; - підприємства, що залучають інвестиції від венчурних фондів та приватних інвесторів; - підприємства, що отримують грантове фінансування на дослідження та розробку продукції; - підприємства, що залучають кредитні ресурси від фінансово-кредитних установ; - підприємства, які отримують фінансову підтримку через моделі колективного інвестування (краудфандинг); - підприємства, що використовують змішане фінансування.
За географією обслуговування клієнтів	<ul style="list-style-type: none"> - локальні підприємства – працюють на внутрішньому ринку України; - експортно орієнтовані підприємства – обслуговують іноземних клієнтів; - підприємства зі змішаним ринком – працюють і в Україні, і за кордоном.
За структурою власності	<ul style="list-style-type: none"> - приватні – підприємства, засновані приватними особами або інвесторами, що володіють переважною часткою у статутному капіталі; - іноземні – підприємства, що перебувають у повній власності нерезидентів; - спільні – підприємства, у яких одночасно присутні як приватні (в тому числі іноземні), так і державні інвестори; - державні або компанії зі значною участю держави – суб'єкти господарювання, які повністю або частково контролюються державними органами.

Рис. 1.9. Класифікація підприємств ІТ-сфери за ознаками, що визначають особливості їх фінансової безпеки

Джерело: [84; 104; 229; 175; 3].

За типом бізнес-моделей виділяють:

- аутсорсингові компанії – здійснюють розробку програмного забезпечення або надання інших ІТ-послуг для зовнішнього замовника. Вони працюють за моделлю, коли замовник делегує їм частину або весь комплекс ІТ-процесів для реалізації чи виконання;

- аутстафінгові компанії – це компанії, що надають замовникам своїх спеціалістів для довготривалого чи тимчасового залучення в їхні проекти. При цьому такі фахівці залишаються у штаті аутстафінгової компанії, яка відповідає за всі кадрові процедури (оформлення, оплату праці, адміністрування тощо);

- продуктові компанії – це підприємства, що самостійно розроблюють та впроваджують власні програмні продукти або ІТ-рішення. Ключовою рисою таких компаній є поєднання в межах одного підприємства всіх етапів життєвого циклу продукту – від ідеї до його комерційного запуску та підтримки користувачів;

- сервісно-продуктові компанії – це компанії, що займаються як розробкою власних продуктів, так і надають ІТ-послуги зовнішнім замовникам;

- стартап-компанії – це новостворені підприємства, які працюють над розробкою та впровадженням інноваційних, але високоризикованих ІТ-продуктів та послуг;

- консалтингові ІТ-компанії – це суб'єкти господарювання, які надають клієнтам експертні консультаційні послуги у сфері ІКТ. Їхня діяльність зазвичай не передбачає створення власних продуктів, а зосереджується на наданні експертизи та консультаційному супроводі клієнтів [104; 25].

Тут варто зазначити, що аутсорсингові, аутстафінгові та консалтингові компанії переважно належать до сервісних компаній, де основним джерелом доходу є надання ІТ-послуг іншим підприємствам та організаціям, а не створення власного продукту. Основна цінність сервісних компаній полягає саме в людських ресурсах та кваліфікації працівників, тоді як успіх продуктових компаній більшою мірою залежить від якості бізнес-моделі,

інноваційності розробок, а також здатності працювати з венчурними фондами та інституційними інвесторами. Хоча, звісно, якість та професіоналізм команди також відіграють важливу роль в ефективності їхньої фінансово-господарської діяльності [104].

В Україні ІТ-компанії можуть реєструватися в різних організаційно-правових формах залежно від розміру бізнесу та форми власності: товариство з обмеженою відповідальністю, акціонерне товариство, приватні підприємства.

З огляду на організацію провадження підприємницької діяльності у вітчизняному ІТ-секторі, особливе місце в ньому займають фізичні особи-підприємці (ФОП). Не зважаючи на те, що ФОП не є юридичною особою, ці суб'єкти господарювання виступають важливою структурною одиницею у сфері інформаційних технологій, особливо в малому ІТ-бізнесі, аутсорсингових послугах та фрилансі. Хоча для індивідуальних підприємців існують певні обмеження в обсягах оборотів, але простота адміністрування, відносно низьке податкове навантаження, спрощена система оподаткування та бухгалтерського обліку робить таку форму ведення бізнесу особливо привабливою для роботи в ІТ-сфері.

ФОП-модель також часто використовується як елемент організаційної структури сервісних ІТ-компаній, де ІТ-спеціалісти офіційно оформлені саме як фізичні особи-підприємці, що дає можливість користуватись перевагами ведення підприємницької діяльності таких суб'єктів господарювання.

З огляду на дослідження особливостей формування системи фінансової безпеки ІТ-підприємств, доцільно виокремити їх класифікацію за структурою власності та джерелами фінансування. У першому випадку підприємства класифікуються за походженням капіталу та рівнем контролю над ними, а у другому – за механізмами надходження фінансових ресурсів для поточної діяльності.

Для вітчизняних ІТ-підприємств доцільною є класифікація за географією обслуговування клієнтів, яка визначає обсяги і структуру валютного виторгу

та ступінь залежності від зовнішніх ринків і, відповідно, впливає на формування системи фінансової безпеки.

Багатьма науковцями [1; 203; 41] підкреслюється, що розвиток цифрової економіки в значній мірі залежить від ефективності функціонування ІТ-сектору, який формує технологічну основу сучасних цифрових змін, які відбуваються практично у всіх сферах суспільно-економічного життя (рис. 1.10). Саме ІТ-підприємства посідають провідне місце в архітектурі цифрової економіки, забезпечуючи створення та впровадження інноваційних технологічних рішень різних сфер господарської діяльності. Вплив ІТ-сектору є визначальним для модернізації управлінських та операційних процесів на державному й корпоративному рівнях, що забезпечує формування нових моделей економічної взаємодії у цифровому середовищі. Наразі ІТ-технології виступають не лише інструментом підвищення ефективності, а й каталізатором структурних змін в економіці.

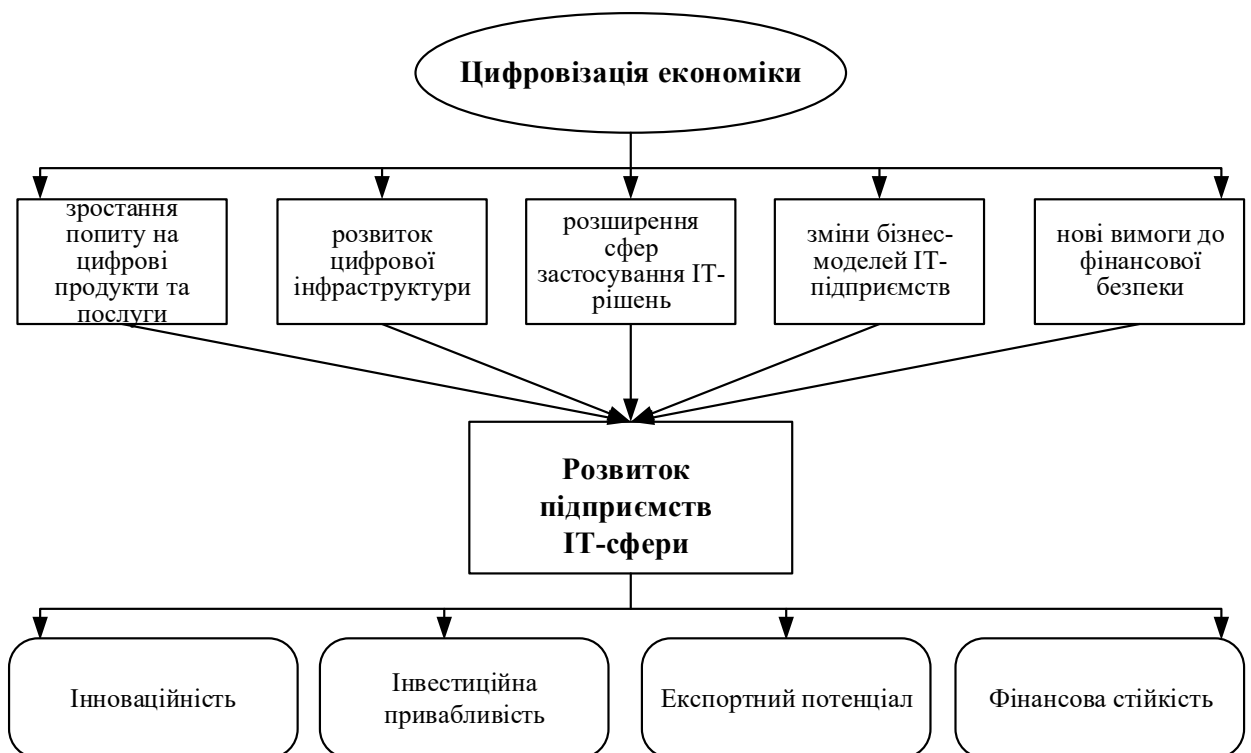


Рис. 1.10. Цифровізація як чинник розвитку підприємств ІТ-сфери

Джерело: складено автором

Ще однією з ключових характеристик ІТ-сектору є мультиплікативний ефект, який він справляє на розвиток інших секторів національної економіки. Цифрові продукти та сервіси, що розроблені ІТ-підприємствами, активно застосовуються у промисловості, сільському господарстві, логістиці, енергетиці, медицині, освіті та сфері послуг, сприяючи модернізації традиційних галузей економіки та посиленню їх конкурентних позицій [203]. На сьогодні ІТ-підприємства виступають активними провайдером цифрових трансформацій, відіграючи провідну роль у формуванні та розвитку цифрової інфраструктури (хмарних обчислень, дата-центрів, телекомунікаційних мереж), розробці цифрових платформ (фінансових, сервісних, галузевих), впровадженні стандартів і забезпеченні технологічної підтримки суб'єктів економіки інших галузей.

Особливо відчутним є вплив ІТ-галузі на розвиток фінансового сектору, де ІТ-рішення стимулюють розвиток фінтех-індустрії, зокрема цифрових банківських послуг, систем електронних платежів, а також таких напрямів, як цифрова ідентифікація клієнтів, RegTech і SupTech-інструменти, краудфандинг, P2P-платформи тощо.

Впровадження інноваційних технологій у діяльність фінансово-кредитних установ сприяє підвищенню ефективності їх функціонування, знижує витрати, підвищує прозорість і швидкість фінансових операцій [203; 190]. Крім того, ІТ-продукти та сервіси стимулюють розвиток систем кіберзахисту у фінансовому секторі, знижуючи ризики фінансових злочинів і шахрайств.

Проте, значення ІТ-галузі полягає не лише у формуванні технологічного фундаменту розвитку цифрової економіки на макрорівні. На сьогодні не менш важливим є роль інноваційних ІТ-рішень в фінансовому управлінні окремих суб'єктів господарювання [142]. При цьому особливої значущості новітні технології набувають в процесі адаптації систем фінансової безпеки підприємств до викликів цифрового середовища. Саме підприємства інформаційно-комунікаційного сектору пропонують інструменти для ефективного управління кіберризиками, забезпечення прозорості фінансових

операцій і підвищення якості фінансового менеджменту в умовах зростаючих зовнішніх та внутрішніх загроз [241; 47].

Як доводить колектив авторів [25], активні процеси цифровізації в усіх секторах вітчизняної економіки створюють сприятливе середовище для динамічного розвитку ІТ-підприємств, стимулюючи попит на їхні продукти та послуги, що сприяє розширенню ІТ-ринку, зростанню інвестиційної привабливості та активному розвитку ІТ-бізнесу в цілому.

Водночас під впливом процесів цифровізації в діяльності самих ІТ-підприємств також відбуваються значні трансформації. Насамперед ці зміни пов'язані з переходом до інноваційних методів фінансового управління, що ґрунтуються на інтеграції цифрових рішень у фінансово-господарську діяльність підприємств. Автоматизація фінансових операцій, використання хмарних сервісів, застосування технологій штучного інтелекту та інструментів аналізу великих даних формують якісно нові можливості для оптимізації витрат, підвищення прозорості фінансових потоків, удосконалення фінансового планування та контролінгу, своєчасного виявлення та мінімізації фінансових ризиків тощо [103; 121].

Поряд з позитивними зрушеннями цифровізація створює і додаткові виклики, що пов'язані з кібербезпекою, захистом даних, ускладненням регуляторних вимог у цифровому середовищі та зростанням вимог до інформаційної безпеки. Це посилює значення спеціалізованих продуктів ІТ-сектору, що застосовуються для забезпечення прозорості, надійності та безпеки фінансово-господарських процесів у різних галузях економіки [103].

Отже, узагальнюючи викладене, можемо констатувати, що диджиталізація та розвиток ІТ-підприємств формують єдиний взаємопов'язаний і синергійний процес: цифрові технології стимулюють розвиток ІТ-сектору, який своєю чергою забезпечує подальшу еволюцію цифрової економіки (рис. 1.11). Тобто цифровізація виступає не лише чинником технологічного та економічного зростання підприємств ІТ-сфери, а й результатом активної діяльності самих ІТ-компаній, що стають головними драйверами сучасних цифрових трансформацій в економіці.

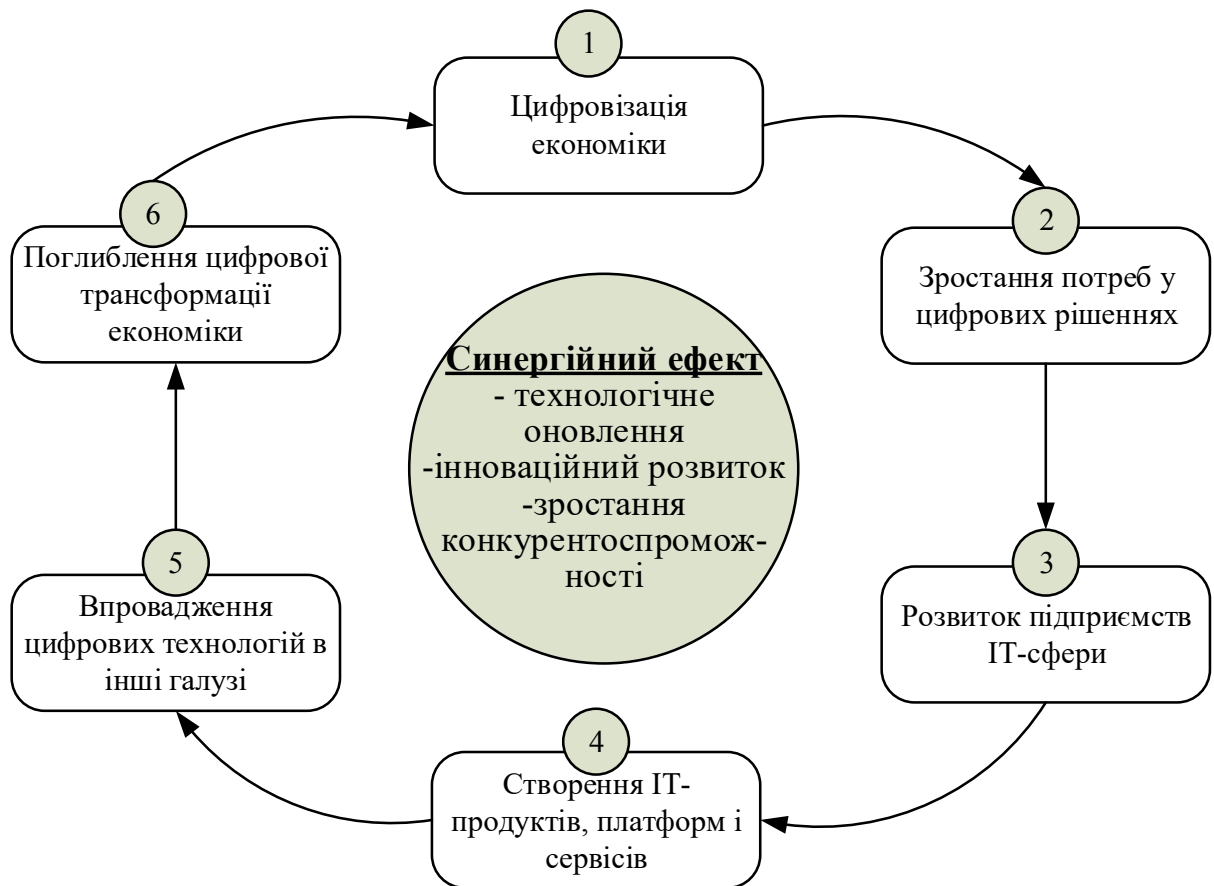


Рис. 1.11. Взаємозв'язок розвитку ІТ-бізнесу та цифрової трансформації економіки

Джерело: складено автором

Розуміння цього взаємозв'язку виступає важливим чинником формування ефективної державної політики у сфері цифрової трансформації, підтримки ІТ-підприємств, розвитку ІТ-кластерів і стартап-екосистеми, а також забезпечення фінансової стабільності та дієвих механізмів фінансування вітчизняного ІТ-сектору [103]. Роль ІТ-підприємств у цифровій економіці представлена на рис. 1.12.

Для подальшого дослідження системи фінансової безпеки підприємств ІТ-сфери важливим є розуміння специфіки їх економічної діяльності, яка суттєво відрізняється від традиційних виробничих підприємств чи підприємств сфери послуг.

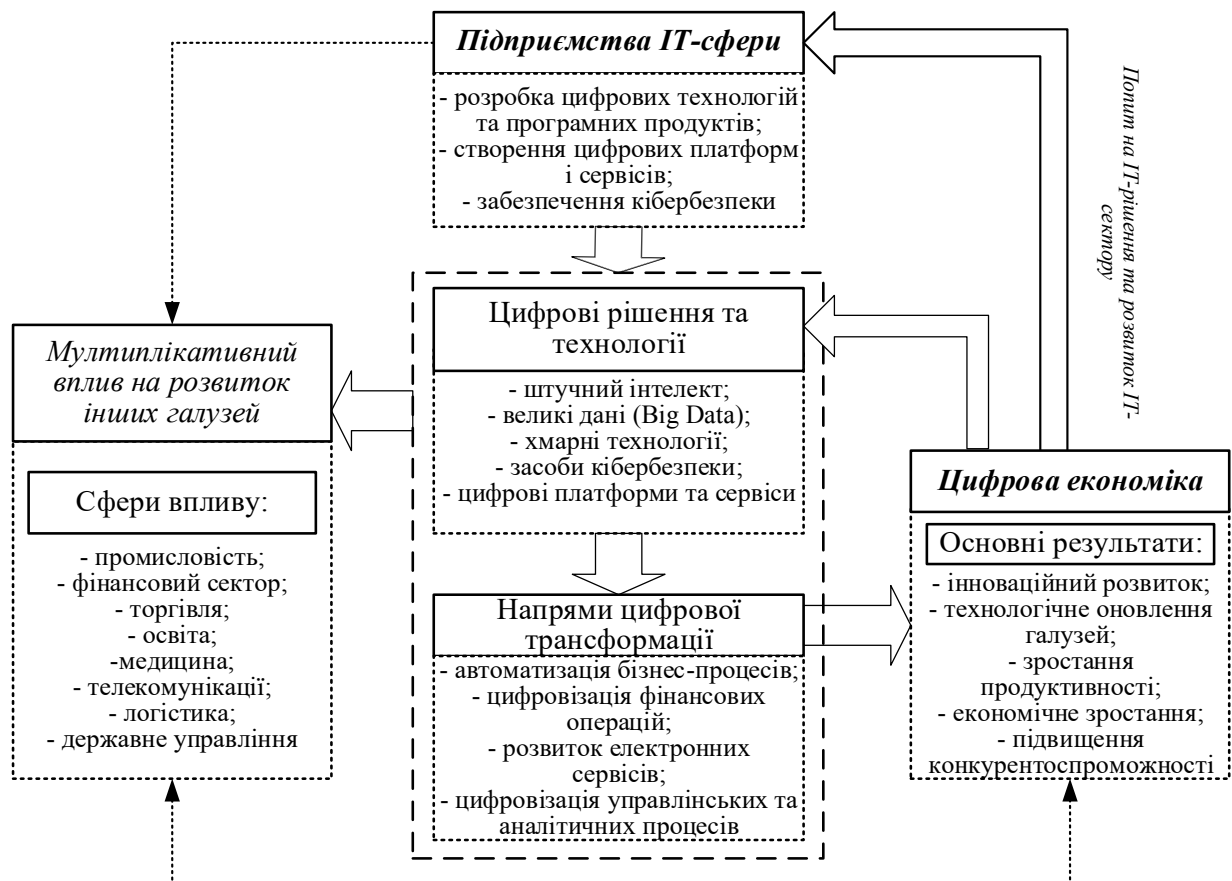


Рис. 1.12 Роль підприємств ІТ-сфери у розвитку цифрової економіки

Джерело: складено автором.

Виявлення цих особливостей дозволить надалі окреслити унікальний спектр викликів і загроз для формування дієвого механізму забезпечення фінансової безпеки підприємств ІТ-сфери у цифровому середовищі. Отже, серед основних специфічних рис економічної діяльності ІТ-підприємств можна виділити такі:

- інтелектуально-нематеріальний характер створюваних ІТ-продуктів та послуг, за якого основна економічна цінність формується за рахунок інтелектуальної власності, програмних рішень і знань персоналу, а не матеріальних активів;

- цифрова форма продуктів та бізнес-процесів ІТ-підприємств підвищує ризики кібератак, несанкціонованого доступу до даних, порушення прав інтелектуальної власності та витоку комерційної таємниці;

- проєктна модель організації діяльності ІТ-підприємств, за якої господарські процеси реалізуються через окремі проєкти, що мають визначені цілі, строки, бюджет, склад команди та очікувані результати;
- високі темпи інноваційного розвитку ІТ-сфери, що зумовлюють постійну потребу у вдосконаленні продуктів і технологій, значні витрати на проведення науково-дослідних і дослідно-конструкторських робіт (R&D) та підвищену залежність ІТ-підприємств від інтелектуального капіталу;
- домінування людського капіталу в структурі ресурсів ІТ-підприємств, що зумовлює пряму залежність результатів діяльності від кваліфікації, досвіду та продуктивності праці ІТ-фахівців;
- висока частка нематеріальних витрат у структурі собівартості, зокрема витрат на оплату праці, дослідження і розробки, маркетинг та кіберзахист;
- висока чутливість фінансових результатів до змін витрат на персонал, оскільки фонд оплати праці становить основну частку витрат ІТ-підприємств, а навіть незначні зміни умов зайнятості або податкового навантаження безпосередньо впливають на собівартість та рентабельність їхньої діяльності;
- використання альтернативних підходів до організації праці, що реалізуються через застосування різних форм зайнятості, зокрема дистанційну роботу, гіг-контракти, співпрацю з фізичними особами-підприємцями, а також моделей аутсорсингу та аутстафіngu;
- експортноорієнтований характер діяльності значної частини вітчизняних ІТ-підприємств, який визначає особливості економічних зв'язків, валютну структуру доходів та залежність від кон'юнктури міжнародних ринків;
- обмежена матеріальна база та складність залучення традиційного банківського фінансування, зумовлена домінуванням нематеріальних активів у структурі ресурсів ІТ-підприємств, що ускладнює використання класичних інструментів кредитування і підвищує роль альтернативних джерел фінансування;

- висока швидкість обороту фінансових ресурсів, що пов'язана з цифровою природою продуктів, відносно коротким виробничим циклом, а також широким застосуванням моделей підписки та програмного забезпечення як послуги (SaaS);

- високий рівень залежності фінансових результатів ІТ-підприємств від стабільності клієнтської бази та довгострокових контрактів, особливо при використанні сервісних і підписних бізнес-моделей;

- нерівномірність динаміки доходів і витрат на різних етапах розвитку ІТ-компанії, коли на початкових стадіях витрати випереджають доходи, тоді як у фазі розширення діяльності можливе стрімке зростання фінансових результатів діяльності [25; 78; 117; 127; 124; 219].

Таким чином, виявлені специфічні риси економічної діяльності ІТ-підприємств безпосередньо впливають на фінансову складову їх функціонування. Особливості економічного середовища ІТ-сектору формують унікальний спектр фінансових викликів і загроз, що відрізняють цю галузь від традиційних секторів економіки. Проектний формат роботи, орієнтація на глобальні ринки, залежність від людського капіталу та цифрових ресурсів, безпосередньо впливають на структуру фінансових потоків та рівень ризиків ІТ-підприємств (рис. 1.13), зумовлюють особливу модель фінансових відносин, що потребує адаптивних інструментів фінансового планування і контролю та необхідність модернізації системи забезпечення фінансової безпеки підприємств ІТ-сфери.

Виявлені специфічні риси економічної діяльності ІТ-підприємств свідчать про їх підвищену чутливість до змін зовнішнього та внутрішнього середовища, що безпосередньо впливає на рівень фінансової стійкості та безпеки таких суб'єктів господарювання.



Рис. 1.13. Галузеві особливості ІТ-підприємств як чинники формування системи фінансової безпеки

Джерело: складено на основі: [25; 78; 86; 117; 127; 221].

У зв'язку з цим доцільним є виокремлення та систематизація зовнішніх і внутрішніх факторів розвитку ІТ-підприємств (табл. 1.1), розгляд яких дозволить в подальшому оцінити потенційні загрози й можливості для забезпечення їх фінансової безпеки в умовах цифрової економіки [47].

Таблиця 1.1

Зовнішні фактори розвитку підприємств ІТ-сфери

Фактори	Характеристика
Нормативно-правові	<ul style="list-style-type: none"> - прозорість та стабільність законодавства; - податкова та фінансова політика; - правовий захист ІТ-продуктів та інтелектуальної власності; - державне регулювання у сфері кібербезпеки; - нормативно-правове забезпечення цифрового розвитку; - державна інноваційна політика; - інституційна підтримка експорту та залучення інвестицій.
Економічні	<ul style="list-style-type: none"> - стабільність національної валюти та валютне регулювання; - рівень інфляції; - загальний рівень економічного розвитку; - конкурентне середовище на ринку ІТ-послуг та продуктів; - доступність фінансових ресурсів (умови кредитування, відсоткові ставки); - розвиненість страхових і фінансових інструментів для ІТ-компаній; - експортний потенціал ІТ-сфери (доступ до зовнішніх ринків, можливість експорту ІТ-послуг, імідж країни).
Політичні	<ul style="list-style-type: none"> - стабільність політичного середовища; - безпекова ситуація в країні; - рівень геополітичної стабільності; - міжнародні санкції та обмеження.
Технологічні	<ul style="list-style-type: none"> - рівень розвитку цифрової інфраструктури (доступ до хмарних сервісів, дата-центрів, швидкісного інтернету); - рівень розвитку систем кібер- та інформаційної безпеки; - наявність технологічних хабів, технопарків та інноваційної інфраструктури; - кадрово-технологічний потенціал ІТ-сфери (інтеграція ІТ-бізнесу з науково-освітнім середовищем, академічна підтримка інновацій); - функціонування та рівень розвитку ІТ-кластерів, державно-приватних партнерств.
Соціальні	<ul style="list-style-type: none"> - рівень кваліфікації та професійної підготовки робочої сили; - стан ринку праці та рівень безробіття; - рівень доходів населення та платоспроможного попиту; - міграційні процеси; - рівень цифрової компетентності населення (цифрова грамотність та культура).

Джерело: [91; 152; 162; 210].

Такий підхід особливо актуальний в умовах вітчизняних реалій, коли на тлі військових, економічних і демографічних викликів ІТ-сектор потребує не лише ефективного внутрішнього фінансового управління окремими суб'єктами господарювання, а й розробки механізмів системної підтримки ІТ-галузі з боку держави в умовах цифрових трансформацій [47].

Як зазначається в працях Завгородньої Є. О., Шестак Є. І., Ільчука В. П., Устинова Я. В. та ін., розвиток підприємств ІТ-сфери значною мірою визначається дією комплексу зовнішніх чинників, які формують інституційне, економічне та технологічне середовище їх функціонування, впливаючи на конкурентоспроможність, інвестиційну привабливість, фінансову стійкість та здатність до інноваційного зростання в умовах цифрової економіки [276; 209].

Зокрема, нормативно-правове середовище визначає правила ведення ІТ-бізнесу та характер взаємодії між державою і суб'єктами ринку ІТ-послуг в Україні. Прозорість і передбачуваність законодавства, податкові умови, дієва інституційна підтримка експортної діяльності ІТ-компаній, наявність сприятливої правової бази для захисту прав інтелектуальної власності й забезпечення цифрової безпеки є критично важливими для залучення інвестицій в ІТ-сферу, збереження людського потенціалу, підвищення конкурентоспроможності ІТ-підприємств та забезпечення їхньої довгострокової фінансової стійкості [117].

Не менш суттєвий вплив на розвиток ІТ-підприємств здійснює загальноекономічна ситуація в країні, яка визначає базові економічні умови функціонування ІТ-сектору, реалізації інвестиційних проєктів та формування фінансових ресурсів. Макроекономічна стабільність, доступність фінансових ресурсів, стан кредитного ринку, валютна політика, інвестиційна активність, а також спроможність держави щодо підтримки високотехнологічних галузей безпосередньо визначають темпи розвитку ІТ-бізнесу та його інвестиційну привабливість [47].

Соціальний вимір впливу зовнішнього середовища проявляється передусім через стан та якість людського капіталу. Значення людського капіталу в процесах цифрової трансформації підтверджується дослідженнями Чупілка О. С., які підкреслюють важливість інвестицій у розвиток кадрів для підвищення ефективності ІТ-підприємств [222]. Рівень професійної підготовки ІТ-фахівців, цифрова грамотність населення, демографічні та міграційні процеси визначають особливості ринку праці та кадровий потенціал галузі. Оскільки саме людський капітал є одним із основних ресурсів ІТ-галузі, його якість та доступність визначають можливості для її фінансово стійкого розвитку.

Погоджуємося з думкою Міщенко В. І., який наголошує, що вагомий вплив на розвиток ІТ-підприємств має також технологічне середовище, яке охоплює насамперед рівень розвитку цифрової інфраструктури, доступ до сучасних технологічних рішень та засобів кіберзахисту. Саме ці чинники формують технологічну базу для активізації інноваційної діяльності підприємств ІТ-сфери, створення та комерціалізації нових конкурентоспроможних ІТ-продуктів та послуг [127].

Не менш важливим є те, що впровадження хмарних платформ, автоматизованих систем управління бізнес-процесами та фінансами (ERP, CRM та ін.), рішень у сфері кібербезпеки, технологій штучного інтелекту, інструментів аналітики великих даних сприяє підвищенню ефективності операційної та фінансової діяльності, зниженню ризиків, а також визначає здатність ІТ-компаній забезпечувати захист фінансово-господарської діяльності в цифрову епоху [13; 151].

Внутрішні чинники розвитку ІТ-підприємств (табл. 1.2) безпосередньо формуються всередині компанії та пов'язані з особливостями її організаційної побудови, системи управління та формування і використання матеріальних, фінансових, трудових та інтелектуальних ресурсів. В умовах інтенсивної технологічної трансформації саме внутрішній потенціал визначає здатність суб'єкта господарювання ефективно функціонувати на ринку цифрових послуг, забезпечувати стабільність фінансових результатів та підтримувати належний рівень фінансової безпеки [47].

Внутрішні фактори розвитку підприємств ІТ-сфери

Фактори	Характеристика
Технологічні та цифрові	<ul style="list-style-type: none"> - рівень використання сучасних цифрових інструментів (AI, Big Data, IoT, блокчейн та ін.); - рівень розвитку та надійності цифрової та ІТ-інфраструктури (хмарні сервіси, внутрішні платформи, технічне забезпечення); - автоматизація та роботизація бізнес-процесів; - рівень інформаційної безпеки та кіберзахисту; - стан матеріально-технічної бази.
Фінансово-економічні	<ul style="list-style-type: none"> - ефективне фінансове планування та бюджетування; - ефективність управління витратами та рівень прибутковості; - оптимальне співвідношення власного та залученого капіталу; - інвестиційна привабливість та рівень інвестиційної активності; - можливість залучення зовнішнього фінансування; - наявність внутрішніх фінансових резервів та механізмів страхового захисту.
Інноваційні	<ul style="list-style-type: none"> - рівень інтеграції новітніх інформаційно-комунікаційних технологій; - здатність до інноваційних розробок та впровадження унікальних ІТ-рішень; - швидкість впровадження інновацій.
Кадрові	<ul style="list-style-type: none"> - рівень професійної підготовки команди; - кадрова політика та система мотивації персоналу; - стабільність кадрового складу (рівень плинності кадрів); - система навчання, підвищення кваліфікації та розвитку персоналу.
Організаційно-управлінські	<ul style="list-style-type: none"> - гнучкість та оперативність управлінських рішень; - цифровізація управлінських процесів; - якість управлінських рішень в сфері фінансового менеджменту; - ефективна система контролю; - корпоративна культура та внутрішні комунікації; - наявність системи управління ризиками.
Маркетингові	<ul style="list-style-type: none"> - ринкове позиціонування ІТ-підприємства; - наявність і ефективність маркетингової стратегії; - активність у цифровому маркетингу; - підтримка та розвиток клієнтської бази; - впізнаваність бренду та ділова репутація.

Джерело: [78; 117; 180; 198; 210].

Як зазначено в дослідженнях, присвячених розвитку ІТ-сектору, стрімкий технологічний прогрес, посилення ринкової турбулентності й нові кіберзагрози суттєво ускладнюють діяльність ІТ-підприємств і підвищують роль внутрішніх управлінських рішень у забезпеченні їхньої фінансової стійкості [151; 219; 25].

Стратегічно орієнтоване фінансове управління внутрішніми ресурсами та бізнес-процесами підприємств ІТ-сфери, що забезпечує ефективний розвиток інноваційного, фінансового, технологічного і кадрового потенціалу, є запорукою фінансової стійкості ІТ-підприємств і здатності протистояти внутрішнім та зовнішнім викликам цифрового середовища.

З огляду на специфіку діяльності ІТ-компаній, серед внутрішніх факторів їхнього розвитку визначальну роль відіграють фінансові, інноваційні, технологічні та кадрові чинники, які мають переважний вплив на фінансовий стан та рівень фінансової безпеки [47].

Одним із головних внутрішніх чинників розвитку ІТ-підприємств є рівень розвитку їх технологічної бази, оскільки саме вона забезпечує не лише ефективність операційної діяльності та автоматизацію бізнес-процесів, а і знижує вразливість суб'єкта господарювання до зовнішніх фінансових, інформаційних та кіберзагроз. У сучасних умовах цифрової економіки технологічна спроможність підприємства дедалі частіше виступає важливим елементом системи його фінансової безпеки, що підтверджується результатами досліджень у сфері фінансово-економічної безпеки та цифрової трансформації [37; 121; 178].

Як зазначалось вище, не менш важливу роль у забезпеченні фінансової стійкості ІТ-підприємств відіграє їх кадровий потенціал. Рівень кваліфікації ІТ-фахівців, наявність ефективної системи навчання, розвитку та мотивації персоналу безпосередньо визначають якість створюваних цифрових продуктів і послуг. Готовність персоналу до впровадження інновацій та його здатність своєчасно реагувати на нові потреби ринку забезпечує зростання конкурентоспроможності ІТ-підприємства та посилення позицій на внутрішньому та міжнародному ринках.

Отже, можемо констатувати, що розвиток та фінансова стійкість ІТ-підприємств ґрунтуються на комплексній взаємодії внутрішніх і зовнішніх чинників, починаючи з регуляторного середовища й закінчуючи ефективною

фінансовою політикою конкретного суб'єкта господарювання. І навіть незначні зміни окремих факторів можуть істотно впливати на фінансові результати та фінансову стійкість ІТ-бізнесу.

Узагальнення наведених положень дозволяє стверджувати, що система фінансової безпеки підприємств ІТ-сфери формується під впливом не лише загальних фінансово-економічних чинників, характерних для більшості суб'єктів господарювання, а й специфічних галузевих детермінант. На відміну від традиційних підприємств, для яких фінансова безпека переважно пов'язується із забезпеченням платоспроможності, фінансової стійкості, прибутковості та раціональної структури капіталу, підприємства ІТ-сфери функціонують в умовах підвищеної ролі нематеріальних ресурсів, інтелектуальної власності, цифрових активів і кіберстійкості. Це зумовлює формування специфічного ризик-профілю, у межах якого фінансові ризики тісно поєднуються з кадровими, інноваційними, інфраструктурними, валютними, регуляторними та кіберризиками. Це дозволяє простежити, яким чином особливості діяльності ІТ-підприємств трансформуються у фінансові виклики та ризики, визначають напрями управлінського впливу і формують потребу в адаптивній системі фінансової безпеки (рис. 1.14).

З огляду на вищезазначене, ефективне фінансове управління суб'єктами ІТ-бізнесу дозволяє підприємствам вчасно реагувати на мінливість внутрішнього та зовнішнього середовища. Саме тому подальший аналіз доцільно зосередити на особливостях фінансового управління на ІТ-підприємствах, які визначають здатність таких суб'єктів господарювання не лише ефективно використовувати фінансові ресурси, а й забезпечувати належний рівень фінансової безпеки в умовах цифрової економіки.

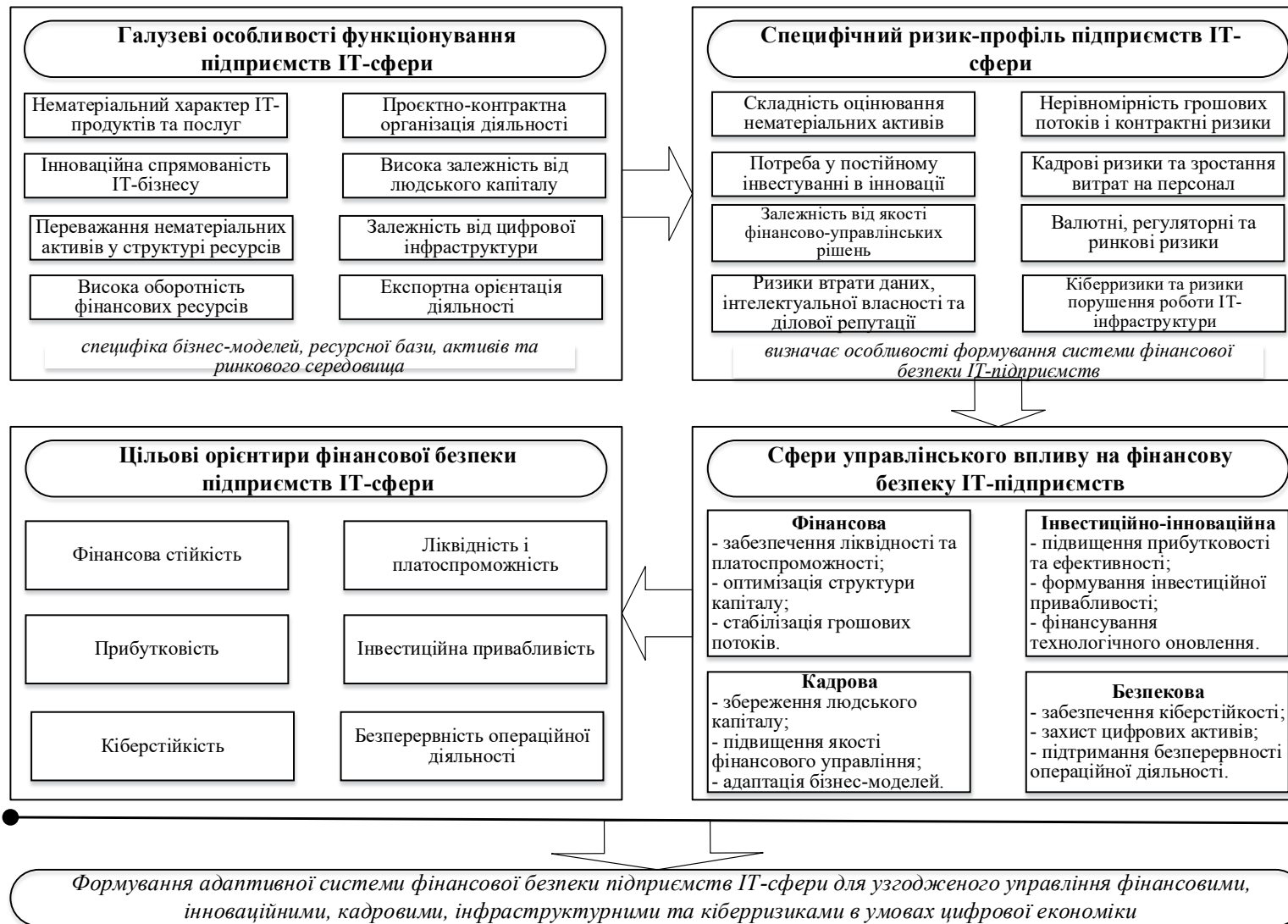


Рис. 1.14. Галузеві детермінанти формування системи фінансової безпеки підприємств ІТ-сфери

Джерело: складено автором.

Стрімка диджиталізація, глобалізація ринків та зростання ризиків цифрового середовища зумовлюють необхідність переосмислення підходів до фінансового управління ІТ-підприємствами. Традиційні методи фінансового менеджменту дедалі частіше виявляються недостатніми для ефективної роботи в умовах високої динамічності ринку, нестабільності зовнішнього середовища та посилення фінансових ризиків та кіберзагроз.

Беззаперечним є той факт, що саме фінансові рішення визначають здатність ІТ-підприємств забезпечувати фінансову стійкість, ліквідність та захищеність бізнесу від зростаючих загроз. У зв'язку з цим доцільно виокремити характерні особливості фінансового управління ІТ-підприємствами, що мають принципове значення для формування ефективної системи їх фінансової безпеки, а саме:

- фінансове управління ІТ-підприємств вимагає урахування зовнішньоекономічної орієнтації діяльності та високої частки експортних операцій вітчизняних ІТ-компаній, що зумовлює потребу в ефективному валютному плануванні, хеджуванні валютних ризиків та курсових коливань, а також ефективному супроводі міжнародних контрактів;

- домінування власних коштів засновників як основного джерела фінансових ресурсів ІТ-підприємств, особливо на початкових етапах розвитку, підвищує роль внутрішнього фінансового планування, контролю за ліквідністю та зваженого управління капіталом за умов обмежених резервів;

- висока частка витрат на оплату праці кваліфікованого персоналу, яка в ІТ-сфері складає від 60 до 80 % усіх операційних витрат, потребує побудови гнучкої системи бюджетування заробітної плати, бонусних та мотиваційних програм, інвестування в розвиток персоналу та соціального пакету;

- суттєва залежність фінансової стійкості ІТ-підприємств від людського капіталу формує потребу у фінансових інструментах, здатних враховувати ризики втрати ключових працівників (особливо в умовах війни), їх заміни, витрати на навчання та адаптацію персоналу, що ускладнює довгострокове фінансове планування;

– переважання нематеріальних витрат у структурі бюджету ІТ-підприємств (оплата праці, R&D, маркетинг, кібербезпека) ускладнює фінансовий контроль, оскільки результати таких витрат не завжди одразу проявляються у фінансових показниках. У багатьох випадках їх економічний ефект має відкладений характер або проявляється опосередковано, що потребує застосування спеціальних підходів до оцінки ефективності використання фінансових ресурсів;

– висока гнучкість бізнес-моделей ІТ-підприємств, що поєднує аутсорсинг, аутстафінг, продаж власних продуктів, платформні моделі, ускладнює прогнозування грошових надходжень та потребує цифрових аналітичних інструментів для управління фінансовими потоками, здатного оперативно реагувати на зміну клієнтської поведінки та ринкових умов;

– використання різних моделей співпраці з ІТ-фахівцями (ФОП, гіг-контракти та ін.) потребують належного податкового обліку, оптимізації податкових витрат та постійного моніторингу змін податкового законодавства;

– динамічні зміни у правовому середовищі щодо вітчизняного ІТ-сектору вимагають від фінансового менеджменту стратегічної гнучкості, адаптації систем бюджетування й податкового планування до нових регуляторних умов і мінливих вимог державної політики;

– проєктна форма організації роботи, характерна для ІТ-компаній, потребує детального фінансового планування за кожним проєктом, контролю його рентабельності, а також управління ризиками на всіх етапах життєвого циклу окремих проєктів чи продуктів;

– постійна потреба в інвестиціях у дослідження та розробки, зумовлена високими темпами технологічного розвитку, вимагає застосування довгострокового інвестиційного аналізу, комплексної оцінки ризиків і прогнозування майбутньої віддачі від вкладень в інновації;

– наявність у ІТ-підприємств значного обсягу нематеріальних активів, потребує їх належного захисту від кіберризиків, тому управління такими активами має бути інтегрованим елементом системи забезпечення фінансової безпеки;

– низька капіталомісткість і домінування нематеріальних активів в структурі активів ІТ-підприємств ускладнюють їх облік і оцінку ринкової вартості компанії, що потребує застосування нестандартних підходів до фінансового аналізу та управління інтелектуальною власністю, а також врахування нематеріальних чинників при плануванні інвестиційної політики;

– нерівномірність грошових потоків у ІТ-сфері, що пов'язана з використанням моделей передоплати, підписки або проєктної оплати, потребує гнучкого управління ліквідністю та постійного прогнозування грошових надходжень з метою забезпечення платоспроможності підприємства;

– обмежений доступ до традиційного банківського кредитування, спричинений нестачею матеріальних активів як застави, змушує ІТ-підприємства орієнтуватися на альтернативні джерела фінансування – венчурний капітал, гранти, кошти міжнародних партнерів тощо.

– залучення венчурного фінансування, грантів і контрактних форм співпраці потребує від ІТ-підприємств підтримання належного рівня фінансової стійкості, ліквідності та інвестиційної привабливості;

– широке використання цифрових платформ, автоматизованих систем і FinTech-рішень у фінансовому управлінні підвищує ефективність бюджетування, обліку і фінансового контролю, але водночас створює нові кіберзагрози, що потребує інтеграції фінансового менеджменту та систем інформаційної безпеки;

– фінансове управління ІТ-підприємствами ускладнюється нерівномірністю потреб у фінансових ресурсах на різних етапах розвитку: на початкових стадіях домінують інвестиційні витрати, тоді як на етапі масштабування зростання доходів відбувається без пропорційного збільшення витрат, що змінює вимоги до управління рентабельністю та ліквідністю;

– характер і складність фінансової діяльності ІТ-компаній залежить від її розміру, орієнтації на внутрішні або міжнародні ринки та особливостей корпоративного управління, що безпосередньо впливає на складність фінансових процесів і вимоги до професійних компетенцій фінансового менеджменту [3; 107; 145; 150; 152; 209; 210].

Таким чином, у межах підрозділу 1.2 здійснено комплексний аналіз концептуальних особливостей функціонування підприємств ІТ-сфери в умовах цифрової економіки. Обґрунтована зростаюча роль ІТ-підприємств в процесах цифровізації та встановлено, що ІТ-компанії є невід'ємними складовими процесу становлення цифрової економіки, які фактично формують його інноваційне ядро.

З метою формування цілісного бачення об'єкта дослідження уточнено межі ІТ-галузі України та проведено класифікацію ІТ-компаній за рядом ознак: за типом бізнес-моделі, чисельністю працюючих, технологічною спрямованістю, організаційно-правовими формами, структурою власності, географією обслуговування клієнтів і джерелами фінансування. Така типологізація дозволяє диференціювати ІТ-підприємства за характером грошових потоків, рівнем залежності від зовнішніх ринків, валютних ризиків, особливостями формування фінансової безпеки тощо.

Проведено узагальнення та систематизацію основних особливостей економічної діяльності ІТ-підприємств в умовах цифрової економіки, що принципово відрізняють їх від суб'єктів господарювання традиційних галузей економіки. Це дозволило встановити, що саме ці особливості формують специфічні умови функціонування ІТ-бізнесу, визначають особливий ризик профіль ІТ-підприємств та зумовлюють підвищену чутливість його фінансових результатів до впливів зовнішніх та внутрішніх умов.

Дослідження внутрішніх і зовнішніх чинників розвитку ІТ-підприємств дозволило дійти висновку, що фінансова стійкість і безпека таких суб'єктів господарювання формуються під впливом складної взаємодії регуляторного,

макроекономічного, соціального та технологічного середовища з внутрішнім фінансовим, кадровим, інноваційним і управлінським потенціалом ІТ-компаній. При цьому саме внутрішні чинники (ефективність управління фінансовими ресурсами, людським капіталом і цифровими активами) відіграють головну роль у забезпеченні адаптації ІТ-підприємств до змін зовнішнього середовища.

Встановлено, що окреслені особливості економічної діяльності безпосередньо впливають на зміст і логіку фінансового управління ІТ-підприємствами. Фінансова діяльність таких компаній характеризується домінуванням нематеріальних витрат, асиметрією потреб у фінансових ресурсах на різних етапах життєвого циклу, нестабільністю грошових потоків, обмеженим доступом до традиційного банківського кредитування та поширенням альтернативних джерел фінансування. Це зумовлює необхідність застосування гнучких підходів до фінансового планування, управління ліквідністю, ризиками та інвестиційними процесами, а також посилює роль фінансового менеджменту у забезпеченні стабільності функціонування ІТ-підприємств.

Узагальнення результатів дослідження дозволило обґрунтувати доцільність використання системного підходу до формування системи фінансової безпеки підприємств ІТ-сфери з урахуванням їх галузевої специфіки, специфічного ризик-профілю, сфер управлінського впливу та цільових орієнтирів фінансової безпеки. Отримані висновки створюють теоретико-методичне підґрунтя для подальшого дослідження системи фінансової безпеки ІТ-підприємств, що буде здійснено в наступному підрозділі дисертаційної роботи.

1.3. Теоретичні засади формування системи фінансової безпеки підприємств ІТ-сфери

У сучасних умовах цифрової трансформації економіки зростає значення забезпечення фінансової безпеки підприємств, що функціонують у високотехнологічних секторах. Як було визначено в попередньому підрозділі, для підприємств ІТ-сфери характерним є домінування інтелектуальних і нематеріальних активів, проєктний характер виробництва, висока залежність фінансових результатів від людського капіталу, експортна орієнтація, тісна інтеграція у глобальне цифрове середовище та ін. Зазначені особливості зумовлюють підвищену чутливість ІТ-підприємств до впливів зовнішнього середовища, цифрових ризиків і кіберзагроз, а також до змін регуляторних і макроекономічних умов. Саме тому виникає необхідність застосування системного підходу до формування та забезпечення фінансової безпеки підприємств ІТ-сфери, що враховує різноплановість зовнішніх та внутрішніх загроз, а також усіх аспектів фінансово-господарської діяльності таких суб'єктів господарювання.

Актуальність системного підходу до формування фінансової безпеки підприємств ІТ-сфери підтверджується сучасними науковими дослідженнями. Зокрема, Н. М. Пантелєєва зазначає, що в умовах цифрової економіки фінансова безпека набуває нових характеристик, пов'язаних зі зростанням залежності фінансових результатів від цифрових технологій, захисту даних і стійкості цифрової інфраструктури, що потребує переосмислення традиційних підходів до її забезпечення [144].

З огляду на вищезазначене в дисертаційній роботі фінансову безпеку підприємств ІТ-сфери пропонуємо розглядати як системну категорію, що забезпечить:

- комплексне бачення фінансової безпеки підприємств ІТ-сфери як складної багаторівневої системи із внутрішніми та зовнішніми взаємозв'язками;

- системний підхід до виявлення ключових загроз фінансової безпеки з урахуванням специфіки цифрового середовища та галузевих особливостей ІТ-бізнесу;

- урахування взаємозв'язків між компонентами системи з огляду на складний характер фінансової безпеки як явища, що формується під впливом як внутрішніх, так і зовнішніх факторів;

- урахування взаємозалежності між специфікою фінансово-економічної діяльності підприємств ІТ-сектору та рівнем їхньої фінансової безпеки;

- можливість виявлення вузьких місць фінансової системи підприємства, включаючи новітні ризики цифрової економіки;

- урахування фінансових, кадрових, інформаційних та кіберзахисних складових у процесі формування системи фінансової безпеки ІТ-підприємств;

- формування теоретичних передумов для підвищення ефективності фінансових управлінських рішень на макро- та мікрорівнях.

Генезис системного підходу пов'язують із серединою ХХ ст., коли він виокремився як загальнонаукова методологія пізнання, що сформувалась під впливом загальної теорії систем австрійського вченого Л. фон Берталанфі [123].

Глибокий інтерес до концептуальних засад системного підходу з боку представників різних галузей наук зумовив його широке застосовування в багатьох сферах (філософії, техніці, біології, соціології, економіці та ін.).

Як зазначають [123], у загальному розумінні системний підхід виступає методологічним напрямом наукового пізнання, що передбачає вивчення будь-якого об'єкта через його трактування як цілісної системи. У цьому контексті постає необхідність уточнення змісту ключового об'єкта дослідження - категорії «система». У сучасному науковому дискурсі існує значна кількість трактувань цього поняття, частину з яких представлено на рис. 1.15.

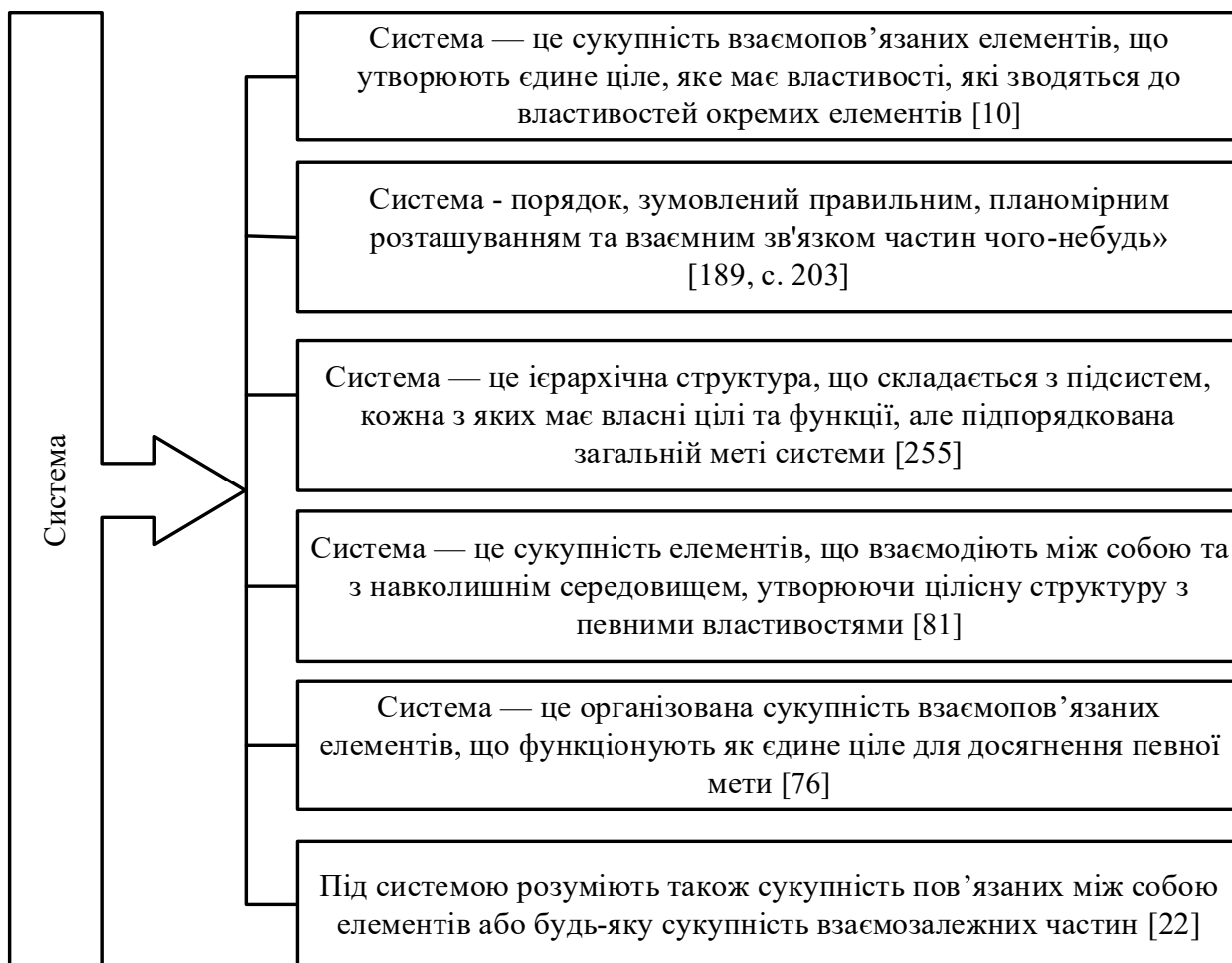


Рис. 1.15. Сутність поняття «система»

Джерело: складено автором.

Тепер, спираючись на результати наших попередніх досліджень, розглянемо сутність поняття «система фінансової безпеки підприємства». Слід зазначити, що воно в науковій літературі трапляється не так часто, а існуючі підходи до його трактування відрізняються за змістовним наповненням та акцентами досліджень.

Так, В. І. Фучеджи зазначає, що «система фінансової безпеки – це організована сукупність спеціальних органів, коштів, методів, заходів, що забезпечують захист діяльності від впливу внутрішніх і зовнішніх загроз» [214]. У цьому визначенні увага зосереджена лише на органах, методах і заходах забезпечення фінансової безпеки, що більше наближує його до трактування механізму її забезпечення, тоді як структура та взаємозв’язках між елементами системи залишаються поза увагою.

Подібний підхід простежується і в працях Козаченко Г. В., Пономарьов В. П., Ляшенко О. М., які розглядають систему фінансової безпеки підприємства як «комплекс взаємозв'язаних заходів організаційно-правового характеру, що здійснюються спеціальними органами, службами, підрозділами суб'єкта господарювання, спрямованих на захист життєво важливих інтересів особистості, підприємства й держави від протиправних дій з боку реальних або потенційних фізичних або юридичних осіб, що можуть призвести до істотних економічних утрат та забезпечення економічного зростання в майбутньому» [79], де також акцент зроблено переважно на заходах забезпечення фінансової безпеки.

Найбільш повне, на нашу думку, визначення надає Т. В. Ганущак, який зазначає, що «система фінансової безпеки підприємства – це сукупність внутрішніх і зовнішніх суб'єктів забезпечення фінансової безпеки, які мають єдині завдання, цілі, методи, організаційно-правове та фінансово-економічне забезпечення, єдину політику залежно від організаційної структури та кадрового забезпечення і направленості виробничо-господарської діяльності, єдиний механізм управління» [32]. Разом з тим у наведеному визначенні домінує організаційно-структурний підхід, тоді як питання ідентифікації ризиків і загроз фінансовій безпеці фактично залишаються поза увагою.

Тому, виходячи з результатів раніше проведеного дослідження категорії «фінансова безпека підприємств», її особливостей в умовах розвитку цифрової економіки та розглянутої вище дефініції «система», пропонуємо розглядати систему фінансової безпеки підприємств ІТ-сфери як цілісну динамічну систему, що складається із сукупності взаємопов'язаних компонентів, які функціонують у єдиному контурі з метою ідентифікації, оцінювання, запобігання та нейтралізації загроз фінансовій безпеці, а також забезпечення стабільного функціонування, адаптації та розвитку підприємств ІТ-сфери в умовах високотехнологічного, інноваційного та динамічного середовища з урахуванням специфіки галузевих ризиків, глобальних викликів та високого рівня технологічної залежності ІТ-сфери.

Запропоноване трактування системи фінансової безпеки підприємств ІТ-сфери узгоджується із сучасними вітчизняними науковими підходами, відповідно до яких фінансова безпека розглядається як багаторівнева система, що поєднує фінансові, інформаційні, кадрові та управлінські компоненти. Так, Б. І. Пшик підкреслює, що ефективне функціонування системи фінансової безпеки можливе лише за умови взаємоузгодженості її структурних елементів і здатності адаптуватися до змін зовнішнього середовища [176]. У цьому контексті системний підхід дозволяє розглядати фінансову безпеку не просто як сукупність окремих елементів, а як цілісну складну систему, орієнтовану на довгострокову стійкість і розвиток підприємства.

Варналій З. С. робить акцент на впливі процесів цифровізації на фінансову безпеку та зазначає, що система фінансової безпеки підприємства повинна формуватися з урахуванням динамічних змін економічного та технологічного середовища, забезпечуючи не лише підтримання фінансової стійкості, а і здатність до адаптації та розвитку в умовах цифрової економіки [75].

Разом з тим процес формування системи фінансової безпеки ІТ-підприємств потребує теоретико-методологічного уточнення, є оскільки ІТ-галузь функціонує в середовищі, де фінансові результати безпосередньо залежать від стану цифрової інфраструктури, захищеності нематеріальних активів, інтегрованості у глобальні ринки та швидкості впровадження технологічних інновацій. Такі умови формують специфічну архітектуру системи фінансової безпеки ІТ-підприємств, її принципів побудови, функцій, внутрішніх підсистем та логіки взаємодії між структурними елементами.

Враховуючи вище зазначене, а також те, що належний рівень фінансової безпеки підприємств ІТ-сфери виступає критично важливим аспектом їхнього стабільного функціонування та розвитку в сучасних умовах динамічного бізнес-середовища та швидких темпів цифровізації економіки, застосування системного підходу до визначення цього поняття дозволить:

- сформулювати мету формування системи фінансової безпеки ІТ-підприємств;
- охарактеризувати структурну побудову системи фінансової безпеки, деталізувати її ключові компоненти;
- окреслити характер взаємодії системи з зовнішнім середовищем, що дозволить в подальшому глибше дослідити зовнішні впливи та загрози (економічні, політичні, технологічні, соціальні), які можуть як сприяти, так і перешкоджати досягненню фінансової стійкості та рівноваги суб'єктів господарювання ІТ-галузі;
- обґрунтувати принципи формування, функціонування та розвитку системи;
- визначити властивості та функціональні характеристики системи фінансової безпеки;
- визначити місце системи фінансової безпеки в загальній архітектурі економічної безпеки підприємств ІТ-сфери.

На рис. 1.16 представлено концептуальну модель системи фінансової безпеки підприємств, що формується під впливом зовнішнього середовища, має низку внутрішніх взаємопов'язаних компонентів, об'єднаних спільною метою - забезпечення фінансової стійкості підприємства шляхом захисту фінансових, інформаційних, цифрових та інтелектуальних ресурсів від потенційних внутрішніх і зовнішніх загроз в умовах динамічного цифрового середовища та високого рівня ризиків. Відповідно до встановленої мети функціонують та еволюціонують усі елементи системи.

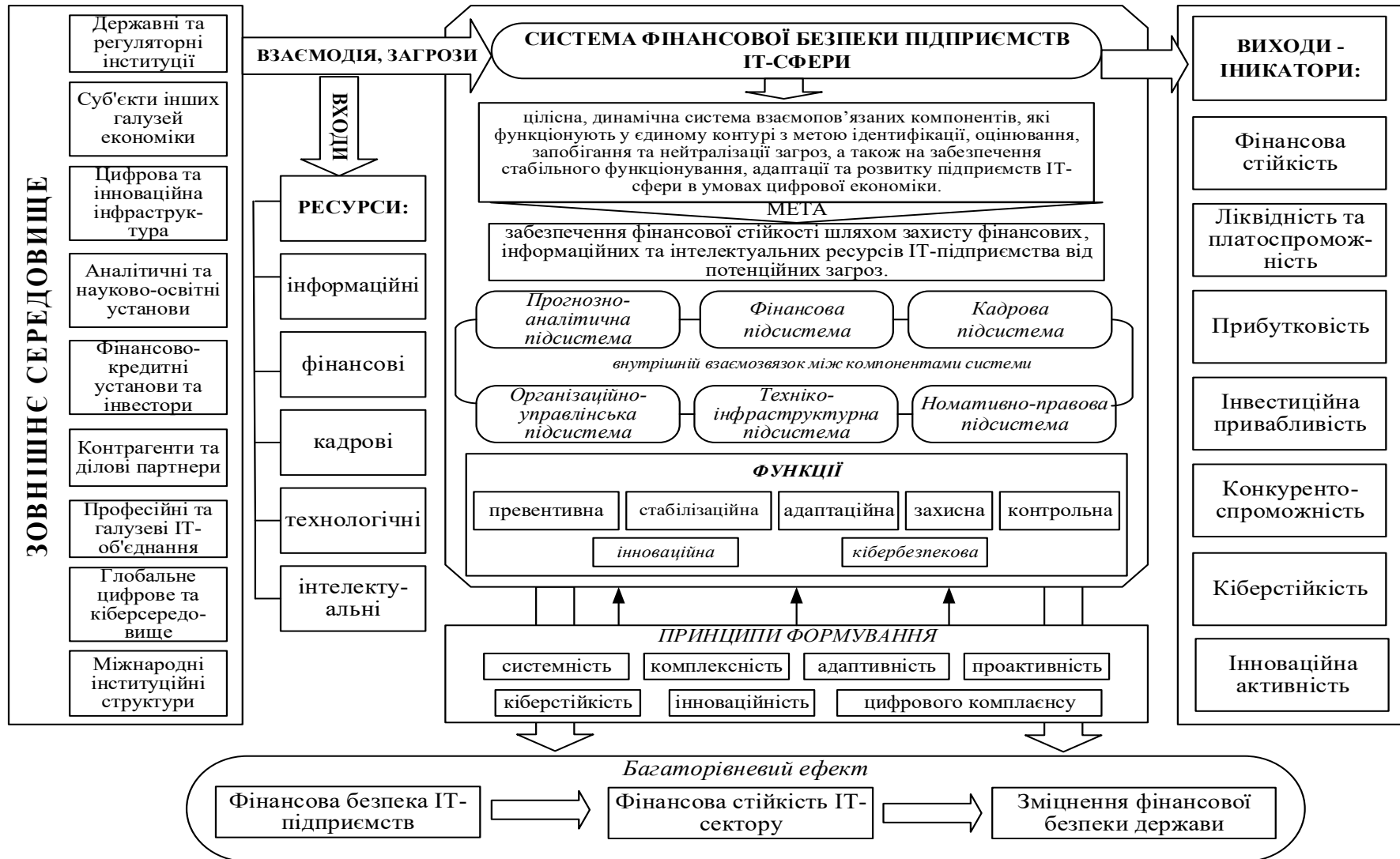


Рис. 1.16. Концептуальна модель системи фінансової безпеки підприємств ІТ-сфери

Джерело: складено автором на основі [121; 203; 219; 221; 86].

Наступним етапом дослідження є розгляд структурно-функціонального наповнення системи фінансової безпеки підприємств ІТ-сфери. Така система не є ізольованою, а функціонує в умовах постійної взаємодії з внутрішніми та зовнішніми чинниками, що зумовлює складність її організації та багатокomпонентність структури. Такий підхід відповідає положенням системної теорії фінансової безпеки підприємств, згідно з якими вона розглядається як відкрита, соціально-економічна система [158].

Функціонування системи фінансової безпеки ІТ-підприємств базується на узгодженій взаємодії суб'єктів, об'єктів захисту та умов зовнішнього середовища, які в сукупності створюють підґрунтя для забезпечення фінансової стійкості та своєчасного реагування суб'єктів господарювання на виклики та загрози.

Важливою складовою моделі системи фінансової безпеки ІТ-підприємств є зовнішнє середовище, яке формує комплекс екзогенних факторів впливу на фінансовий стан, ризик-профіль та стабільність функціонування суб'єктів ІТ-сфери. Воно окреслює інституційні, економічні, технологічні та інформаційні рамки взаємодії підприємства з державними органами, ринком, цифровою та інноваційною інфраструктурою, науково-освітнім простором, фінансовими установами та глобальним кіберпростором. Сукупний вплив зовнішніх факторів визначає характер та інтенсивність ризиків та загроз, що впливають на фінансову стійкість і здатність підприємств ІТ-сфери ефективно функціонувати та розвиватися в умовах постійних змін.

Крім того, зовнішнє середовище виступає не лише джерелом ризиків та регуляторних впливів, а і стає простором залучення до системи фінансової безпеки підприємства ключових ресурсів. У процесі взаємодії підприємства з інституціями зовнішнього середовища до системи інтегруються інформаційні, фінансові, кадрові, технологічні та інтелектуальні ресурси, що формують її ресурсну основу.

Виокремлення саме цих ресурсів зумовлено специфікою діяльності ІТ-підприємств в умовах цифрової економіки, адже саме вони створюють основу їх функціонування, визначають рівень технологічного розвитку, конкурентоспроможність та характер ризиків і загроз, притаманних ІТ-галузі.

Функціонування системи фінансової безпеки ІТ-підприємств орієнтовано на захист таких ключових об'єктів, як майно, капітал, грошові потоки, прибуток, інвестиції, а також інформаційних ресурсів, цифрових та нематеріальних активів, інноваційного потенціалу, технологічної інфраструктури, людського й репутаційного капіталу. Тобто сукупність цих об'єктів охоплює як традиційні фінансові ресурси, так і специфічні для ІТ-сфери активи, які прямо або опосередковано впливають на рівень фінансової стійкості, інвестиційну привабливість та конкурентоспроможність підприємств в ІТ-секторі [27].

Наступним кроком є визначення суб'єктів системи фінансової безпеки, які здійснюють управлінські, захисні, аналітичні та регуляторні дії, спрямовані на захист ключових об'єктів фінансової безпеки та формують організаційно-інституційну основу її функціонування.

Суб'єкти системи фінансової безпеки ІТ-підприємства являють собою сукупність внутрішніх управлінських структур та зовнішніх інституцій, діяльність яких пов'язана з координацією, контролем і регулюванням процесів забезпечення фінансової стійкості, мінімізації ризиків та захисту ключових активів підприємства [118]. При цьому ефективність функціонування системи значною мірою залежить від узгодженості їхніх дій, чіткості розподілу повноважень, рівня координації та якості комунікацій між ними.

Внутрішніми суб'єктами виступають ті структурні одиниці та посадові особи, які безпосередньо залучені до моніторингу, аналізу та забезпечення стабільності фінансово-економічної діяльності конкретного підприємства. Їхня діяльність охоплює оцінку стану фінансової безпеки, підготовку інформаційно-аналітичних матеріалів для прийняття управлінських рішень, контроль за їх реалізацією, а також оперативне реагування на зміни в зовнішньому і внутрішньому середовищі [176].

До основних внутрішніх суб'єктів переважно належать засновники та керівництво підприємства, фахівці з фінансів, ризик-менеджменту, бухгалтерського обліку та управління персоналом. Особливу роль для підприємств ІТ-сфери набуває служба інформаційної безпеки, яка забезпечує захист цифрової інфраструктури та фінансових даних. З огляду на високий рівень диджиталізації фінансових процесів, саме ця ланка поєднує технічний захист із фінансовою стійкістю підприємства, оскільки кіберінциденти безпосередньо трансформуються у фінансові ризики, що зумовлює необхідність інтеграції кіберзахисту в систему фінансової безпеки ІТ-підприємства.

Зовнішніми суб'єктами виступають інституції, що здійснюють регулятивний, контрольний або фінансовий вплив на діяльність ІТ-компаній. До них належать державні органи регулювання (Державна податкова служба, Міністерство цифрової трансформації, Міністерство фінансів, Національний банк України), фінансово-кредитні установи, інвестори, партнери й контрагенти, освітньо-наукові установи, міжнародні інституції, аудиторські та консалтингові організації, а також професійні ІТ-об'єднання. Їхній вплив формує зовнішнє інституційне середовище, у межах якого функціонує система фінансової безпеки ІТ-підприємства.

Подальше дослідження потребує розгляду внутрішніх структурно-функціональних компонентів системи фінансової безпеки ІТ-підприємства, які забезпечують перетворення наявних ресурсів на конкретні управлінські дії, превентивні й захисні механізми, аналітичні процеси та інструменти реагування. Саме ці компоненти визначають внутрішню будову системи, логіку взаємодії її елементів та здатність до ефективного реагування на ризики високотехнологічного середовища цифрової економіки.

Прогнозно-аналітична підсистема є однією з ключових функціональних складових системи фінансової безпеки підприємств ІТ-сфери, оскільки забезпечує її інформаційно-аналітичне підґрунтя. Її призначення полягає у формуванні цілісного уявлення про поточний і перспективний фінансовий стан

підприємства, своєчасному виявленні внутрішніх і зовнішніх загроз фінансовій безпеці, а також прогнозуванні можливих сценаріїв розвитку з урахуванням їхнього потенційного впливу на стабільність функціонування.

Сутність цієї підсистеми полягає у зборі, обробці та інтерпретації інформації фінансового, ринкового, регуляторного характеру з метою оцінювання ризиків, здійснення фінансового планування та прогнозування ключових фінансових показників. З позицій системного підходу прогнозно-аналітична підсистема виконує роль аналітичного ядра у структурі системи фінансової безпеки ІТ-підприємств, забезпечуючи інформаційно-прогнозну підтримку інших підсистем та їх скоординоване функціонування.

Для підприємств ІТ-сфери, діяльність яких відзначається високою динамічністю, залежністю від зовнішніх ринків і підвищеною чутливістю до кіберризиків, прогнозно-аналітична підсистема в умовах цифрової економіки має особливе значення. Саме вона визначає здатність системи фінансової безпеки своєчасно враховувати зміни зовнішнього й внутрішнього середовища для оперативного реагування.

Фінансова підсистема є центральною функціональною складовою системи фінансової безпеки підприємств ІТ-сфери, оскільки саме вона безпосередньо формує основу їх фінансової стійкості, забезпечує безперервність операційної діяльності та здатність підприємства до самофінансування. Її призначення полягає у створенні умов для ефективного формування, раціонального використання та захисту фінансових ресурсів з метою недопущення кризових явищ, втрати активів, погіршення платоспроможності та недофінансування стратегічно важливих проєктів чи напрямів діяльності.

У структурі системи фінансової безпеки фінансова підсистема забезпечує достатність та узгодженість грошових потоків, підтримує внутрішню фінансову рівновагу і створює фінансову ресурсну основу для функціонування інших складових системи. Її роль полягає у формуванні цілісного фінансового середовища, що здатне зменшувати вразливість підприємства до ризиків та загроз як внутрішнього, так і зовнішнього походження.

Особливе значення фінансова підсистема має для підприємств ІТ-сфери, діяльність яких характеризується високою часткою нематеріальних активів, значними обсягами інвестицій в інноваційні проєкти, науково-дослідницьку діяльність, висококваліфікований персонал тощо. За таких умов саме фінансова підсистема визначає спроможність фінансового забезпечення діяльності та підтримання фінансової стійкості в умовах швидкозмінного зовнішнього середовища.

Організаційно-управлінська підсистема забезпечує внутрішню керованість і узгоджену взаємодію між усіма елементами системи, вона формує управлінську архітектуру фінансової безпеки, у межах якої визначаються ролі, обов'язки та відповідальність при прийнятті рішень щодо забезпечення фінансової стійкості підприємства.

Призначення організаційно-управлінської підсистеми полягає у створенні процедурних засад функціонування системи фінансової безпеки, які відповідають стратегічним цілям розвитку підприємства та специфіці його діяльності. Вона інтегрує фінансові, аналітичні, кадрові та інші складові в цілісну систему управління фінансовою безпекою.

У структурі системи фінансової безпеки організаційно-управлінська підсистема виконує координуючу роль, забезпечуючи внутрішню дисципліну виконання рішень і стабільність функціонування системи в умовах невизначеності зовнішнього середовища.

Для підприємств ІТ-сфери, які характеризуються проєктною організацією діяльності та достатньо гнучким управлінням, організаційно-управлінська підсистема відіграє важливу роль в узгодженні стратегічних і оперативних рішень щодо формування системи фінансової безпеки. Вона забезпечує координацію дій між структурними підрозділами, сприяє своєчасному реагуванню на зміни цифрового середовища та адаптації системи фінансової безпеки до нових ризиків і викликів.

Кадрова підсистема є однією з базових складових системи фінансової безпеки підприємств ІТ-сфери, оскільки саме через людський ресурс забезпечується реалізація її принципів, функцій та управлінських рішень на

практиці. У межах системного підходу саме кадрова підсистема формує основу здійснення заходів щодо забезпечення фінансової безпеки через людський капітал, поєднуючи професійні компетенції персоналу, відповідальність і культуру дотримання правил безпеки.

Призначення кадрової підсистеми полягає у приведенні компетентностей персоналу у відповідність до завдань забезпечення фінансової безпеки підприємства, а також у зниженні внутрішньої вразливості системи, що пов'язана з людським фактором. Через неї досягається стабільність функціонування всієї системи фінансової безпеки шляхом формування кадрового потенціалу, здатного діяти в умовах невизначеності та підвищених ризиків.

Для підприємств ІТ-сфери значення кадрової підсистеми істотно зростає з огляду на високу мобільність фахівців, концентрацію критично важливих знань у людському капіталі та високу залежність фінансової стійкості від якості та професійних компетенцій персоналу. Тому кадрова підсистема відіграє важливу роль у мінімізації внутрішніх загроз, підтриманні фінансової дисципліни та забезпеченні рівня фінансової безпеки.

Техніко-інфраструктурна підсистема є матеріально-технологічною основою функціонування системи фінансової безпеки підприємств ІТ-сфери, що визначає рівень її технологічної надійності і стійкості. Саме через цю підсистему підтримується безперервна робота фінансових, аналітичних і управлінських процесів, а також здатність реалізації захисних і контрольних функцій в умовах цифрової економіки.

У структурі системи фінансової безпеки техніко-інфраструктурна підсистема охоплює сукупність технічних та програмних рішень, які забезпечують зберігання, обробку та захист фінансової інформації, ефективність внутрішніх бізнес-процесів і створюють умови для своєчасного виявлення ризиків і загроз різної природи. Її роль полягає у підтримці технологічної готовності підприємства до реагування на збої, кібератаки та інші деструктивні впливи.

Оскільки фінансова безпека ІТ-компаній безпосередньо залежить від надійності цифрової інфраструктури, захищеності інформаційних ресурсів і безперервності функціонування технологічних платформ для підприємств ІТ-сфери техніко-інфраструктурна підсистема має системоутворююче значення.

Нормативно-правова підсистема формує внутрішнє нормативне поле, у межах якого реалізуються управлінські, фінансові та захисні рішення, і забезпечує їх узгодженість із вимогами національного і міжнародного законодавства.

У структурі системи фінансової безпеки нормативно-правова підсистема виконує функцію формалізації правил, процедур і стандартів, що регламентують фінансово-економічну діяльність підприємства, розподіл відповідальності, порядок контролю та реагування на порушення. Саме через цю підсистему вимоги зовнішнього регуляторного середовища трансформуються у внутрішні політики, положення та інструкції.

Для підприємств ІТ-сфери значення нормативно-правової підсистеми зростає з огляду на міжнародний характер діяльності, використання цифрових фінансових інструментів і залучення іноземних контрагентів та інвесторів. Вона виступає головним елементом мінімізації правових і регуляторних ризиків, забезпечення прозорості фінансових операцій і підтримання довіри з боку фінансових інституцій та органів контролю, а також створює передумови для узгодження системи фінансової безпеки зі змінами правового середовища.

Ефективність функціонування системи фінансової безпеки ІТ-підприємств значною мірою визначається дотриманням базових принципів (рис. 1.17) її формування та розвитку. Вони поєднують загальноекономічні засади забезпечення фінансової безпеки підприємств із галузевими особливостями ІТ-сфери, розглядаючи систему як складну відкриту структуру, що перебуває у постійній взаємодії із зовнішнім середовищем. Принципи відображають особливості її внутрішньої організації та формують методологічну основу функціонування в умовах швидкозмінного зовнішнього середовища.

Принципи формування системи фінансової безпеки підприємств ІТ-сфери			
Принцип системності забезпечення узгодженого функціонування всіх елементів фінансової безпеки (ресурси, процеси, цифрові активи, персонал, інфраструктура) у єдиному контурі управління	Принцип комплексності врахування широкого спектра фінансових, інформаційних, технологічних і кіберзагроз та застосування різних механізмів їх нейтралізації	Принцип адаптивності здатність системи фінансової безпеки оперативно коригувати підходи та процедури управління відповідно до змін у цифровому та фінансовому середовищі	Принцип проактивності завчасне виявлення потенційних загроз цифрового середовища та їх попередження через використання прогностичних і аналітичних інструментів
Принцип безперервного контролю постійний моніторинг фінансових операцій та цифрових процесів для оперативного виявлення відхилень і загроз	Принцип кіберстійкості забезпечення стійкості фінансових процесів до кіберінцидентів через захист ІТ-інфраструктури, цифрових сервісів і каналів передачі даних	Принцип технологічної автоматизації впровадження автоматизованих систем фінансового моніторингу, контролю та аналізу для ефективного управління фінансами	Принцип інноваційності необхідність постійного оновлення інструментарію забезпечення фінансової безпеки через впровадження новітніх ІТ-рішень, технологій аналітики даних і кіберзахисту
Принцип конфіденційності та захисту даних дотримання стандартів збереження, обробки та передачі фінансової інформації, забезпечення захисту інтелектуальної власності	Принцип гнучкості можливість швидкої зміни підходів, процедур та інструментів для реагування на зовнішні й внутрішні зміни чи нові ризикові ситуації	Принцип масштабованості здатність системи фінансової безпеки ефективно функціонувати при збільшенні обсягів даних, фінансових операцій та зростанні навантаження на ІТ-інфраструктуру	Принцип цифрового комплаєнсу дотримання нормативно-правових вимог у сферах фінансових операцій, кіберзахисту, захисту даних та інформаційної безпеки

Рис. 1.17. Принципи формування системи фінансової безпеки ІТ-підприємств

Джерело: складено за [27; 46; 121; 176].

Запропонована сукупність принципів системи фінансової безпеки ІТ-підприємств ґрунтується на положеннях системного та ризик-орієнтованого підходів, які широко застосовуються в сучасних наукових дослідженнях фінансової безпеки [121; 159; 9], та водночас є адаптованою до особливостей функціонування ІТ-підприємств у цифровому середовищі.

Побудована концептуальна модель системи фінансової безпеки ІТ-підприємств дає змогу виокремити низку ключових властивостей, тобто основних характеристик, за допомогою яких можна описати саму систему, виходячи з її природи. На відміну від принципів, що окреслюють методологічні засади побудови системи, властивості розкривають її характеристики, які проявляються у процесі функціонування та взаємодії складових елементів системи.

По-перше, система фінансової безпеки ІТ-підприємств є *цілісною*, тобто функціонує як цілісна конструкція, у межах якої взаємопов'язані підсистеми об'єднані спільною метою та функціонують як єдине ціле. При цьому взаємодія компонентів системи утворює якісно нові властивості, не притаманні кожній підсистемі окремо [129].

По-друге, система характеризується *структурованістю*, яка проявляється у впорядкованій внутрішній будові, в межах якої кожна підсистема виконує відповідну функцію та взаємодіє з іншими елементами системи. Це дозволяє чітко ідентифікувати складові компоненти системи, визначати їх роль і призначення та аналізувати взаємодію між ними в межах єдиної архітектури фінансової безпеки [227].

По-третє, важливою характеристикою системи фінансової безпеки ІТ-підприємств є *адаптивність*, тобто її здатність змінювати параметри свого функціонування відповідно до трансформацій у фінансово-економічному, нормативному чи технологічному середовищі, що особливо актуально для підприємств ІТ-сфери [227].

Прогностичність є ще однією вагомою рисою системи фінансової безпеки ІТ-підприємств, яка реалізується через її здатність до випереджального виявлення потенційних загроз, аналізу ймовірних сценаріїв розвитку та формування превентивних управлінських фінансових рішень. Прогностичність забезпечує перехід від реактивної до проактивної моделі управління фінансовою безпекою.

Наступною властивістю системи фінансової безпеки підприємств ІТ-сфери можна виокремити *технологічну інтегрованість*, що проявляється у вбудованості цифрових рішень у всі її підсистеми – від аналітики та фінансового контролінгу до моніторингу ризиків і кіберзахисту. Це забезпечує автоматизацію, оперативність та прозорість фінансових і управлінських процесів.

Окремо варто відзначити *правову обґрунтованість* системи, яка полягає у її відповідності вимогам вітчизняного та міжнародного законодавства, нормам фінансового моніторингу, податкового та валютного регулювання, а також стандартам захисту даних і цифрової безпеки. Це формує інституційні рамки функціонування системи фінансової безпеки підприємств ІТ-сфери.

Наступною характеристикою системи слід виділити *комунікативність*, суть якої проявляється в наявності ефективних горизонтальних та вертикальних зв'язків між окремими підсистемами фінансової безпеки, а також у системній взаємодії підприємства із зовнішніми суб'єктами. Розвинені канали зворотного зв'язку забезпечують оперативність отримання інформації щодо ризиків, узгодженість управлінських рішень та своєчасне реагування на загрози.

Нарешті, система фінансової безпеки характеризується *результативністю* та є спрямованою не лише на нейтралізацію ризиків і загроз, а й на досягнення позитивних фінансово-економічних результатів діяльності ІТ-підприємств: підвищення фінансової стійкості, зростання інвестиційної привабливості, забезпечення конкурентоспроможності та стратегічної витривалості ІТ-бізнесу в умовах цифрової економіки.

Найбільш повно сутність системи фінансової безпеки підприємств ІТ-сфери доцільно розглянути через дослідження її функцій. Вони відображають цільову спрямованість системи та її роль у підтримці стійкого і прогнозованого фінансового стану підприємств в умовах цифрових трансформацій. У контексті ІТ-сфери ці функції набувають галузевої специфіки, оскільки визначаються не лише базовими завданнями протидії ризикам і загрозам, а й

високою динамікою ІТ-ринку, активним інноваційним розвитком та залежністю фінансових процесів ІТ-бізнесу від цифрової інфраструктури.

У науковій літературі до базових функцій системи фінансової безпеки підприємств традиційно відносять превентивну, стабілізаційну, адаптаційну, захисну та контрольну [25; 227; 208]. Розглянемо їх сутність більш детально з фокусом на підприємства ІТ-сфери.

1. Превентивна функція – полягає у спрямованості системи фінансової безпеки на раннє попередження та своєчасне виявлення потенційних загроз, а також мінімізацію ймовірних фінансових втрат ще до їх настання. Її зміст пов'язаний із формуванням у межах системи такого аналітичного та управлінського середовища, яке здатне своєчасно розпізнавати ризикові тенденції та реагувати на них ще до настання кризових явищ у фінансовій сфері підприємства [176; 192].

У випадку ІТ-компаній превентивна функція особливо важлива через високу чутливість до ризиків, пов'язаних із втратою даних, кібератаками, збоями цифрової інфраструктури, відтоком ключових фахівців та іншими загрозами цифрового середовища. На системному рівні реалізація цієї функції проявляється у постійному моніторингу внутрішніх і зовнішніх факторів впливу, формуванні системи «фінансових сигналів» на ризики та підтримці готовності підприємства до раннього попередження та реагування, в тому числі й із застосуванням новітніх цифрових технологій.

2. Стабілізаційна функція – спрямована на підтримання належного рівня фінансової стійкості підприємства, збереження платоспроможності та стабільності грошових потоків в умовах постійної трансформації бізнес-середовища під впливом розвитку новітніх цифрових технологій. Вона відображає здатність системи фінансової безпеки утримувати ключові фінансові параметри в межах допустимих коливань навіть за наявності зовнішніх чи внутрішніх потрясінь [176].

У межах цієї функції система орієнтована на підтримку збалансованості доходів і витрат, формування фінансових резервів та створення запасу ліквідності, достатнього для безперервного здійснення операційної діяльності. Для підприємств ІТ-сфери це особливо важливо з огляду на значні коливання ринкового попиту, проєктний характер діяльності та залежність від зовнішніх замовників. Реалізація стабілізаційної функції дозволяє зменшити чутливість ІТ-бізнесу до зовнішніх і внутрішніх фінансових шоків й сформувати необхідний запас фінансової міцності.

3. Адаптаційна функція - проявляється у спроможності системи фінансової безпеки змінювати параметри свого функціонування у відповідь на зміни технологічного, регуляторного або ринкового характеру (коливання валютних курсів, появу нових технологічних рішень, зміни нормативно-правової бази та конкурентного середовища тощо). На відміну від стабілізаційної функції, що спрямована на утримання фінансової рівноваги, адаптаційна функція передбачає гнучке коригування фінансової політики, ресурсного забезпечення та пріоритетів фінансово-економічного розвитку [176; 154].

Для підприємств ІТ-сфери ця функція є важливою з огляду на високу швидкість технологічних змін та інноваційний характер їх продукції та послуг. Зміст цієї функції полягає у здатності ІТ-підприємства оперативно перебудовувати фінансові та операційні процеси відповідно до технологічних і ринкових змін, забезпечуючи фінансову стабільність та безперервність діяльності.

4. Захисна функція - полягає в протидії вже реалізованам або неминучим загрозам та спрямована на мінімізацію їх негативного впливу на фінансово-господарські процеси та фінансовий стан підприємства. Якщо превентивна функція має випереджальний характер, то захисна активізується в умовах фактичного настання ризикової події та орієнтована на мінімізацію втрат [93; 192].

Для підприємств ІТ-сектору у межах системи фінансової безпеки вона проявляється у здатності нейтралізувати наслідки несанкціонованого доступу до фінансових даних, витоку інформації, кібершахрайства та інших загроз, що

можуть порушити фінансову стійкість компанії. Реалізація захисної функції забезпечує збереження фінансової стійкості підприємства навіть у кризових умовах та формує підґрунтя для відновлення діяльності, підтримуючи довіру інвесторів, клієнтів і партнерів.

5. *Контрольна функція* полягає у систематичному оцінюванні рівня фінансової безпеки та його відповідності встановленим критеріям, показникам чи орієнтирам. Її призначення полягає у контролі та зіставленні фактичних результатів фінансово-господарської діяльності із запланованими параметрами, а також у виявленні відхилень, що можуть свідчити про зростання фінансових ризиків [93].

В умовах цифрової економіки значення контрольної функції істотно зростає, оскільки фінансові процеси підприємств характеризуються високим рівнем автоматизації та складною системою інформаційної взаємодії. Тому, для ІТ-підприємств це означає необхідність поєднання фінансового контролю з цифровими засобами обробки та аналізу даних, що підвищує точність оцінки фінансового стану та своєчасність фінансових управлінських рішень.

Контрольна функція формує інформаційну основу для коригування фінансової політики підприємства та забезпечує внутрішню узгодженість системи фінансової безпеки.

Разом з тим, враховуючи особливості фінансово-економічної діяльності ІТ-компаній в умовах цифрової економіки, на нашу думку, виникає необхідність розширення традиційного переліку функцій системи фінансової безпеки підприємств. Сучасні дослідження доводять, що для таких компаній інноваційна активність і кібербезпека інтегруються у функціональний контур системи фінансової безпеки, оскільки безпосередньо впливають на фінансові результати, збереження фінансових ресурсів, стабільність грошових потоків і ринкових позицій ІТ-підприємств.

Наприклад, З. Тітенко наголошує, що інноваційна складова фінансової безпеки є визначальним чинником підвищення адаптивності підприємств до цифрових викликів, тоді як посилення кіберзагроз актуалізує необхідність

інтеграції кібербезпекових рішень у загальну систему фінансової безпеки [200]. Таким чином, пропонуємо розширити функціональний зміст системи фінансової безпеки, додавши інноваційну та кібербезпекову функції.

6. Інноваційна функція - відображає спрямованість системи фінансової безпеки підприємств ІТ-сфери на активне впровадження сучасних цифрових технологій та рішень у фінансовому менеджменті. Такі інновації розширюють аналітичні можливості підприємства, підвищують точність прогнозування фінансових результатів, удосконалюють процедури фінансового аналізу, контролю та моніторингу ризиків.

Як зазначає Тітенко З., у сучасному високотехнологічному середовищі, де характер загроз змінюється надзвичайно швидко, здатність до впровадження інновацій є не лише перевагою, а й необхідною умовою забезпечення належного рівня фінансової безпеки [200].

При цьому йдеться не лише про оновлення інструментарію фінансового менеджменту, а й про зміну самих підходів до управління ризиками з урахуванням специфіки цифрової економіки та появи нових фінансових і кіберзагроз. Інноваційна складова в цьому контексті також означає здатність системи діяти на випередження, використовуючи дані, алгоритми та цифрові рішення для своєчасного виявлення ризиків, посилюючи тим самим фінансовий захист.

Водночас реалізація цієї функції знижує вразливість підприємства до цифрових загроз, підвищує прогнозованість фінансових результатів та формує більш стабільне та контрольоване фінансове середовище, що створює основу фінансової стабільності, підґрунтя для залучення інвестицій та довгострокового розвитку компанії.

7. Кібербезпекова функція відображає спрямованість системи фінансової безпеки на захист фінансових даних, цифрових активів та ІТ-інфраструктури підприємства від кіберзагроз, які здатні призвести до значних фінансових втрат, порушення операційної діяльності або репутаційних ризиків.

Зміст кібербезпекової функції полягає у формуванні в межах системи фінансової безпеки моделі цифрового захисту, орієнтованої на збереження цілісності, конфіденційності та безперервності фінансових процесів. Як слушно зазначає А. Ю. Мунько, кібербезпека дедалі більше розглядається як складова фінансової безпеки, оскільки цифрові атаки прямо впливають на стабільність фінансових потоків та довіру до суб'єкта господарювання [131].

Для підприємств ІТ-сфери ця функція має особливо важливе значення, оскільки їх фінансові процеси тісно інтегровані з цифровим середовищем, коли будь-який кіберінцидент фактично перетворюється на фінансову загрозу. Відтак захист інформаційних ресурсів стає водночас і захистом фінансової стабільності ІТ-бізнесу.

Ефективне функціонування системи фінансової безпеки ІТ-підприємства дозволяє сформулювати результати, що проявляються у зовнішньому та внутрішньому середовищі через конкретні індикатори (виходи): підвищення фінансової стійкості ІТ-підприємств, зниження рівня ризиків, зростання інвестиційної привабливості, активізацію інноваційної активності, а також посилення кіберстійкості, технологічного потенціалу та конкурентоспроможності підприємств ІТ-сфери. На макрорівні це створює позитивний мультиплікативний ефект для національної економіки, оскільки сприяє зростанню експорту ІТ-послуг, розширенню участі українських компаній у міжнародних проєктах та підвищенню довіри іноземних партнерів до українського ІТ-бізнесу, і, як наслідок, зміцнює фінансову безпеку держави.

Варто підкреслити, що вихідні індикатори моделі мають узагальнюючий характер, оскільки поєднують результат взаємодії всіх складових системи фінансової безпеки ІТ-підприємства. Вони відображають не лише фінансові параметри (рівень фінансової стійкості, ліквідність, прибутковість), а й такі характеристики, що актуальні саме для ІТ-компаній – інноваційний потенціал, кіберстійкість тощо. Саме таке поєднання дозволяє оцінити не тільки поточний рівень фінансової захищеності, а й спроможність ІТ-компаній стабільно працювати та розвиватися в умовах цифрової економіки.

Узагальнення теоретичних підходів та результати проведеного дослідження дають змогу систематизувати ключові сутнісні характеристики фінансової безпеки підприємств ІТ-сфери (рис. 1.18), які відображають її специфіку функціонування в умовах цифрової економіки. На відміну від традиційного розуміння фінансової безпеки як сукупності заходів із захисту фінансових ресурсів, у сфері ІТ вона набуває комплексного змісту, поєднуючи фінансово-ресурсну стабільність, ризик-орієнтованість, технологічну інтегрованість та інституційну взаємодію.



Рис. 1.18. Сутнісні характеристики фінансової безпеки підприємств ІТ-сфери

Джерело: систематизовано автором на основі [77; 117; 121; 219].

Важливо зауважити, що система фінансової безпеки має бути індивідуальною для кожного ІТ-підприємства, оскільки її зміст та структура визначаються масштабами діяльності, бізнес-моделлю (аутсорсингова, продуктова чи змішана), організаційною структурою, а також унікальним ризик-профілем окремих підприємств.

Водночас результати функціонування системи фінансової безпеки підприємств ІТ-сфери мають і макроекономічне значення. Підвищення рівня фінансової безпеки окремих ІТ-підприємств сприяє підвищенню фінансової стійкості галузі загалом, зростанню її експортного потенціалу, активізації інвестиційних процесів та формуванню стабільних податкових надходжень. У результаті формується мультиплікативний ефект, що поширюється на мезо- та макrorівні, посилюючи фінансову стійкість національної економіки.

В умовах розвитку цифрової економіки саме високотехнологічні галузі дедалі більше впливають на стабільність фінансової системи держави, формування економічного потенціалу країни та її конкурентоспроможність на світовому ринку. Розвиток ІТ-сектору забезпечує стабільність валютних надходжень, формування бюджетних ресурсів, інвестиційну активність та інноваційний розвиток. Важливою особливістю ІТ-галузі є її експортна спрямованість, що зумовлює регулярний приплив валютної виручки до країни та сприяє підтримці платіжного балансу (рис. 1.19).

Крім того, діяльність ІТ-підприємств пов'язана з формуванням податкових надходжень до бюджету, що зумовлено достатньо високим рівнем зайнятості у галузі та специфікою організації ІТ-бізнесу. Особливістю української ІТ-індустрії є використання різних моделей діяльності - від функціонування ІТ-компаній як юридичних осіб до їх співпраці з фізичними особами-підприємцями або резидентами спеціального правового режиму Дія.City.

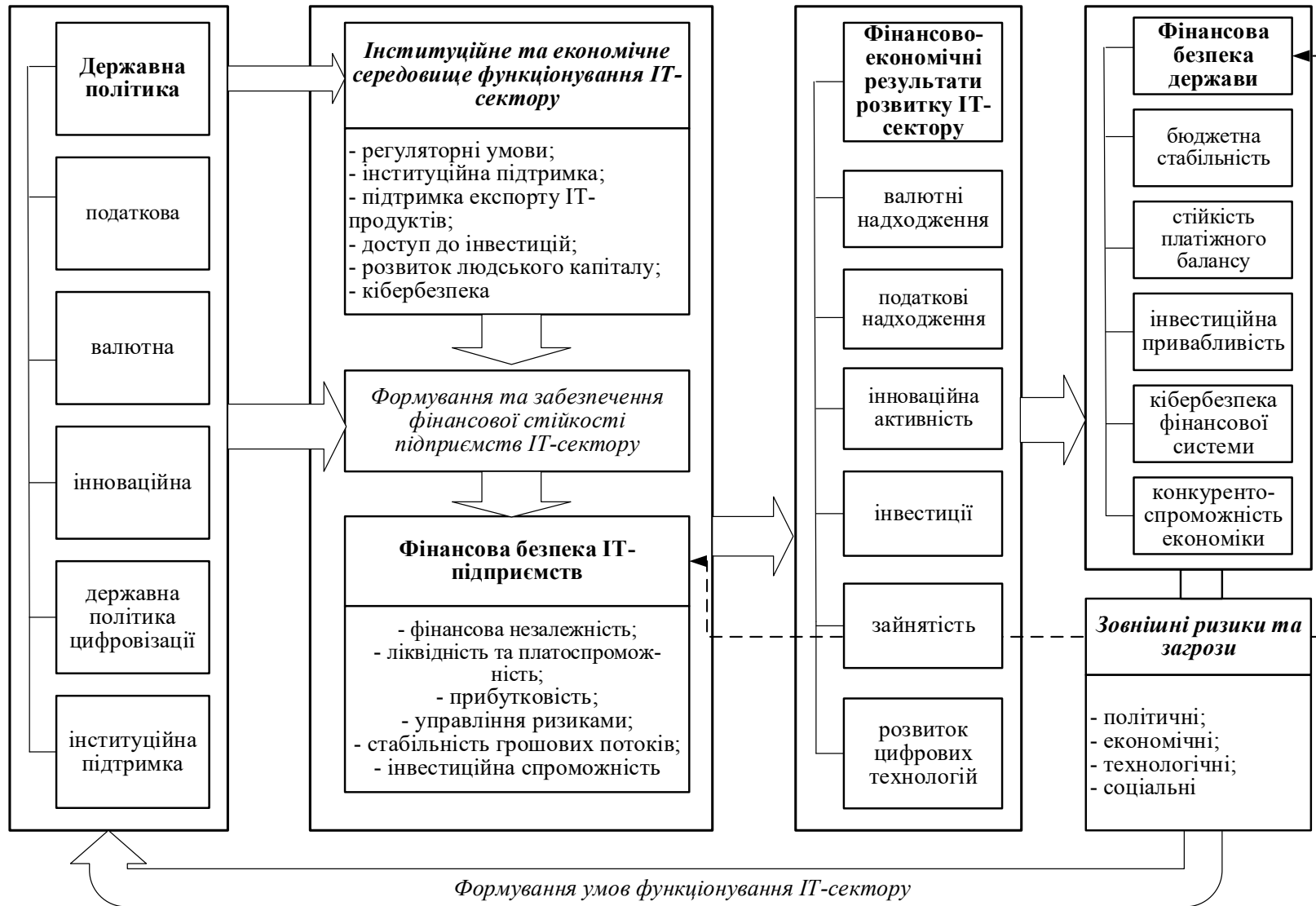


Рис. 1.19 Місце фінансової безпеки ІТ-підприємств у системі фінансової безпеки держави

Джерело: складено автором.

Висока зайнятість і відносно високі доходи працівників ІТ-сектору сприяють розширенню податкової бази. У результаті зростає обсяг фіскальних надходжень у розрахунку на одного зайнятого, а також формується додатковий фінансовий ресурс для бюджетів різних рівнів, що особливо важливо в умовах воєнного часу та зростання соціальних видатків держави.

Крім прямого фіскального впливу та забезпечення високих обсягів валютних надходжень, ІТ-галузь формує мультиплікаційний вплив на економіку країни. Розвиток ІТ-сектору стимулює підприємницьку активність в суміжних сферах (фінансах, освіті, ринку нерухомості, медицині та ін.), тим самим сприяючи зростанню податкової бази та зміцненню фінансової стійкості держави навіть в умовах економічної нестабільності.

Важливе значення для довгострокової фінансової спроможності держави має також людський капітал ІТ-сектору. Висококваліфіковані фахівці формують інтелектуальний потенціал, який забезпечує конкурентоспроможність української економіки на глобальному ринку цифрових послуг. Саме людський капітал ІТ-галузі сприяє розвитку інновацій, створенню нових технологічних продуктів та розширенню експортних можливостей країни.

Окрему роль ІТ-галузь відіграє у процесах цифрової трансформації публічного сектору. Розробка цифрових сервісів електронного урядування, впровадження електронних реєстрів та автоматизація державних послуг сприяють підвищенню прозорості фінансових потоків, покращують податкову дисципліну та зменшують можливості для тіньових операцій. Таким чином, цифрові рішення, створені ІТ-компаніями, підвищують ефективність державного управління.

Крім того, ІТ-галузь сприяє зміцненню фінансової безпеки держави через розвиток інноваційного середовища та залучення інвестицій. Формування стартап-екосистем, розвиток технологічних кластерів і створення

центрів досліджень та розробок (R&D) підвищують інвестиційну привабливість країни, сприяють появі нових технологічних компаній і стимулюють модернізацію економіки.

Таким чином, фінансова безпека підприємств ІТ-сфери має багаторівневий характер і виступає важливим чинником національної фінансової стабільності. Її системне забезпечення створює основу для сталого розвитку вітчизняного ІТ-сектору та підвищення конкурентоспроможності економіки України в умовах цифрових змін.

У підрозділі 1.3 обґрунтовано доцільність формування системи фінансової безпеки підприємств ІТ-сфери як складної відкритої багаторівневої системи, що функціонує в умовах цифрової економіки. Уточнено характеристики фінансової безпеки ІТ-підприємств з урахуванням їх галузевої специфіки та доведено, що вона має розглядатися не лише як стан фінансової захищеності, а як системна категорія, що поєднує ресурсні, ризикоорієнтовані, технологічні, інституційні та кадрові аспекти.

Розроблено концептуальну модель системи фінансової безпеки підприємств ІТ-сфери, яка відображає взаємодію внутрішніх елементів із зовнішнім середовищем та визначено її структурні компоненти, функції, принципи та властивості. Обґрунтовано, що ефективність системи залежить від її адаптивності, цифрової інтегрованості та здатності до раннього виявлення фінансових і технологічних загроз.

Підкреслено індивідуальний характер формування системи фінансової безпеки ІТ-підприємства з урахуванням масштабів діяльності, бізнес-моделі та ризик-профілю компанії. Доведено, що фінансова безпека ІТ-підприємств має багаторівневий характер та стає важливим чинником фінансової стабільності національної економіки в цифрову епоху.

Висновки до першого розділу

1. Розширено теоретичні положення щодо розуміння сутності фінансової безпеки підприємства в умовах цифрової економіки. На основі узагальнення наукових підходів до трактування категорій «безпека», «економічна безпека», «фінансова безпека» та підходів до розуміння сутності фінансової безпеки ІТ-підприємства виокремлено інноваційний підхід, який, на відміну від традиційних, акцентує увагу на важливості цифрових технологій, інноваційної активності, захищеності інформаційних систем у забезпеченні фінансової безпеки суб'єктів господарювання. У результаті встановлено, що в умовах цифрової трансформації фінансова безпека повинна розглядатися як динамічний стан захищеності фінансових ресурсів, інформаційних систем і бізнес-процесів від внутрішніх та зовнішніх загроз, який забезпечується ефективним управлінням ризиками, підтримкою ліквідності, платоспроможності та фінансової рівноваги з використанням сучасних цифрових технологій.

2. Узагальнено та систематизовано наукові підходи до розуміння сутності цифрової економіки, серед яких виокремлено техніко-технологічний, трансформаційний, еволюційний і системний підходи. Визначено ключові характеристики цифрової економіки як середовища формування нових умов фінансово-економічної діяльності підприємств, зокрема трансформацію природи економічних благ, зростання ролі даних, цифрових платформ, інновацій, глобалізації, а також посилення значення кібербезпеки. Це дало змогу обґрунтувати, що цифровізація не лише створює додаткові можливості для розвитку підприємств, а й супроводжується появою нових ризиків, зумовлених цифровою трансформацією бізнес-процесів, підвищенням ролі даних та залежністю підприємств від цифрової інфраструктури.

3. Визначено та обґрунтовано основні аспекти впливу цифрової економіки на фінансову безпеку підприємства. Доведено, що такий вплив має комплексний характер і проявляється через технологічний, інформаційний,

організаційний, ризиковий, інфраструктурний та інституційний аспекти. У результаті встановлено, що в сучасних умовах фінансова безпека підприємства значною мірою залежить від якості фінансового планування, оперативності управлінських рішень, рівня захищеності інформаційних систем і цифрових фінансових операцій, а також здатності підприємства адаптуватися до змін цифрового та регуляторного середовища.

4. Обґрунтовано особливу роль підприємств ІТ-сфери в розвитку цифрової економіки. Визначено, що ІТ-підприємства формують цифрову інфраструктуру економіки, розробляють і впроваджують інноваційні цифрові продукти та забезпечують цифрову трансформацію фінансово-економічних процесів у різних секторах економіки. Це дало змогу встановити, що фінансова безпека підприємств ІТ-сфери має стратегічне значення, оскільки впливає не лише на стабільність і розвиток самих ІТ-підприємств, а й на стійкість ІТ-галузі, конкурентоспроможність національної економіки та зміцнення фінансової безпеки держави загалом.

5. Систематизовано особливості формування фінансової безпеки підприємств ІТ-сфери. Проведено класифікацію ІТ-підприємств за ознаками, що визначають специфіку їх фінансової безпеки. Виділено специфічні особливості економічної діяльності ІТ-підприємств та обґрунтовано їх вплив на формування фінансової безпеки, що проявляється у домінуванні нематеріальних активів, високій ролі людського капіталу, значній залежності від інноваційної активності, цифрової інфраструктури, інформаційних систем і зовнішнього бізнес-середовища. Визначено характерні особливості фінансового управління ІТ-підприємствами, які мають принципове значення для побудови ефективної системи їх фінансової безпеки. На цій основі доведено, що забезпечення фінансової безпеки підприємств ІТ-сфери потребує поєднання традиційних фінансових механізмів із цифровими інструментами контролю, аналізу, прогнозування, управління ризиками та кіберзахисту.

6. Обґрунтовано теоретичний базис для формування системи фінансової безпеки підприємств ІТ-сфери як цілісної, відкритої, структурованої, адаптивної та динамічної системи. Доведено, що така система повинна забезпечувати не лише ідентифікацію, оцінювання, запобігання та нейтралізацію загроз, а й стабільне функціонування, фінансову стійкість, адаптацію та розвиток ІТ-підприємств у високотехнологічному цифровому середовищі. Визначено, що вона має ґрунтуватися на узгодженій взаємодії фінансових, інформаційних, технологічних, кадрових і управлінських компонентів, враховувати специфіку галузевих ризиків, високий рівень технологічної залежності ІТ-сфери та вплив зовнішнього середовища. На цій основі розкрито основні властивості, функції та принципи формування системи фінансової безпеки підприємств ІТ-сфери, а також обґрунтовано її багаторівневе значення: від забезпечення фінансової стійкості окремого ІТ-підприємства до зміцнення фінансової безпеки ІТ-сектору та держави загалом.

Основні результати дослідження опубліковані в таких наукових роботах [47; 102; 64; 103].

РОЗДІЛ 2

ДОСЛІДЖЕННЯ СУЧАСНОГО СТАНУ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ІТ-СФЕРИ

2.1. Сучасний стан та тенденцій розвитку підприємств ІТ-сфери України

На сьогодні завдяки потужному інтелектуальному потенціалу та своїй інноваційній спрямованості ІТ-сектор України виступає одним із провідних драйверів цифровізації національної економіки, формуючи її конкурентні переваги та зміцнюючи позиції на світовому ринку високотехнологічних продуктів і послуг. Вітчизняні ІТ-підприємства дедалі активніше інтегруються у світові виробничі та сервісні ланцюги, задаючи темпи технологічного розвитку нашої держави.

Водночас діяльність ІТ-підприємств в умовах становлення цифрової економіки супроводжується зростанням складності бізнес-процесів і підвищенням ризиковості середовища функціонування, що зумовлює необхідність удосконалення підходів до фінансового менеджменту та формування ефективної системи фінансової безпеки підприємств ІТ-сфери.

Розуміння стану та тенденцій розвитку ІТ-сфери України створює фундамент для подальшого дослідження рівня фінансової безпеки ІТ-підприємств, а також дозволяє виявити проблеми та окреслити перспективи розвитку підприємств ІТ-галузі в умовах диджиталізації та підвищених безпекових ризиків.

Динаміка кількості суб'єктів господарювання, що здійснюють діяльність у сфері ІТ, є важливим індикатором тенденцій розвитку ІТ-галузі. Особливістю вітчизняного ІТ-ринку є складна корпоративна структура, що відрізняє його від інших галузей економіки. В ІТ-секторі одна компанія нерідко представлена кількома юридичними особами, що створюються для реалізації окремих проєктів, напрямів діяльності чи операційних процесів. Як

наслідок, це ускладнює статистичний облік та створює варіативність оцінок загальної кількості ІТ-компаній, залежно від використаної методології.

Так, за даними галузевої аналітики Lviv IT Cluster [243], станом на 2024 рік в Україні діяло 2118 активних верифікованих ІТ-компаній, тоді як Ukrainian Tech Ecosystem [163] фіксує понад 2300 компаній. Водночас Lviv IT Cluster наводить дані про 9,6 тис. діючих юридичних осіб, що надають ІТ-послуги [243], а за інформацією Державної служби статистики їх кількість становила 8,04 тис.

Аналіз статистичних даних засвідчує стійку тенденцію зростання корпоративного сектору вітчизняної ІТ-галузі впродовж 2014 - 2021 рр. (табл. 2.1). За цей період кількість юридичних осіб, що надають ІТ-послуги, збільшилась з 5,6 тис. до 8,9 тис., тобто більше ніж у 1,5 раза, а середньорічний темп приросту становив близько 4,5 %. Такі темпи зростання перевищували аналогічні показники більшості секторів національної економіки, що свідчить про становлення ІТ-галузі як одного з найбільш динамічних її сегментів.

Таблиця 2.1

Кількість діючих юридичних осіб, що надають ІТ-послуги, тис.

Показник	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Кількість діючих юридичних осіб, що надають ІТ-послуги, тис.	5,6	6,0	5,4	6,3	7,0	8,1	8,4	8,9	6,6	7,9	8,0

Джерело: [40].

Найбільш інтенсивне зростання ІТ-ринку за кількістю юридичних осіб відмічається у 2017-2019 рр., коли середньорічний приріст досягав 14,7 %. Цей період характеризувався відносною макроекономічною стабілізацією після кризових явищ 2014-2015 рр., поступовим відновленням економічної активності, стабілізацією валютного ринку та покращенням інвестиційного клімату в країні. Також завдяки прискоренню процесів цифрової трансформації, як то, розширенню впровадження хмарних технологій, електронної комерції, фінтех-рішень, автоматизації управлінських і виробничих процесів та інше, активно зростає попит на ІТ-продукти та послуги в усьому світі.

У таких умовах вітчизняний ІТ-сектор зміг успішно інтегруватись у глобальний ІТ-ринок. До повномасштабної війни сформувався стабільний зовнішній попит на вітчизняні ІТ-продукти та послуги переважно завдяки їхнім конкурентним перевагам за співвідношенням «ціна-якість» та наявності в Україні висококваліфікованих фахівців, вартість роботи яких нижча, ніж у спеціалістів більш розвинених країн. Свою роль у розвитку ІТ-сектору довоєнного періоду відіграв і відносно ліберальний податковий режим для суб'єктів малого підприємництва та ФОП.

У 2020-2021 рр. на тлі пандемії COVID-19, незважаючи на те, що бізнес масово переходив в онлайн і попит на цифрові послуги збільшувався, темпи зростання кількості юридичних осіб в ІТ-сфері уповільнились до 4,6 % за рік. Суб'єкти господарювання ІТ-сфери більше зосереджувались на підтриманні стабільної роботи, оптимізації операційних витрат і перегляді власних бізнес-моделей, а не на створенні нових юридичних осіб.

Повномасштабна війна стала серйозним викликом для вітчизняної ІТ-галузі та всіх галузей національної економіки. У 2022 р. відзначається рекордне за останнє десятиріччя скорочення чисельності ІТ-компаній (на 25,8 % за рік). Очевидним є той факт, що військові дії зумовили падіння попиту на ІТ-послуги з боку іноземних партнерів, неможливість реалізації частини експортних контрактів, часткову або повну втрату доступу до матеріальної та цифрової інфраструктури, вимушену релокацію бізнесу та відтік кадрів, що призвело до припинення діяльності частини ІТ-підприємств.

Проте вже починаючи з 2023 року спостерігається поступове, хоча й повільне, відновлення ІТ-ринку: кількість діючих юридичних осіб в ІТ-сфері зросла на 19,7 % у 2023 р. та дещо меншими темпами у 2024 році – на 1,2 %.

У 2025 р. українські компанії продовжили свою ділову активність, відкриваючи нові офіси, але переважно за кордоном, передусім через складну безпекову та економічну ситуацію в країні. Так, за даними [205] нові представництва відкрили близько 27 % ІТ-компаній, з яких 23 % – за кордоном і лише 4 % – на території України.

Таким чином, можемо констатувати, що навіть попри суттєве скорочення кількості ІТ-компаній у 2022 р., на сьогодні галузь демонструє ознаки відновлення та стабілізації. Впровадження дистанційних форматів роботи, диверсифікація ринків збуту та географічне розширення присутності за кордоном дозволили багатьом суб'єктам господарювання ІТ-сфери забезпечити безперервність операційної діяльності.

Для дослідження фінансової безпеки важливе значення має аналіз структури вітчизняного ІТ-ринку за типами бізнес-моделей ІТ-компаній, оскільки саме вона значною мірою визначає параметри їхньої фінансово-економічної діяльності: обсяги та джерела доходів, структуру витрат, рівень прибутковості та можливості нарощення власного капіталу. Очевидно, що тип бізнес-моделі безпосередньо впливає на чутливість підприємства до змін кон'юнктури зовнішнього ринку, масштаби його діяльності та інвестиційну привабливість.

Аналіз статистичних даних (табл. 2.2) свідчить про поступову, але суттєву трансформацію внутрішньогалузевої структури ІТ-ринку України впродовж 2015-2024 рр. Частка сервісних компаній, які значний час були традиційною основою українського ІТ-сектору, скоротилась з 49,5 % у 2015 р. до 36,1 % у 2024 р., тоді як питома вага продуктових компаній відповідно зросла з 28,5 до 44,5 %. Такі тенденції демонструють поступовий перехід вітчизняного ІТ-сектору від традиційно домінуючої аутсорсингової моделі до продуктової, яка орієнтована на створення власних технологічних продуктів.

З позиції фінансової стійкості галузі такі зміни мають переважно позитивний характер. Продуктові компанії, які генерують дохід від розробки та комерціалізації власних інтелектуальних продуктів, характеризуються меншою залежністю від одного замовника та вищою маржинальністю діяльності, що забезпечує їм вищий рівень фінансової автономії та капіталізації. Натомість аутсорсингові компанії традиційно мають проектно-контрактну організацію діяльності, де обсяги виручки безпосередньо залежать від кількості активних контрактів і тривалості співпраці з клієнтами, що зумовлює їх більшу залежність від зовнішнього попиту та умов співробітництва з партнерами.

Типи ІТ-компаній України за 2015-2024 рр.

Рік	Продуктові компанії, %	Сервісні компанії, %	Аутстафінгові, %	Стартапи, %	Інше, %
2015	28,5	49,5	9,4	4,5	8,0
2016	29,4	48,3	9,0	5,3	8,0
2017	30,8	47,3	9,3	5,6	7,0
2018	32,5	46,6	10,1	4,8	6,0
2019	32,6	46,2	10,8	4,3	6,0
2020	35,3	44,5	11,5	4,4	4,2
2021	36,1	44,5	11,7	3,9	3,8
2022	35,4	44,1	12,8	3,8	3,9
2023	39,7	40,4	12,6	4,3	3,0
2024	44,5	36,1	12,0	4,2	3,3

Джерело: [163].

Відповідно, скорочення або призупинення контрактів одразу позначається на фінансових показниках сервісних компаній, тоді як продуктові ІТ-компанії завдяки диверсифікованій клієнтській базі, можливостям швидкого виходу на нові ринки збуту та адаптації продуктів до змін попиту змогли зберегти, а в окремих випадках і розширити свою ринкову присутність навіть в умовах високої економічної невизначеності та воєнних ризиків.

Показовим в аспекті структурних змін є той факт, що у 2024 році частка ІТ-фахівців, які працюють у продуктових компаніях (45 %), вперше за 14 років перевищила частку працівників сервісних компаній (36 %), тоді як у 2015 році співвідношення було протилежним: 50 % фахівців працювали в сервісних компаніях і 29 % у продуктових. Крім того, у 2025 р. вперше у п'ятірку найбільших роботодавців ІТ-сектору увійшли дві продуктові компанії – Genesis та Ajax Systems [202].

Також цікавим є той факт, що станом на літо 2025 р. у рейтингу "ТОП-50" вже представлено 21 продуктову компанію, 23 сервісні та 5 гібридних. При цьому всі дев'ять підприємств, що продемонстрували зростання штату на понад 10 % у першому півріччі 2025 року, належать до продуктового або гібридного сегмента [202]. Така динаміка ще раз підтверджує посилення ролі компаній, орієнтованих на створення власних технологічних рішень, у загальній структурі вітчизняної ІТ-галузі.

Водночас сегмент аутстафінгових компаній демонструє помірне, але стійке зростання (частка таких компаній збільшилась за 2015-2024 рр. на 27,7 %). Це пояснюється зростанням попиту на гнучкі формати залучення персоналу, особливо в умовах війни. Так, аутстафінг дозволяє компаніям-замовникам оперативно розширювати або скорочувати команди без довгострокових трудових зобов'язань та додаткових адміністративних витрат. Відповідно, зменшуються кадрові ризики, що пов'язані з утриманням постійного штату працівників. Самі аутстафінгові компанії при цьому мають відносно стабільний грошовий потік за рахунок найму та контрактної оплати своїх спеціалістів. Проте їхній фінансовий стан безпосередньо залежить від тривалості контрактів і своєчасності розрахунків з боку клієнтів.

Стартап-сегмент ніколи не був домінуючим на ІТ-ринку України. Його частка протягом усього досліджуваного періоду залишається відносно невисокою (від 4,2 до 5,6 %), із тенденцією до незначного зниження у 2022-2024 рр. Такі дані свідчать про наявність внутрішньої проблеми розвитку галузі – недостатню представленість вітчизняних компаній, орієнтованих на створення та масштабування власних технологічних продуктів, які не тільки задають темпи нарощування інноваційного потенціалу ІТ-сектору, а і стимулюють модернізацію інших галузей національної економіки.

Аналіз структури вітчизняного ІТ-ринку за розміром компаній свідчить про домінування малих та середніх підприємств (табл. 2.3), причому така тенденція зберігається протягом усього досліджуваного періоду з певними варіаціями. Якщо у 2015-2019 рр. в ІТ-секторі значну частку становили саме малі підприємства (41-42 %), що в принципі характерно для початкового етапу становлення та активного розширення галузі, то починаючи з 2020 р. відбувається поступове, але стабільне зростання питомої ваги середніх і великих ІТ-компаній. Найбільш помітним це збільшення було у 2021-2022 рр., які стали піковими для цифрового прориву в багатьох сферах суспільного життя, що зумовило максимальне зростання попиту на ІТ-рішення [163].

Розподіл компаній за кількістю працівників у 2024 році

Кількість працівників	Частка компаній на ринку, %
до 50	37
51-200	35
251-1200	17
Понад 1200	11

Джерело: [243].

Переважання на ринку малих та середніх підприємств визначає особливості фінансово-економічної діяльності суб'єктів господарювання ІТ-галузі. Розмір підприємства безпосередньо впливає на його можливості щодо розширення діяльності, акумулювання власного капіталу, фінансування довгострокових розробок і реалізації великих інноваційних проєктів.

Невеликі масштаби діяльності зазвичай дозволяють забезпечити оперативність у прийнятті управлінських рішень та швидке пристосування суб'єктів господарювання до змін ринкового середовища. Однак, з іншого боку, обмеженість власних фінансових ресурсів та складність доступу до альтернативних джерел фінансування, знижують інвестиційну активність, можливості реалізації дорогих R&D-проєктів та технологічного розвитку невеликих ІТ-компаній загалом. Середні та великі ІТ-підприємства завдяки більшій концентрації фінансових та кадрових ресурсів мають більші можливості залучення інвестицій та реалізації технологічно складних проєктів.

Тому зміни структури вітчизняного ІТ-сектору в бік зростання чисельності середніх та великих компаній свідчать про поступовий перехід галузі до більш стабільної та зрілої моделі розвитку. У результаті формується більш збалансована структура вітчизняного ІТ-ринку, яка посилює інвестиційний потенціал галузі.

Важливо також зазначити той факт, що за даними [202] станом на 2025 р. у п'ятдесяти найбільших ІТ-компаніях України зосереджено 79,1 тис. фахівців, що становить близько 26 % від загальної кількості ІТ-спеціалістів

країни. Тобто майже три чверті ІТ-спеціалістів працюють на середніх та малих підприємствах, що свідчить про високу роль малого та середнього бізнесу в забезпеченні зайнятості у вітчизняному ІТ-секторі.

На сьогодні в Україні лідерами за чисельністю ІТ-спеціалістів та обсягами отримуваних доходів залишаються такі великі компанії, як EPAM, SoftServe, GlobalLogic, Genesis та Ajax Systems тощо [202]. Вони виступають своєрідними «якорями стабільності» для галузі. Проте фінансова безпека ІТ-сектору в Україні визначається не лише діяльністю великих гравців, а також фінансовою стійкістю значної кількості малих і середніх компаній.

Український ІТ-сектор упродовж тривалого часу формувався як експортноорієнтована галузь, основні доходи якої генеруються за рахунок надання послуг та реалізації продуктів на зовнішніх ринках. Станом на 2024 рік переважна більшість вітчизняних ІТ-компаній (понад 90 %) працює з іноземними замовниками, що підтверджує домінування експортної моделі розвитку галузі [264].

Відповідно, експортноорієнтований характер галузі створює подвійний контур фінансової стійкості та безпеки: з одного боку, забезпечує високі валютні надходження, стабільні доходи та доступ до глобального ІТ-ринку, з іншого – робить галузь чутливою до кон'юнктури світового ІТ-ринку та економічного розвитку країн-партнерів.

На сьогодні конкурентні переваги українських ІТ-компаній на міжнародному ринку формуються завдяки сильним позиціям вітчизняної ІТ-індустрії в таких сегментах як: FinTech, GovTech, DefenceTech, кібербезпека тощо, наявності висококваліфікованих кадрів, високій якості виконання замовлень, а також невисокій вартості ІТ-послуг. До цього ще додається унікальний досвід роботи вітчизняних компаній у складних умовах війни та їх швидка адаптація до зовнішніх дестабілізуючих впливів і загроз. Усе це забезпечує збереження інтересу до українських ІТ-продуктів з боку іноземних клієнтів в умовах сьогодення.

Разом із тим сучасний розвиток українського ІТ-сектору відбувається в умовах посилення міжнародної конкуренції та певного уповільнення темпів зростання світового технологічного ринку. Тому необхідність розширення географії експорту та переходу від виконання окремих сервісних замовлень до створення власних технологічних продуктів із вищою доданою вартістю, наразі стає одним із факторів успішного розвитку українських ІТ-підприємств.

Одним із ключових показників, що відображає ефективність функціонування ІТ-сфери України, є загальна динаміка експорту ІТ-послуг (рис. 2.1). Упродовж 2013-2021 рр. в Україні спостерігається стійке та динамічне зростання експорту, коли його середньорічний приріст становив приблизно 23 %, що перевищувало середні темпи зростання світового ІТ-ринку. При цьому у 2020 р. вперше обсяги експорту комп'ютерних послуг перевищили обсяги експорту транспортних [267].

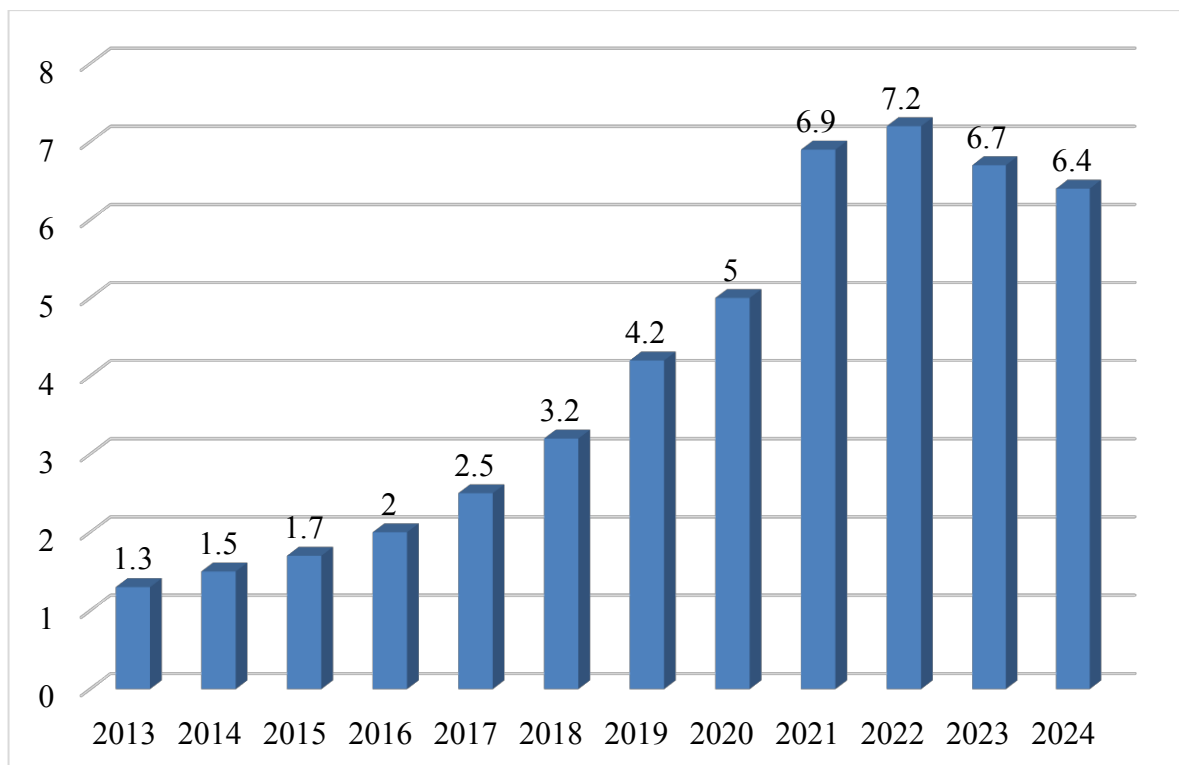


Рис. 2.1. Динаміка експорту ІТ-послуг, млрд дол.

Джерело: складено автором за даними [137].

І навіть попри війну ІТ-сектор у 2022 р. зміг зберегти позитивну динаміку, досягнувши рекордного обсягу в 7,2 млрд дол. у рік початку

повномасштабного вторгнення. Продовження у цей період дії довгострокових контрактів, швидка мобілізація ресурсів для підтримки безперервного функціонування компаній та релокація команд або зміна форм співпраці (віддалена робота) стали основними чинниками, що забезпечили такий результат. Фактично такі дії стали засобами підтримки фінансової стійкості бізнесу, дозволивши ІТ-компаніям уникнути масових зупинок діяльності.

Проте під впливом воєнних чинників вже у 2023-2024 рр. обсяги експорту ІТ-послуг знизились на 6,9 та 4,5% відповідно. У 2025 році ситуація дещо стабілізувалась. За даними [267] обсяг експорту ІТ-послуг у першому півріччі 2025 р., порівняно з аналогічним періодом 2024 р. зріс на 0,1 %. І хоча темпи зростання невеликі, але все ж таки спостерігається позитивний тренд порівняно з іншими галузями національної економіки.

Про системне зростання внеску галузі у формування валового внутрішнього продукту свідчить стабільне зростання частки експорту ІТ-послуг у ВВП України – з 0,7 % у 2013 р. до 3,4 % у 2024 р. (рис. 2.2).

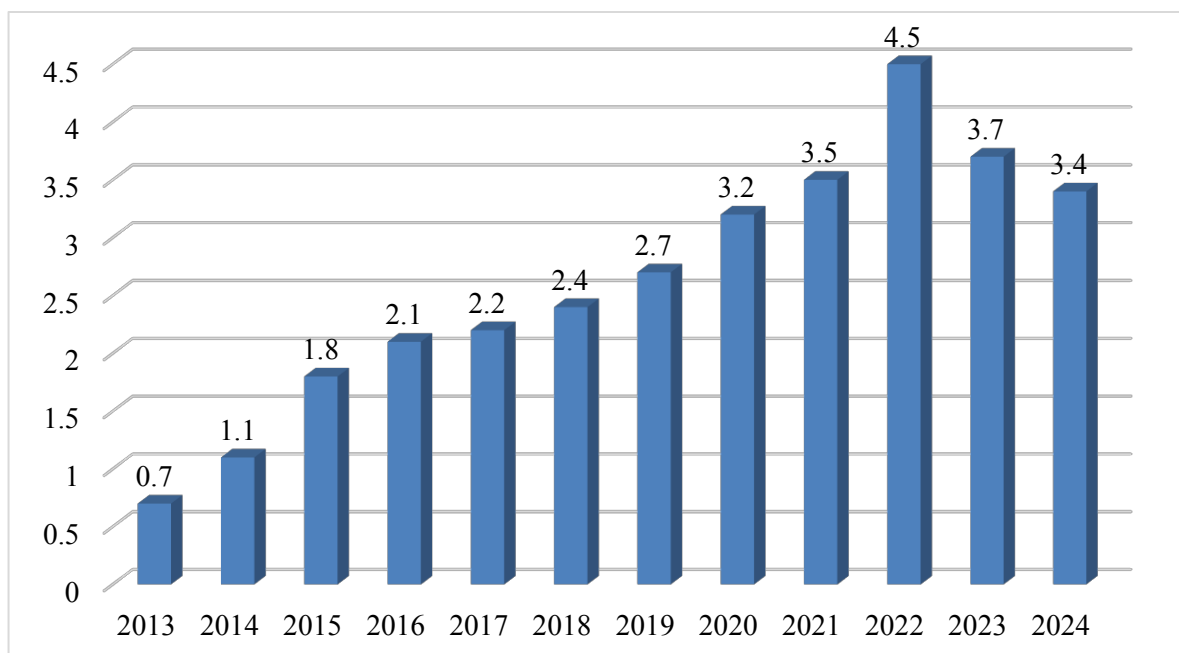


Рис. 2.2. Динаміка частки експорту ІТ-послуг у ВВП, %

Джерело: складено автором за даними [137].

Така динаміка підтверджує тенденцію посилення ролі ІТ-індустрії в економіці країни, зростаючу роль ІТ-сектору у забезпеченні макроекономічної

стабільності, формуванні національного доходу та зміцненні інвестиційного клімату, навіть в умовах військової агресії та економічної турбулентності.

При цьому скорочення даного показника у 2024 р. порівняно з 2022 р. на 24,4 % пояснюється загальним спадом економічної активності у зв'язку з повномасштабною війною. Також поступове відновлення та адаптація інших галузей економіки (оборонна промисловість, будівництво тощо) у 2024 р. позначилися на зміні структурних пропорцій експорту у ВВП України.

Навіть попри активні військові дії на території України ІТ-сектор продовжує залишатися ключовим джерелом валютних надходжень в економіку України, утримуючи статус найбільшого експортера послуг та забезпечуючи майже 37,4 % загального експорту послугу 2024 р. (рис. 2.3). І хоча частка ІТ у 2024 р. дещо знизилась у порівнянні з попередніми роками, що сталося, зокрема, й через часткове відновлення інших галузей (агропослуги, транспорт), ІТ-галузь зберігає провідні позиції у структурі експорту вітчизняних послуг.

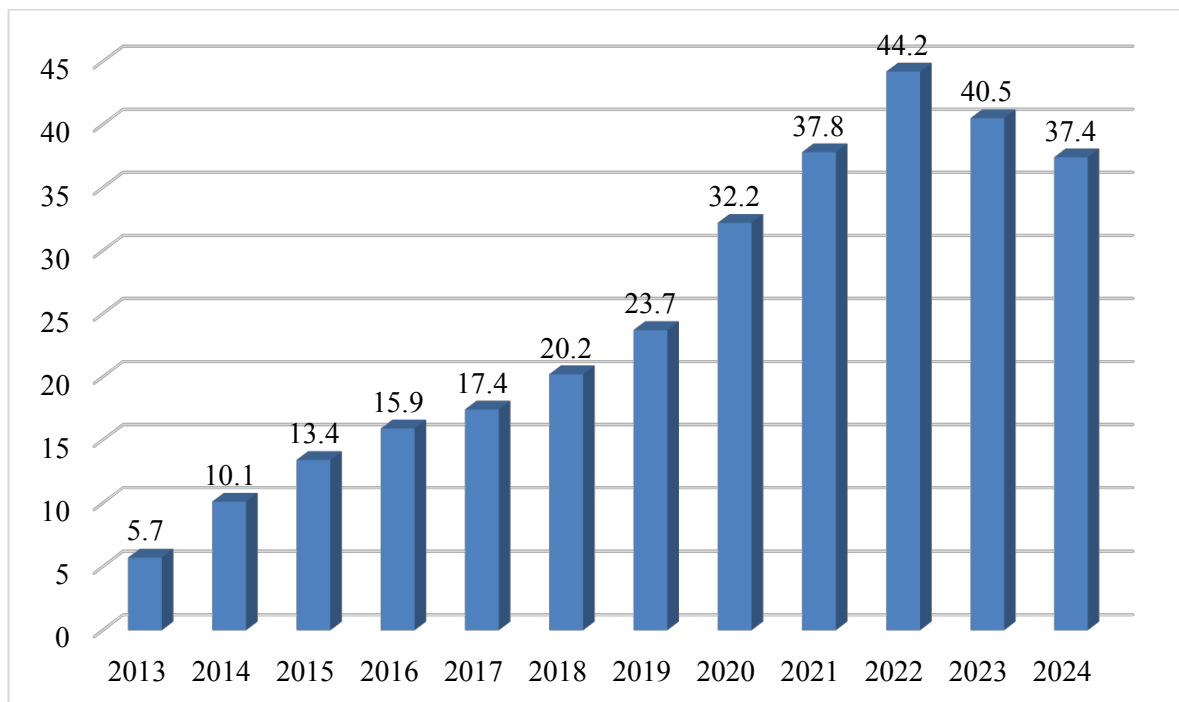
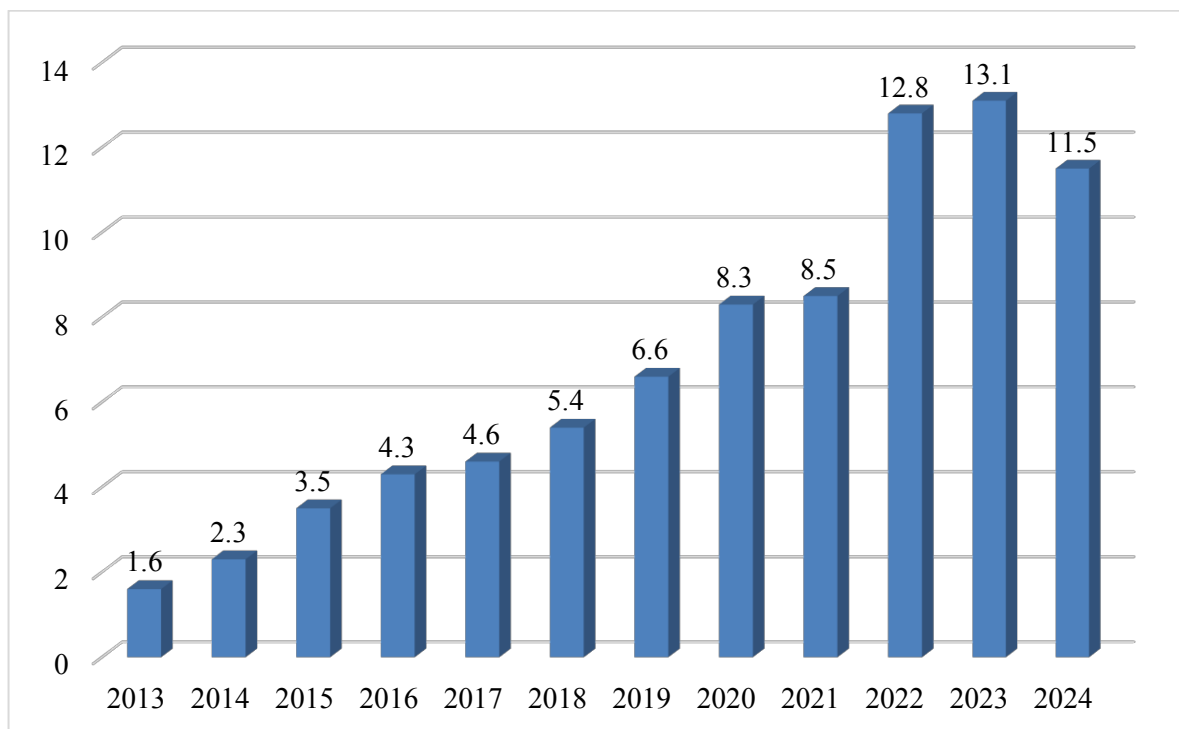


Рис. 2.3. Динаміка частки ІТ-послуг у загальному експорті послуг, %

Джерело: складено автором за даними [137].

Про зростаючу роль ІТ-індустрії як драйвера економічного розвитку України свідчить також суттєве збільшення питомої ваги експорту ІТ-послуг

серед інших галузей економіки з 1,6 % у 2013 р. до 11,5 % у 2024 р. (рис. 2.4). Варто зазначити, що структура українського експорту товарів і послуг є достатньо різноманітною, і хоча провідні позиції на сьогодні в ньому продовжує зберігати аграрний сектор, в останні роки ІТ-індустрія демонструє помітну позитивну динаміку, поступово посилюючи свою роль у формуванні експортного потенціалу держави. Насамперед це пов'язано з активними процесами трансформації економіки країни в бік високотехнологічних, інноваційно орієнтованих секторів, що стають у сучасних умовах більш експортно привабливими. Причому ІТ-сектор, на відміну від традиційних експортно орієнтованих галузей, здатний генерувати валютні надходження незалежно від фізичної логістики. Це в умовах війни робить його критично важливим для забезпечення валютної стабільності та фінансової безпеки держави.



**Рис. 2.4. Динаміка питомої ваги експорту ІТ-послуг
серед інших галузей економіки України, %**

Джерело: складено автором за даними [137].

Якщо говорити про основні іноземні ринки, на яких працюють українські підприємства ІТ-сфери, то на сьогодні вони залишаються

стабільними з погляду ключових партнерів. Як і десять років тому, у 2024 р. провідним імпортером залишаються США з обсягом імпорту на рівні 2397 млн дол. До трійки лідерів країн-імпортерів також належить Велика Британія – на другому місці (565 млн дол.) та Мальта – на третьому (501 млн дол.), яка часто використовується для міжнародних транзакцій. Ізраїлю було надано ІТ-послуг на 297 млн дол., Кіпру – на 397 млн дол., Швейцарії – на 266 млн дол., Німеччині – на 263 млн дол. тощо [243]. Цікавим є вибухове зростання експорту до Фінляндії (+49,8 %) та Латвії (+44,3 %) у першому півріччі 2025 року, що вказує на диверсифікацію ринків збуту в межах країн ЄС [132].

Вагомим чинником, що визначає успішність розвитку ІТ-галузі, є наявність висококваліфікованого людського капіталу. Саме кадровий потенціал виступає тим ключовим ресурсом, від якого залежить інноваційність, конкурентоспроможність та прибутковість діяльності вітчизняних ІТ-підприємств. В умовах війни та повоєнного відновлення цей чинник набуває ще більшого значення, адже стабільність роботи суб'єктів господарювання ІТ-бізнесу значною мірою пов'язана з якістю кадрових ресурсів та можливістю збереження професійної команди фахівців. Високий професіоналізм ІТ-спеціалістів та здатність швидко адаптуватись до нових викликів та змін формують конкурентні переваги українського ІТ-ринку праці та зумовлюють стабільний інтерес до нього з боку іноземних замовників.

Важливо зазначити, що в Україні сформувались три основні форми взаємодії між ІТ-спеціалістами та компаніями, кожна з яких має свої особливості та переваги як для працівників, так і для роботодавців:

- фізичні особи-підприємці – форма співпраці, за якої ІТ-спеціаліст працює як ФОП та укладає контракт з ІТ-компанією для виконання визначеного обсягу робіт за певними проєктами;
- наймані працівники – ІТ-спеціалісти, які перебувають у трудових відносинах з ІТ-компанією та є її штатними співробітниками;
- гіг-спеціаліст – ІТ-спеціаліст, який працює з компаніями-резидентами спеціального правового режиму Дія.City на підставі гіг-контракту.

При аналізі чисельності працівників ІТ-сектору України (табл. 2.4) слід розуміти, що один ІТ-спеціаліст може поєднувати декілька форм зайнятості або змінювати їх протягом певного часу.

Таблиця 2.4

Кількість працівників в ІТ-сфері України

Показник	2018	2019	2020	2021	2022	2023	2024
Кількість фізичних осіб-підприємців, тис. осіб	139,0	168,6	195,1	243,9	272,8	265,0	258,2
Кількість найманих працівників, тис. осіб	55,2	61,3	61,2	67,0	58,1	51,0*	23,0
Кількість гіг-спеціалістів, тис. осіб	-	-	-	-	5,9	23,2	35,0**
Загальна кількість зайнятих в ІТ-галузі, тис. осіб	194,2	229,9	256,3	310,9	336,8	339,2	316,2

Примітки. *У 2023 році Державна служба статистики України, як розпорядник даних, визначила, що деякі дані про працівників є конфіденційними. Тому кількість працівників в ІТ-компаніях оцінювалася як сума відкритих даних та оцінки закритих даних на основі середньої частки таких працівників у 2019-2022 роках. Дані за 2024 рік не повні.

**Оцінка базується на частці гіг-спеціалістів та загальній кількості ІТ-спеціалістів, які працюють у компаніях-резидентах Дія.City.

Джерело: [243; 245].

Протягом 2018-2023 рр. загальна кількість спеціалістів, зайнятих у вітчизняній ІТ-сфері, стабільно зростала, збільшившись за цей період майже на 63 %. Проте, з початком активної фази війни темпи зростання чисельності зайнятих в ІТ-галузі з 2023 р. суттєво уповільнились, а у 2024 р. взагалі вперше відзначається скорочення їх кількості на 6,8% порівняно з попереднім роком. На сьогодні однією з актуальних кадрових проблем для ІТ-сектору стала мобілізація ІТ-спеціалістів та їх вимушений виїзд за кордон. Іншим негативним чинником було скорочення працівників в ІТ-компаніях через зміни обсягів замовлень іноземних партнерів та загальне падіння активності ІТ-ринку. Таке скорочення або переформатування команд безпосередньо впливає на структуру витрат підприємств, насамперед на фонд оплати праці, що є однією з ключових статей витрат ІТ-компаній.

Зміни в кількості ФОП також мали суттєвий вплив на стан ринку праці в ІТ-секторі. Фізичні особи-підприємці з ІТ-КВЕДами завжди складали основну частину зайнятих у вітчизняному ІТ-секторі, де їх кількість за останні 10 років

зросла більше ніж у 3,5 рази. Водночас найм традиційно залишався більш поширеним в продуктових компаніях. Поширена в ІТ-бізнесі співпраця через ФОП відповідає його специфічному, переважно проєктному характеру роботи. ФОП-модель дозволяє спрощувати ведення обліку та оптимізувати податкове навантаження, але водночас створює передумови для прихованої зайнятості та роботи «в тіні».

Пік зростання чисельності активних фізичних осіб-підприємців припав на передвоєнні роки, коли щороку їх кількість зростала приблизно на 30 тис. осіб. Однак у період війни приріст ФОП був мінімальним. Так, протягом 2023 року кількість нових зареєстрованих ІТ-ФОП зменшилася вдвічі, а кількість закритих ФОП зросла у п'ять разів [1]. У 2024 році було зафіксовано рекордну кількість закритих ІТ-ФОП – майже 40 тис., проте їх частково компенсували 27 тис. нових реєстрацій, де майже половину склали жінки [187].

Результати галузевих досліджень засвідчують, що у 2025 р. відбувається суттєве скорочення фізичних осіб-підприємців в ІТ-галузі. Так, за даними ІТ Ukraine Association, частка фахівців, які працюють як ФОП у 2025 р. складала найнижче значення і становила лише 57 %, тоді як у 2024 р. їх було ще 70-75 %, а у 2022 р. аж 87 % [164].

Важливу роль у цих змінах відіграла поява з 2022 р. нової форми співпраці між ІТ-спеціалістами та компаніями – гіг-контрактів у межах правового режиму «Дія.City». Так, у 2024 р. кількість гіг-спеціалістів у резидентів «Дія.City» стрімко зросла майже в 6 разів порівняно з 2022 р. Розвиток цього сегменту відображає поступовий перехід частини ІТ-ринку до більш регламентованих та інституційно врегульованих трудових відносин. Для менеджменту ІТ-компаній перевагою такої форми співпраці стає зростання контролю над формуванням та роботою команд ІТ-фахівців та більша прогнозованість витрат на оплату праці. Як наслідок, це підвищує якість фінансового планування та управління витратами ІТ-підприємств.

Рівень оплати праці в ІТ-секторі на сьогодні стабільно залишається одним з найвищих на українському ринку праці та істотно перевищує середні

значення по національній економіці. Високі зарплати в ІТ-секторі визначають його привабливість для кваліфікованих фахівців та безпосередньо впливають на структуру витрат ІТ-підприємств, де оплата праці є їх ключовою статтею.

Найбільш інтенсивне зростання медіанної заробітної плати ІТ-фахівців (табл. 2.5) спостерігалось у 2017-2021 рр. Саме тоді активний розвиток ІТ-індустрії, високий попит на українських ІТ-спеціалістів на міжнародних ринках, а також посилення конкуренції між роботодавцями за висококваліфіковані кадри зумовили підвищення заробітної плати в ІТ з 1200 дол. у 2017 р. до 2500 дол. у 2021 р. При цьому темпи зростання становили від 13 до 25 % на рік, що значно перевищувало динаміку доходів у більшості інших секторів вітчизняної економіки.

Таблиця 2.5

Темпи зміни медіанної зарплати ІТ-фахівця на українському ІТ-ринку

Рік	Середня зарплата ІТ-фахівця, дол./міс.	Темпи зміни до попереднього року, %
2017	1200	-
2018	1500	+25
2019	1700	+13
2020	2000	+18
2021	2500	+25
2022	2200	-12
2023	2350	+7
2024	2500	+6

Джерело: [243; 245].

Проте у 2022 р. вперше за останні роки медіанна заробітна плата в ІТ-сфері знизилася на 12 %. В умовах повномасштабної війни через тимчасове призупинення дії частини експортних контрактів та скорочення кількості нових проєктів, ІТ-компанії були змушені переглядати підходи до управління витратами, зокрема й фондом оплати праці, адаптуючи свої бюджети та фінансові плани до нових реалій.

Протягом останніх десятиліть помітно зросла роль ІТ-сектору у формуванні державного та місцевих бюджетів. Аналіз обсягів податкових надходжень від ІТ-сектору України у 2019 – 2024 рр. демонструє стійку тенденцію до зростання фінансового внеску галузі в національну економіку

(табл. 2.6). Протягом зазначеного періоду обсяги сплачених податків ІТ-сектором збільшились у 2,5 раза. Це відображує не лише динамічний розвиток ІТ-індустрії, а й поступове посилення її фінансової значущості для національної економіки. Показово, що навіть в умовах повномасштабної війни ІТ-сфера демонструє здатність генерувати стабільні податкові надходження, тоді як інші галузі переживають різке скорочення економічної активності.

Таблиця 2.6

Обсяги сплачених податків ІТ-сектором України

Показник	2019	2020	2021	2022	2023	2024
Обсяги сплачених податків, млрд грн	16,8	19,7	27,8	32,2	35,9	41,6
Кількість платників податків від ІТ-сектору, тис.	176,9	203,7	253,5	281,7	273,1	266,8

Джерело: [243; 245].

Важливо зазначити, що зростання податкових надходжень відбувалось паралельно зі збільшенням кількості платників податків ІТ-сектору. Їх чисельність у період 2019-2022 рр. зросла у 1,6 раза, що свідчить не тільки про зростання зайнятості та високий рівень підприємницької активності в галузі загалом, а і про зростання ступеня легалізації діяльності в ІТ-сфері, в тому числі й через механізм Дія.Сіті.

Хоча у 2023-2024 рр. кількість платників податків дещо скоротилась, загальний обсяг сплачених податків продовжив зростати. Однією з причин цього стало зростання доходів окремих сегментів вітчизняного ІТ-бізнесу, насамперед корпоративного сектору, який демонструє посилення своїх позицій. Підтвердженням цього є той факт, що хоча формат ФОП традиційно залишається домінуючим видом співпраці в ІТ-сфері, саме юридичні особи формують дедалі більшу частку податкових надходжень. Причому в останні роки такі тенденції ще більше посилюються: у 2024 р. понад 58 % усіх податкових надходжень забезпечували саме юридичні особи, а за перше півріччя 2025 р. їхні податкові платежі перевищили податки від фізичних осіб-підприємців удвічі [188].

Такі тенденції пов'язані як зі скороченням кількості ФОП, так і з розширенням найму та активним впровадженням гіг-контрактів у межах спеціального правового режиму Дія. City. Станом на серпень 2025 року кількість резидентів Дія.City перевищила 2 210 компаній [61].

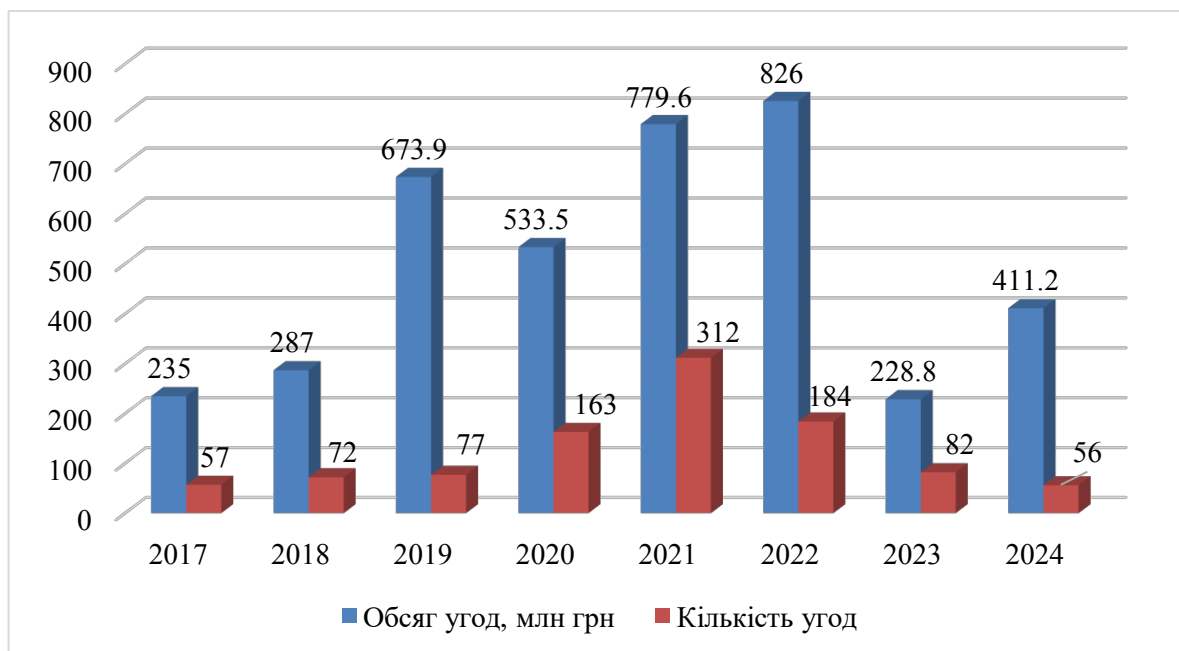
Завдяки прозорим умовам оподаткування, можливості застосування податку на виведений капітал, чітко визначеним умовам резидентства та новим форматам взаємодії з ІТ-фахівцями, вітчизняна ІТ-галузь поступово переходить до більш прозорих моделей ведення бізнесу, що сприяє детінізації оплати праці, зміцненню податкової дисципліни, розширенню податкової бази та зростанню бюджетних надходжень.

Так, у 2024 році резиденти сплатили 9,7 млрд грн прямих податків, що становить 27 % усіх надходжень від ІТ-сектору (проти 17 % у 2023 році) [85]. Також показовим є той факт, що саме резиденти сплатили 67 % усього ПДФО по ІТ-сектору, хоча в них працює значно менше людей, ніж зареєстровано ІТ-ФОП. Це свідчить про більшу прозорість заробітних плат, зменшення використання ФОП-схем та поступову легалізацію доходів.

Безумовно, додатковим чинником зростання обсягів податкових надходжень у 2025 р. стало підвищення податкових ставок. Зокрема, військовий збір для багатьох категорій, включаючи гіг-спеціалістів Дія.City, зріс з 1,5 до 5 %, а для ФОП 3-ї групи було впроваджено збір у розмірі 1 % від доходу [188; 85].

Поряд із фіскальним внеском важливим індикатором економічної ролі ІТ-сектору є його інвестиційна привабливість. Інвестиційний ринок України протягом останнього десятиліття пережив кілька хвиль стрімкого зростання і різких спадів. При цьому ІТ-галузь залишалась одним із небагатьох секторів національної економіки, який навіть у періоди загальноекономічних спадів та повномасштабної війни зберіг позиції «точки зростання». Про це свідчать як масштабні угоди за участю таких компаній, як Grammarly, Creatio та Allset, так і інтерес міжнародних інвесторів до українських активів, зокрема придбання Intellias та Digitally Inspired глобальними технологічними гравцями [206].

У період 2014 – 2023 рр. інвестиційний ландшафт українського ІТ-простору зазнав істотних змін (рис. 2.5). Після різкого спаду 2014-2015 рр., спричиненого початком російської агресії, ринок поступово відновлювався й уже у 2019-2021 рр. демонстрував рекордні показники залучення капіталу. Навіть ще у 2022 р., коли з початком повномасштабної агресії обсяги інвестицій в Україні різко впали, ІТ-сектор показав хоч і незначне, але зростання обсягів прямих та венчурних інвестицій. Хоча кількість укладених угод суттєво скоротилась. У 2023 р. інвестиційна активність в ІТ-галузі різко зменшилась, обсяг угод складав 228,8 млрд дол., а кількість – лише 82. Звісно, що у зв'язку з війною суттєво зріс рівень інвестиційної невизначеності, що одразу відобразилось на темпах та обсягах інвестування.



**Рис. 2.5. Динаміка прямих і венчурних інвестицій
на українському ІТ ринку**

Джерело: [245].

Загалом, під час війни внутрішні інвестиції зросли до 55 % за кількістю угод (проти 40 % у 2014–2021 роках), тоді як американські та європейські інвестори скоротили частку з 22 до 17 %, а з інших країн — з 16 до 11 % [206].

Поряд із цим відбулася і трансформація інвестицій за секторами. Якщо у 2021 р. ІТ і телеком займали 46 % інвестиційного ринку, то у 2024 році їхня частка зменшилася до 35 %. Натомість суттєво зріс інтерес до енергетики та оборонних технологій. Саме ці напрями, поряд із кібербезпекою, на сьогодні формують «ядро» нової економіки воєнного часу [206].

Проте, незважаючи на складні економічні умови та погіршення інвестиційного клімату, Україна продовжує приваблювати іноземних засновників. Так, лише у 2024 році було зареєстровано 1 109 компаній з іноземними власниками, хоча це на 24,2 % менше, ніж у 2023 р. При цьому навіть у воєнний час український ІТ-бізнес пропонує конкурентні можливості, адже серед нових зареєстрованих іноземних компаній друге місце займають компанії, що обрали сферу комп'ютерного програмування як основний вид діяльності близько 10 % (109). Найактивнішими засновниками стали представники Туреччини, Польщі та США [186].

Тобто можемо констатувати, що з одного боку інтерес іноземних інвесторів до ІТ-сфери зберігається. Але з іншого – змінюється її інвестиційний профіль. Скорочення кількості інвестиційних операцій, зміщення капіталу в бік оборонних технологій та енергетики вказують на перехід ІТ-галузі до більш стриманої моделі розвитку під впливом воєнної економіки та нових ризиків.

Не менш показовою та важливою для оцінки сучасного стану ІТ-сектору є динаміка розвитку української стартап-екосистеми, яка, попри війну, продовжує нарощувати інноваційний потенціал. По-перше, варто зазначити, що саме стартапи забезпечують формування нових технологічних рішень ІТ-сектору. В Україні понад 70 % активних стартапів мають ІТ-орієнтацію, а їхній розвиток безпосередньо відображає інноваційний потенціал галузі та її здатність перетворювати фінансові ресурси на нові технологічні продукти. По-друге, саме через стартапи на ринок заходить більша частина венчурного капіталу, формується попит на висококваліфікованих ІТ-фахівців і з'являються нові можливості для технологічного та економічного розвитку галузі.

За останні п'ятнадцять років українська екосистема стартапів еволюціонувала з локальних груп розробників у повноцінну інноваційну економіку. Станом на 2024 рік в Україні налічувалося близько 2600 активних стартапів, а країна посіла 46-те місце у світовому рейтингу Global Startup Ecosystem Index, піднявшись на 4 позиції за рік [263].

Водночас перший рік повномасштабного вторгнення став серйозним ударом для стартап-середовища – близько 12% команд взагалі припинили діяльність. Проте вже у 2023-2024 рр. в українському сегменті стартапів спостерігались ознаки його відновлення та адаптації. Так, понад 66 % засновників відзначили покращення становища своїх компаній, а 41 % збільшили команди порівняно з попереднім роком [260].

Утім, у реаліях сьогодення функціонування вітчизняного стартап-середовища супроводжується рядом суттєвих проблем. Навіть попри появу протягом 2022-2023 рр. в Україні близько 200 нових стартапів, та у 2024 році – укладання близько 100 інвестиційних угод на суму понад 350 млн дол. США [270], галузь стикається з дефіцитом фінансування, слабкою участю внутрішніх інвесторів та високою конкуренцією за інженерні кадри. Значна частина компаній змушена орієнтуватися на іноземні ринки та залучати капітал у зарубіжних юрисдикціях через недосконалість та нестабільність внутрішнього інституційного середовища.

За даними Українського стартапу фонду у першому півріччі 2025 року українські компанії залучили близько 180 млн дол. венчурних інвестицій, що на 12 % більше, ніж за аналогічний період 2024 року [251].

Нові потреби економіки та суспільства також змінюють і структуру ІТ-стартапів. У 2024 р. більшість продуктових компаній, що становлять ядро стартап-екосистеми, були зосереджені на проєктах у сфері програмного забезпечення та даних (40 %) і оборонних технологіях (19 %), які стрімко перетворились на новий драйвер інновацій. Зміна технологічної парадигми чітко простежується також у зростанні інтересу до кібербезпеки та штучного інтелекту. Разом з тим, частки FinTech (9 %), EdTech (8 %) та маркетингових

технологій (8 %) підтверджують збереження багатoproфільності вітчизняних ІТ-стартапів [260].

Особливе значення у формуванні інвестиційної привабливості України відіграють компанії-«єдинороги». За даними UVCA, українська екосистема вже створила сім «єдинорогів», і показово, що два з них отримали відповідний статус вже після початку повномасштабної війни [233]. Успіх Grammarly, GitLab, People.ai чи Firefly Aerospace формує потужний репутаційний імідж країни, демонструючи світовим інвесторам, що українські технології здатні розвиватися навіть у складних економічних та політичних умовах.

Утім, стійкість ринку ґрунтується на левовій частці венчурного капіталу, що надходила саме від іноземних інвесторів. У 2022 році 95,2 % загального обсягу венчурних інвестицій в українські проєкти забезпечили західні фонди, тоді як частка українських інвесторів становила лише 4,8 %. Водночас 76,5 % загального обсягу інвестицій припало лише на п'ять найбільших угод, що вказує на суттєву нерівномірність розподілу капіталу та обережність інвесторів [242].

Таким чином, попри очевидні досягнення, стартап-екосистема стикається з низкою проблем та обмежень:

- дефіцит фінансування для стартапів, що перебувають на стадіях активного масштабування. Тут домінує іноземний капітал, а українських фондів майже немає;
- активність бізнес-ангелів після 2021 року зменшилася більш ніж удвічі, що створює дефіцит початкового капіталу для стартапів;
- низький рівень R&D-інвестицій – лише 0,33 % ВВП, що у 5-6 разів менше, ніж у країнах ЄС;
- обмежений доступ до глобальних ринків, що знижує масштаби експорту технологічних продуктів та ймовірність швидкого зростання компаній [260].

Слід зазначити, що ІТ-галузь України має виражену регіональну специфіку, що сформувалася під впливом історичних, економічних, кадрових

та інфраструктурних чинників. Основними центрами концентрації вітчизняного ІТ-бізнесу залишаються Київ, Львів, Харків, Дніпро та Одеса. Проте, після початку війни розподіл ІТ-бізнесу за регіонами істотно змінився, що відбилося на загальній конфігурації ІТ-ринку.

Київ на сьогодні зберігає статус головного центру ІТ-індустрії та є незмінним лідером за кількістю ІТ-компаній, експортними надходженнями та чисельністю ІТ-фахівців. Безпосередньо у місті Києві зареєстровано 55,1% усіх ІТ-компаній України, де також генерується близько 67% сукупного чистого доходу галузі (станом на 2022 р.) [264]. Тут зосереджені головні офіси як великих сервісних компаній, так і продуктових розробників, дослідницьких центрів та представництв міжнародних корпорацій. Особливо помітним є зростання частки працюючих у продуктових компаніях столиці з 35 % у 2015 р. до 55 % у 2024 р. [264]. Водночас надмірна концентрація бізнесу в столиці робить ринок більш вразливим до інфраструктурних та безпекових ризиків.

Львів натомість істотно посилив свої позиції, ставши одним із ключових центрів релокації ІТ-бізнесу. За даними [264] станом на 2024 р. у Львові знаходиться 7,8 % ІТ-компаній та 18 % ІТ-спеціалістів. Висока активність Львівського ІТ-кластера створює потужну підтримку для бізнесу, сприяє співпраці бізнесу з університетами, підтримці стартапів та розвитку інноваційних центрів. Тобто на сьогодні цей регіон фактично перетворився на тил галузі, забезпечуючи безперервність роботи компаній, що були вимушені покинути східні області.

Для комплексної оцінки сучасного стану ІТ-сектору доцільно проаналізувати його структуру за сферами діяльності, адже галузева спеціалізація безпосередньо впливає на диверсифікацію доходів, ризик-профіль підприємств та їх фінансову стійкість.

Вітчизняні ІТ-компанії працюють в різних сферах. Якщо розглядати структуру вітчизняного ІТ-сектору в розрізі сфер діяльності, то за останні роки вона є відносно стабільною. На сьогодні найбільшими сегментами залишаються FinTech, електронна комерція та корпоративне управління. Так, у 2024 році більшість ІТ-компаній України були зосереджені на FinTech (15,3 %),

електронній комерції (13,8 %), програмному забезпеченні для підвищення продуктивності бізнесу (12,6 %), агротехнологіях (12,6 %), освіті (8,6 %) та кібербезпеці (9,2 %). Крім того, підприємства вітчизняної ІТ-сфери активно працюють у сферах робототехніки, ігрових технологіях та медицині [243].

Важливо зазначити, що збройна агресія стала каталізатором стрімкого розвитку нового потужного напрямку ІТ-сектору – Military Tech. На сьогодні радикально змінюється концепція сучасних бойових дій. Вони дедалі більше базуються на алгоритмах, інженерних розробках, технологічних рішеннях та системах автоматизованого управління. У таких умовах саме ІТ-сфера стає рушійною силою, що володіє значним потенціалом у напрямку модернізації оборонного сектору.

Безумовним позитивним аспектом розвитку вітчизняного ІТ-сектору стало суттєве посилення його ролі у процесах цифровізації державних послуг протягом останніх п'яти років. Одним із найуспішніших прикладів взаємодії держави та ІТ-бізнесу є впровадження в Україні національної платформи "Дія". Станом на 2025 р. кількість користувачів "Дії" в Україні досягла 23 млн [246], що свідчить про високий рівень інтеграції державних цифрових сервісів у повсякденну діяльність населення та бізнесу.

Крім «Дії», в Україні активно розвиваються й інші цифрові платформи в сфері GovTech - системи електронного документообігу, електронні платформи державних закупівель (наприклад Prozorro), інструменти цифрового податкового адміністрування тощо. Ефективна взаємодія ІТ-бізнесу та держави забезпечує додатковий обсяг замовлень для ІТ-компаній і стабільні джерела доходів.

Серед ключових напрямів розвитку українського ІТ-сектору особливе місце посідають фінансові технології. Фінансова сфера сьогодні є одним із найбільш динамічних сегментів цифрової трансформації, адже фінансово-кредитні установи масово переходять на цифрові рішення - від мобільних банківських сервісів до онлайн-кредитування. Для ІТ-компаній FinTech - це не просто новий напрям роботи, а й розширення ринків збуту, можливість

створення власних продуктів та вибудовування довгострокових стратегічних партнерств із банками та іншими фінансовими установами [275; 235].

Враховуючи результати представленого в цьому підрозділі аналізу, сформулюємо базові тренди, які на сьогодні притаманні розвитку ІТ-сектору України. Серед них доцільно виділити такі:

- попри вплив воєнних та економічних викликів, вітчизняний ІТ-сектор демонструє високу стійкість, швидку адаптацію, здатність до відновлення та нарощування експортного потенціалу, що дозволило йому зберегти ключові позиції на глобальному ринку та забезпечити валютні надходження до країни;

- зміцнення ролі ІТ як системоутворюючої галузі національної економіки, що забезпечує суттєву частку валютних надходжень, зростаючий внесок у ВВП та стабільне наповнення державного та місцевих бюджетів. Завдяки цьому ІТ-індустрія стає фундаментальним елементом фінансової стійкості та безпеки держави;

- збереження високої експортної орієнтації вітчизняних ІТ-компаній, що забезпечує стабільні валютні надходження, але й формує залежність від коливань світового ІТ-ринку та конкурентного тиску з боку інших країн;

- поступове зміщення фокуса від сервісної моделі до продуктового та змішаного формату діяльності підприємств ІТ-сфери, що свідчить про прагнення суб'єктів господарювання до створення власних продуктів, що сприяє підвищенню прибутковості та інноваційності вітчизняного ІТ-сектору;

- значна роль малого та середнього бізнесу в ІТ-секторі, що забезпечує гнучкість, мобільність та швидкість реагування вітчизняного ІТ-бізнесу на зовнішні виклики та загрози. Проте, саме МСП мають обмежені фінансові ресурси для розвитку і залишаються найбільш вразливими до ризиків;

- достатньо динамічний розвиток вітчизняних стартап-екосистем та їх висока привабливість для внутрішніх та зовнішніх інвесторів;

- зосередженість вітчизняного ІТ-бізнесу переважно у великих містах зі зміною з початком масштабної війни географії розміщення до більш безпечних регіонів;

- зменшення частки ІТ-ФОП та поширення найму і гіг-контрактів у межах правового режиму «Дія.City», що сприяє детінізації ринку праці та підвищенню прозорості трудових відносин;

- збільшення обсягів податкових надходжень та частки юридичних осіб у їхній структурі свідчить про поступову детінізацію ІТ-галузі та посилення її фіскальної значущості;

- активний розвиток GovTech-сегмента, що сприяє розширенню внутрішнього ринку ІТ-послуг та зниженню залежності галузі від зовнішнього попиту;

- формування та інтенсивний розвиток MilitaryTech, який стає важливою статтею експорту, одним із ключових драйверів технологічного оновлення ІТ-індустрії та зміцнення конкурентних позиції України на глобальному ринку оборонних технологій.

Таким чином, виявлені тенденції розвитку вітчизняного ІТ-сектору формують нову конфігурацію внутрішніх та зовнішніх загроз, а також ресурсних можливостей підприємств галузі, що зумовлює необхідність поглибленої діагностики їх фінансового стану та рівня фінансової безпеки.

2.2. Комплексна оцінка фінансового стану підприємств ІТ-сфери України

Важливим етапом оцінки фінансової безпеки підприємства є попередній комплексний аналіз його фінансового стану, адже саме результати такого аналізу формують інформаційну основу для подальшого визначення рівня фінансової безпеки та спроможності суб'єктів господарювання протистояти зовнішнім та внутрішнім загрозам.

У наукових дослідженнях [230; 215; 48] підкреслюється, що рівень фінансової безпеки підприємства визначається через низку фінансових параметрів та показників: структуру капіталу, ліквідність, фінансову стійкість, рентабельність, ділову активність тощо. Саме тому, як зазначає О. Дубинська, оцінювання фінансової безпеки має спиратися на ґрунтовне вивчення даних фінансової звітності та динаміки основних фінансових коефіцієнтів [48].

З огляду на вищезазначене, вважаємо за доцільне провести комплексний аналіз фінансового стану підприємств ІТ-сфери України, що дозволить сформувати основу подальшої кількісної оцінки рівня їхньої фінансової безпеки.

Фінансова стійкість будь-яких суб'єктів господарювання безпосередньо залежить від обсягів та ефективності використання фінансових ресурсів, що відображаються у структурі активів і капіталу підприємств. Збалансованість джерел фінансування та раціональне розміщення ресурсів в активах визначають здатність ІТ-компаній підтримувати стійке фінансово-економічне зростання, фінансувати інноваційний розвиток і своєчасно реагувати на зовнішні та внутрішні ризики і загрози. Для технологічного сектору доступ до фінансових ресурсів і ефективне управління ними визначають не лише рівень фінансової стійкості та платоспроможності, а й можливості масштабування бізнесу, виходу на нові ринки та формування конкурентних переваг у цифровій економіці.

Протягом 2013 - 2024 рр. загальний обсяг фінансових ресурсів підприємств вітчизняного ІТ-сектору (рис. 2.6) зріс з 18,5 млрд грн до 159,6 млрд грн, тобто більше ніж у 8,5 раза. Таке суттєве зростання активів ІТ-компаній свідчить про підвищення їхнього фінансового потенціалу, розширення господарського обігу та фінансових можливостей, а також активний розвиток галузі загалом.

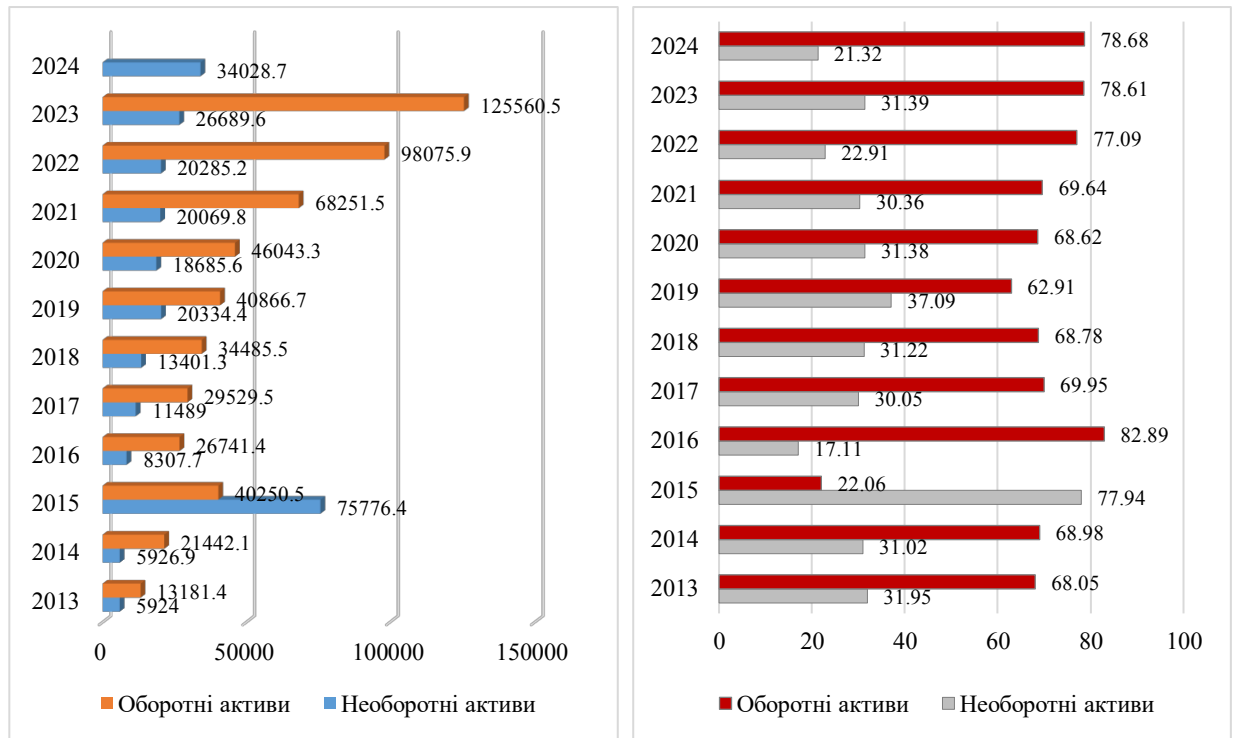


Рис. 2.6. Динаміка та структура активів підприємств ІТ-сфери України
Джерело: складено автором за даними [141].

Структура майна ІТ-підприємства за період 2013-2024 рр. відображує специфіку ІТ-бізнесу, а саме відносно невелику частку необоротних активів і домінування оборотних активів на рівні 68 -78 %, тобто тих активів, що не потребують значних довгострокових інвестицій у матеріальну базу. Також варто зазначити, що протягом досліджуваного періоду структура активів залишається практично стабільною, не дивлячись на економічні кризи, пандемію, повномасштабну війну тощо. Така стабільність характерна далеко не для всіх секторів національної економіки, особливо в умовах макроекономічної турбулентності.

Переважання оборотних активів є важливою перевагою ІТ-бізнесу у порівнянні з традиційними галузями економіки. Мобільність активів дозволяє ІТ-підприємствам підтримувати достатній рівень ліквідності та стабільну платоспроможність, забезпечувати маневреність та швидкість перебудови операційних процесів у відповідь на зовнішні виклики та загрози.

Особливу увагу привертає 2015 рік, коли відбулося різке зростання необоротних активів до 75,8 млрд грн, що становило 78 % від їх загальної величини. Така ситуація є нехарактерною для ІТ-галузі, а причини її виникнення не пов'язані зі змінами бізнес-моделей в ІТ. Передусім вона була зумовлена різкою девальвацією гривні, яка підвищила гривневий еквівалент валютних і не тільки активів підприємств. Штучність пікового росту необоротних активів 2015 року підтверджує й те, що вже у 2016 р. структура активів ІТ-компаній майже повертається до звичайної: понад 82 % становили оборотні активи, тоді як необоротні знизились до 17,11 %.

Протягом 2016-2021 рр. ІТ-галузь активно розвивається на тлі глобального запиту на цифрові технології: зростає експорт ІТ-послуг, відновлюється стабільність валютного ринку, удосконалюється фінансовий менеджмент, а ІТ-підприємства розширюються навіть без значних інвестицій в матеріальні активи. Тобто саме в цей період ІТ-сектор фактично формує ту фінансову гнучкість, що згодом стане його ключовою конкурентною перевагою та важливим чинником стійкості ІТ-сфери під час війни.

У 2022 - 2024 рр. на тлі повномасштабної війни відбувається подальше зростання мобільності активів ІТ-компаній, а частка оборотних активів досягає максимальних значень за весь досліджуваний період. Зазначені структурні зрушення стали наслідком зміни інвестиційних пріоритетів ІТ-підприємств та перерозподілу активів на користь більш ліквідних і мобільних форм з метою оперативного реагування на умови макроекономічної нестабільності. Зменшення капіталовкладень у необоротні активи обумовили скорочення їх питомої ваги у 2024 році до 21,32 %.

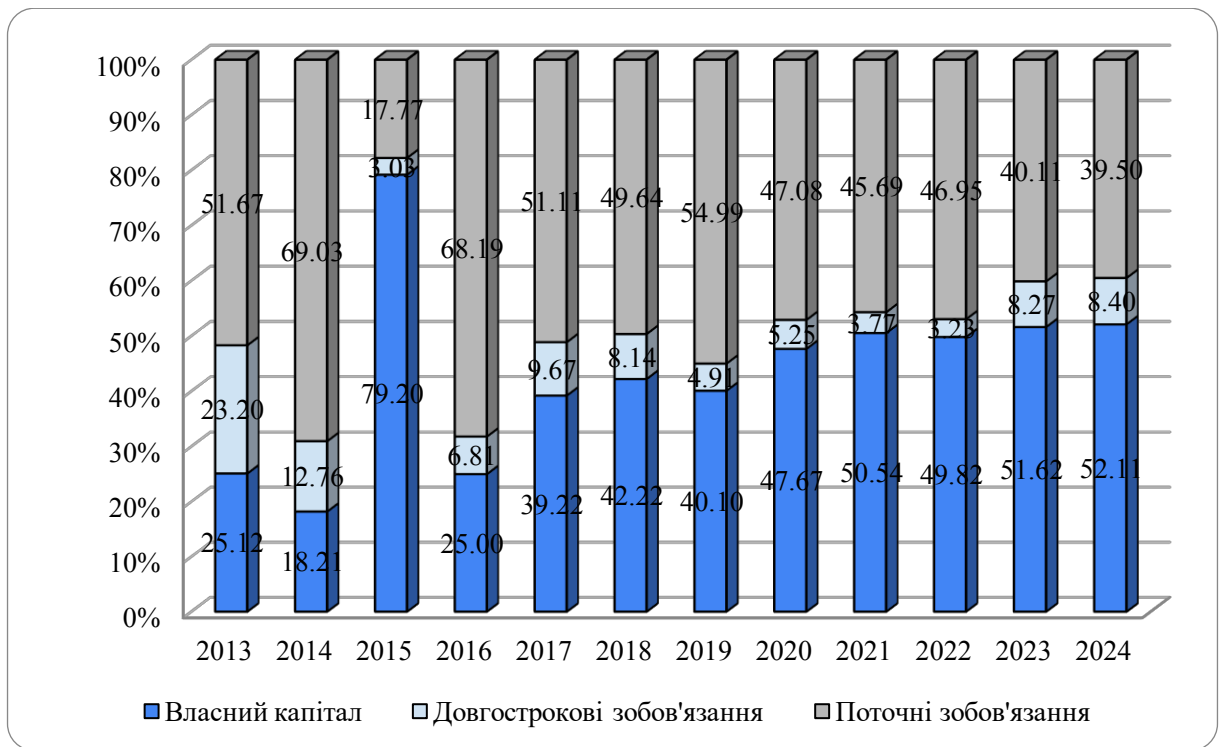


Рис. 2.7. Структура джерел фінансування підприємств ІТ-сфери України, %
Джерело: складено автором за даними [141].

У структурі джерел фінансування вітчизняних ІТ-компаній (рис.2.7) протягом 2013-2024 рр. простежується чітка тенденція до зростання обсягів та частки власного капіталу. Так, за досліджуваний період його величина зросла майже в 18 разів із 4,7 млрд грн у 2013 році до 83,5 млрд грн у 2024 році, а питома вага – з 25,12 до 52,11 % відповідно. Тобто відбувається зміна моделі фінансування в ІТ-секторі, що дозволяє сформулювати такі ключові тенденції:

- переважання власного капіталу у фінансуванні ІТ-компаній;
- поступове зниження залежності від короткострокових джерел фінансування;
- незначна роль довгострокових зобов'язань і забезпечень у фінансуванні ІТ-бізнесу.

Особливо швидке зростання власного капіталу відбулося у 2015 р., коли його обсяг досяг 77 млрд грн, а питома вага у структурі пасивів – 79,2 %, що стало рекордним показником за досліджуваний період. Таке різке зростання пояснюється кількома ключовими факторами.

По-перше, девальвація гривні у 2014-2015 рр. суттєво вплинула на ІТ-компанії, які працюють в експортноорієнтованому секторі та отримують дохід в іноземній валюті, а їхні фінансові результати номінуються в гривні. Це призвело до різкого зростання гривневого еквівалентну валютної виручки експортноорієнтованих ІТ-компаній, а отже, фінансових результатів та збільшення нерозподіленого прибутку як складової власного капіталу, хоча його реальний приріст був значно меншим.

По-друге, в умовах кризових явищ в економіці значна частина ІТ-підприємств була змушена переглядати підходи до формування та реалізації фінансової політики. Це проявлялося в оптимізації витрат, переоцінці активів та реструктуризації зобов'язань, що також мало вплив на зміну пропорцій між власними та позиковими джерелами фінансування підприємств ІТ-сфери.

Проте вже у 2016 р. структура капіталу ІТ-компаній стала більш збалансованою, а обсяги власного капіталу повернулися до економічно обґрунтованих рівнів після різких коливань попередніх років. У подальшому спостерігалось поступове вирівнювання ситуації, а починаючи з 2019 р. – відновлення стабільного зростання власного капіталу, зумовлене результатами операційної діяльності та накопиченням нерозподіленого прибутку. У 2021-2024 рр. частка власного капіталу перевищила 50%, що свідчить про поступове зменшення залежності ІТ-підприємств від позикових джерел фінансування та посилення їх фінансової автономії.

Свою позитивну роль у зростанні власного капіталу відіграло й запровадження спеціального податкового режиму «Дія.City», який у 2022-2024 рр. забезпечив більш передбачувані умови ведення бізнесу й тому спрацював як фактор зростання нерозподіленого прибутку в ІТ-секторі.

Довгострокові зобов'язання в ІТ-секторі у 2024 році порівняно з 2013 р. зросли в 5,6 раза та становили 13,4 млрд грн, тоді як у 2013 р. – 2,4 млрд грн. Питома вага довгострокових джерел фінансування коливалася протягом досліджуваного періоду на рівні 3,23 - 23,2% у різні роки. Упродовж останніх

двох років як обсяги, так і частка довгострокових зобов'язань суттєво зросла – з 3,23 % у 2022 р. до 8,4 % у 2024 р. Хоча ще у 2019-2022 рр. їхня частка залишалась досить низькою. Незначні обсяги довгострокових зобов'язань в ІТ-секторі значною мірою пояснюються активним притоком венчурного та приватного інвестиційного капіталу в українські стартапи, що дозволяє компаніям фінансувати розвиток переважно власними джерелами без суттєвого боргового навантаження. З початком повномасштабної війни, коли інвестиційний клімат у країні погіршився, підприємства були змушені більше залучати й довгостроковий зовнішній капітал.

Отже, можемо констатувати, що основними джерелами позикових коштів для вітчизняних ІТ-підприємств залишаються поточні зобов'язання і забезпечення. Їхній обсяг у 2024 році зріс до 63 млрд грн, що в 6,6 раза більше, ніж у 2013 році (9,6 млрд грн). У 2022-2024 рр. приріст поточних зобов'язань склав понад 50 %, хоча їхня питома вага у структурі капіталу дещо зменшилась і у 2024 році становила 39,5 %. Така структура позикових коштів з домінуванням поточних зобов'язань пояснюється специфікою ІТ-бізнесу, адже підприємства ІТ-сфери не потребують значних капіталовкладень у довгострокові матеріальні активи, що зменшує потребу в довгостроковому зовнішньому фінансуванні та, наприклад, лізингу.

Для більш ґрунтовної оцінки ступеня фінансової залежності ІТ-компаній від зовнішніх джерел необхідно проаналізувати систему показників фінансової стійкості за трьома групами коефіцієнтів: показниками структури капіталу, частковими показниками, що відображають зміни у структурі джерел фінансування та показниками, що характеризують джерела формування активів за 2013-2023 роки (табл. 2.7).

Таблиця 2.7

Показники фінансової стійкості підприємств ІТ-сектору України за 2013-2024 рр.

Показники фінансової стійкості	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
<i>Показники структури капіталу</i>												
Коефіцієнт автономії	0,251	0,182	0,792	0,250	0,392	0,422	0,401	0,477	0,505	0,498	0,516	0,521
Коефіцієнт фінансової залежності	3,981	5,491	1,263	4,000	2,550	2,368	2,494	2,098	1,979	2,007	1,937	1,919
Коефіцієнт концентрації позикового капіталу	0,749	0,818	0,208	0,750	0,608	0,578	0,599	0,523	0,495	0,502	0,484	0,479
Коефіцієнт фінансового ризику	2,981	4,491	0,263	3,000	1,550	1,368	1,494	1,098	0,979	1,007	0,937	0,919
Коефіцієнт фінансової стійкості	0,336	0,223	3,808	0,333	0,645	0,731	0,669	0,911	1,022	0,993	1,067	1,088
<i>Часткові показники, які відображають тенденції в зміні структури окремих джерел фінансування</i>												
Коефіцієнт довгострокового залучення позикових коштів	0,480	0,412	0,037	0,214	0,198	0,162	0,109	0,099	0,069	0,061	0,138	0,139
Коефіцієнт фінансової незалежності капіталізованих джерел	0,520	0,588	0,963	0,786	0,802	0,838	0,891	0,901	0,931	0,939	0,862	0,861
Коефіцієнт довгострокової фінансової стійкості	0,483	0,310	0,822	0,318	0,489	0,504	0,450	0,529	0,543	0,530	0,599	0,605
Коефіцієнт короткострокової заборгованості	0,69	0,844	0,854	0,909	0,841	0,859	0,918	0,9	0,924	0,936	0,829	0,829
<i>Показники, що характеризують джерела формування активів</i>												
Величина власного оборотного капіталу	3037,2	-8,5	4165,9	7136,8	7200,5	8218,0	4338,9	12827,6	15835,3	26682,2	48034,0	62528,8
Коефіцієнт маневреності власного капіталу	0,652	-0,002	0,054	0,588	0,480	0,453	0,197	0,452	0,474	0,605	0,746	0,752
Коефіцієнт забезпеченості оборотних активів	0,241	-0,001	0,194	0,177	0,269	0,278	0,126	0,314	0,344	0,391	0,490	0,498

Джерело: розраховано автором на основі [141].

Аналіз динаміки показників фінансової стійкості підприємств ІТ-сектору України за період 2013-2024 рр. підтверджує результати оцінки структури їхнього капіталу за даними балансу та демонструє поступове зміцнення фінансових позицій суб'єктів господарювання ІТ-галузі.

Найбільш критичним для фінансової стійкості ІТ-сектору виявився період 2013-2014 рр. Значне падіння коефіцієнта автономії до 0,182 та зростання коефіцієнта фінансового ризику до 4,491, разом зі зниженням величини власного оборотного капіталу до від'ємного значення (–8,5 тис. грн), відображають деструктивний вплив у цей період на ІТ-сферу певних макроекономічних факторів (девальвація гривні, падіння внутрішнього попиту та ВВП, банківська криза та обмеженість фінансових ресурсів).

Починаючи з 2015 р., фінансова стійкість ІТ-підприємств поступово відновлюється: зростає рівень фінансової автономії, знижується боргове навантаження, вирівнюється структура капіталу. Так, у 2024 р. коефіцієнт автономії досяг 0,521, коефіцієнт фінансового ризику знизився до 0,919, а коефіцієнт фінансової стійкості зріс до 1,088, що означає переважання власних джерел фінансування у структурі капіталу та зниження залежності від позикових коштів. Фактично галузь перейшла від кризового стану до стану з помірним рівнем фінансового ризику. За цей період ІТ-компанії наростили обсяги виручки та покращили фінансову результативність, що дозволило акумулювати власний капітал та створити більш стійку фінансову основу функціонування.

Динаміка величини власного оборотного капіталу додатково підтверджує ці тенденції. Його обсяги зросли з 3037,2 млн грн у 2013 р. до 62 528,8 млн грн у 2024 р., а коефіцієнт маневреності власного капіталу досяг 0,752, перевищивши нормативне значення 0,5. Тобто після кризового падіння цих показників підприємства ІТ-галузі зуміли акумулювати достатній обсяг власних ресурсів для фінансування операційної діяльності, що свідчить про посилення внутрішньої фінансової стабільності та наявність достатніх внутрішніх резервів для фінансування оборотних активів і зменшення ризиків ліквідності.

Аналіз часткових показників, що відображають зміни у структурі окремих джерел фінансування ІТ-підприємств України, підтверджує вищенаведені висновки щодо формування їхньої структури фінансування.

Після різкого зниження коефіцієнта довгострокового залучення позикових коштів до 0,037 у 2015 р. через загальноекономічні кризові явища та фактичне обмеження доступу до довгострокового кредитування, протягом наступних років спостерігається його повільне відновлення – до 0,139 у 2024 р. Це свідчить про поступове зростання довіри до галузі як об'єкта інвестування. І хоча масштаби такого залучення на сьогодні залишаються помірними, це певною мірою узгоджується з низькою капіталомісткістю ІТ-бізнесу.

Зростання коефіцієнта фінансової незалежності капіталізованих джерел з 0,520 до 0,861 додатково підтверджує, що довгострокова база фінансування підприємств ІТ-сфери формується переважно за рахунок власного капіталу.

Динаміка коефіцієнта покриття інвестицій у 2013–2015 рр. була нестабільною (0,483–0,822). Девальвація, фінансова турбулентність і обмежений доступ до фінансових ресурсів змусили частину ІТ-компаній переглядати інвестиційні плани та рішення. Проте вже починаючи з 2016 р. спостерігається стабілізація цього показника до 0,605 у 2024 р. Для ІТ-сфери, де інвестиції зосереджені у людському капіталі, R&D та цифрових рішеннях, така стабілізація є індикатором відновлення довгострокової фінансової спроможності.

Разом з тим, протягом усього періоду зберігається висока залежність підприємств ІТ-сфери від короткострокових зобов'язань (0,829-0,936), що відображає специфіку фінансово-господарської діяльності ІТ-компаній. Переважання короткострокових контрактів, значні обсяги авансових платежів, специфічний характер господарських операцій підприємств ІТ-сфери формують структуру зобов'язань, у якій переважають саме короткострокові. Хоча така залежність формально підвищує ризик втрати ліквідності та появу касових розривів, в ІТ-сфері це є цілком нормальним. Проте ключовим

моментом при цьому для фінансового менеджменту залишається ефективно управління ліквідністю, грошовими потоками та оборотним капіталом, а не механічне скорочення короткострокових зобов'язань.

Отже, проведений аналіз показників фінансової стійкості підприємств ІТ-сфери дозволяє зробити низку важливих висновків. По-перше, протягом 2013-2024 рр. в ІТ-галузі спостерігається поступове зміцнення фінансової стійкості ІТ-підприємств та достатньо збалансовану структуру джерел фінансування.

По-друге, зміни, що відбулись у структурі капіталу, по суті, відповідають економічній природі ІТ-сектору. Низька капіталомісткість, мінімальна потреба у матеріальних активах та орієнтація на експорт зумовлюють пріоритет власного фінансування та обмежене використання довгострокового боргу в господарській діяльності підприємств ІТ-сфери. Фінансова стійкість ІТ-компаній у цьому випадку формується не за рахунок масштабного залучення позикових ресурсів, а через акумулювання прибутку та нарощення власного оборотного капіталу.

По-третє, високий рівень короткострокової заборгованості є характерною рисою ІТ-бізнесу, а не ознакою фінансової нестабільності. Проте, така структура капіталу підвищує вимоги до фінансового управління (ліквідністю, грошовими потоками, дебіторською та кредиторською заборгованістю тощо).

Для здійснення комплексної оцінки фінансового стану підприємств ІТ-сектору після оцінки показників фінансової стійкості доцільно перейти до дослідження ліквідності (рис. 2.8). Аналіз динаміки показників ліквідності ІТ-підприємств України за 2013-2024 рр. засвідчує поступове зміцнення платоспроможності та підвищення їхньої здатності до виконання короткострокових зобов'язань без залучення зовнішнього фінансування. Позитивна динаміка ключових коефіцієнтів ліквідності вказує на формування запасу фінансової міцності та ліквідності, що знижує ризик виникнення касових розривів навіть в умовах воєнних загроз та макроекономічної нестабільності.

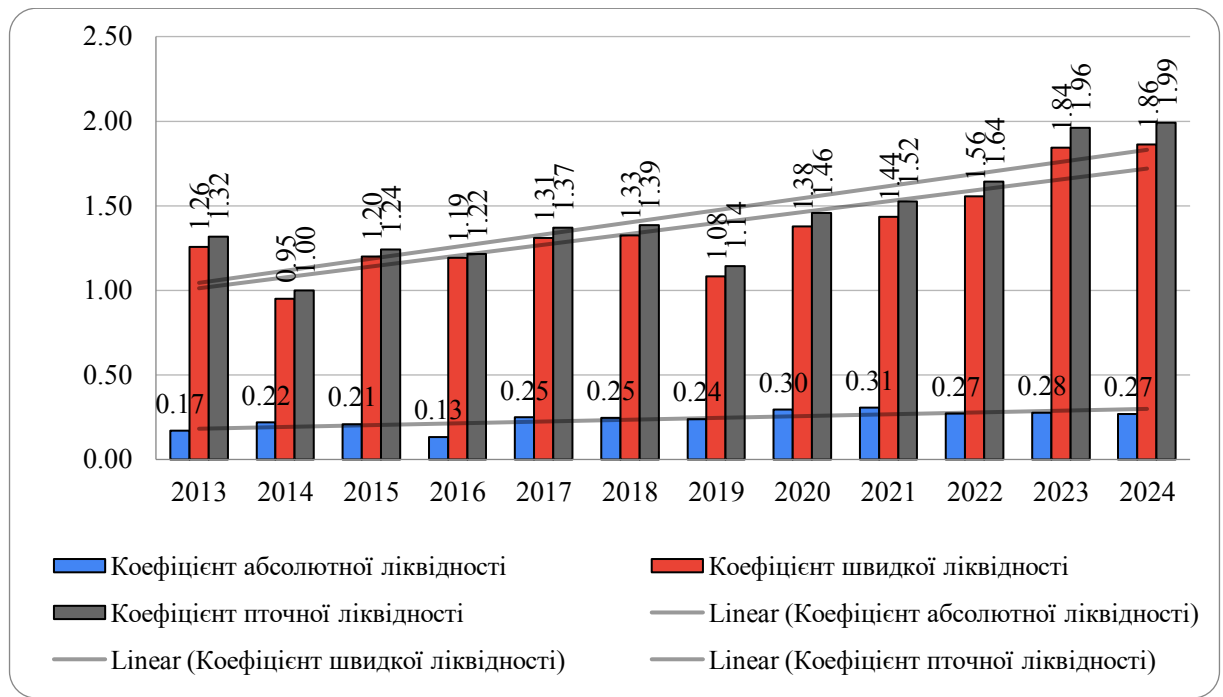


Рис. 2.8. Динаміка коефіцієнтів ліквідності ІТ-підприємств за 2013-2024 роки
Джерело: розраховано автором на основі [141].

Так, коефіцієнт абсолютної ліквідності за аналізований період зріс із 0,17 у 2013 році до 0,27 у 2024 році, наблизившись до нормативного рівня, що свідчить про нарощення обсягів грошових коштів та їхніх еквівалентів у структурі оборотних активів. Коефіцієнт поточної ліквідності ІТ-підприємств у 2013-2021 рр. перебував на рівні, близькому до мінімально допустимого й лише у 2022 р. досяг загальноприйнятого нормативного значення, що свідчить про наявність достатнього обсягу оборотних активів для покриття поточних зобов'язань.

Значне покращення демонструє коефіцієнт швидкої ліквідності, який збільшився на 46 % та суттєво перевищує нормативні межі. Це характерно для ІТ-сектору, оскільки оборотні активи таких підприємств, як правило, включають мінімальні запаси, але мають високий рівень грошових коштів, короткострокових фінансових вкладень та дебіторської заборгованості. Водночас надмірно високі значення коефіцієнта швидкої ліквідності можуть свідчити про накопичення оборотних активів, які не залучені до активного господарського обороту, що за певних умов потенційно знижує ефективність

їх використання і може негативно позначитися на рівні рентабельності. Для ІТ-підприємств така ситуація не завжди є негативною, однак потребує додаткової оцінки швидкості обігу ресурсів.

Саме тому доцільним є подальший аналіз ефективності використання оборотних активів шляхом оцінки показників ділової активності ІТ-підприємств (табл. 2.8).

Оцінка ділової активності підприємств ІТ-сфери України свідчить про зростання інтенсивності використання їхніх активів у господарському обороті у 2016-2021 рр., що відображає фазу активного розвитку та масштабування галузі. Так, у період до повномасштабної війни коефіцієнт оборотності активів зріс з 0,679 у 2016 р. до 2,443 у 2021 р., тобто більше ніж утричі. Це означає, що кожна гривня, вкладена в активи почала генерувати значно більший обсяг виручки, що свідчить про підвищення ефективності операційної діяльності та розширення господарського обороту ІТ-компаній.

Після 2022 р. динаміка ділової активності дещо змінюється. Зокрема, спостерігається певне уповільнення оборотності активів ІТ-компаній, що проявилось у зниженні загального коефіцієнта оборотності з 2,443 у 2021 р. до 1,781 у 2024 р. Така тенденція зумовлена випереджальним зростанням обсягів активів порівняно з темпами приросту виручки. Так, у 2024 р. обсяги активів ІТ-підприємств зросли у 1,28 раза, тоді як виручка – лише у 1,17 раза, що свідчить про зниження інтенсивності використання активів.

Аналогічні тенденції простежуються і за коефіцієнтом оборотності оборотних активів. Протягом 2016-2024 рр. він зріс більше ніж у двічі (з 1,605 до 3,532), що свідчить про високу інтенсивність використання грошових коштів, дебіторської заборгованості та інших оборотних ресурсів в процесі операційної діяльності. Натомість після 2022 р. показник знизився до 2,264 у 2024 р., що корелює зі збільшенням обсягу ліквідних активів і подовженням операційного циклу.

Таблиця 2.8

Динаміка показників ділової активності підприємств ІТ-сфери за 2016-2024 рр.

Показник	2016	2017	2018	2019	2020	2021	2022	2023	2024
Коефіцієнт оборотності активів	0,679	1,469	1,965	1,998	1,990	2,443	2,379	2,019	1,781
Коефіцієнт оборотності оборотних активів	1,605	1,903	2,834	3,051	3,021	3,532	3,219	2,590	2,264
Коефіцієнт оборотності постійних активів	1,287	11,949	11,278	10,131	9,595	12,116	13,798	14,132	13,349
Коефіцієнт оборотності робочого капіталу	8,761	8,890	10,344	15,555	13,260	10,710	8,652	5,765	4,580
Коефіцієнт оборотності запасів	48,545	49,191	49,835	46,676	42,395	48,294	47,368	35,852	27,637
Коефіцієнт оборотності дебіторської заборгованості	2,390	2,862	5,049	5,308	5,150	6,009	5,234	4,135	3,649
Коефіцієнт оборотності кредиторської заборгованості	4,986	5,524	5,923	6,678	6,792	7,781	7,641	6,816	6,594
Тривалість обороту оборотних активів, дн.	227,4	191,9	128,8	119,6	120,8	103,3	113,4	140,9	161,2
Тривалість обороту запасів, дн.	7,5	7,4	7,3	7,8	8,6	7,6	7,7	10,2	13,2
Тривалість обороту дебіторської заборгованості, дн.	152,7	127,5	72,3	68,8	70,9	60,7	69,7	88,3	100,0
Тривалість обороту кредиторської заборгованості, дн.	73,2	66,1	61,6	54,7	53,7	46,9	47,8	53,6	55,4
Тривалість операційного циклу, дн.	160,2	135,0	79,6	76,6	79,5	68,3	77,4	98,4	113,2
Тривалість фінансового циклу, дн.	87,0	68,9	18,0	21,9	25,7	21,4	29,7	44,9	57,9

Джерело: розраховано автором на основі [141].

Як бачимо, коефіцієнт оборотності необоротних активів у підприємств ІТ-галузі дуже високий протягом всього досліджуваного періоду (10-14 разів). Тобто ІТ-сектор генерує значні обсяги виручки від реалізації продукції при незначних вкладеннях у матеріальні ресурси. Тобто кожна гривня, інвестована в основні засоби, створює значно більший дохід, ніж у традиційних галузях.

Динаміка коефіцієнта оборотності робочого капіталу найбільш показово демонструє зміну фінансової політики ІТ-підприємств протягом 2016-2024 рр.: від інтенсивної моделі використання оборотних ресурсів із незначними запасами власного оборотного капіталу у 2016 – 2019 рр., до більш обережної політики накопичення власного оборотного капіталу в ковідний та воєнний період. Зниження показника до 4,58 у 2024 р. є наслідком суттєвого нарощення обсягів власного оборотного капіталу. Тобто можна говорити, що зменшення оборотності тут є результатом зміцнення фінансової стійкості, але водночас це означає певне зниження ефективності використання ресурсів ІТ-компаній у воєнні роки.

Високі значення коефіцієнта оборотності запасів (48-53 рази) у поєднанні з короткою тривалістю їх обігу (6,8–7,5 дня) протягом 2016-2021 рр. свідчить не стільки про ефективне управління товарними залишками, скільки про специфіку структури активів ІТ-бізнесу, оскільки їхня діяльність орієнтована переважно на створення нематеріальних продуктів та послуг, що не потребують тривалого зберігання у формі товарних запасів.

Певне подовження тривалості оборотності запасів можемо спостерігати протягом воєнних 2023-2024 рр., що пов'язано з порушенням логістичних ланцюгів, релокацією частини ІТ-бізнесу та збільшенням частки супутніх матеріальних витрат для забезпечення безперервності діяльності в умовах війни (придбання енергообладнання, облаштування нових робочих локацій, підтримка технічної інфраструктури тощо).

Коефіцієнт оборотності дебіторської заборгованості стабільно зростає протягом 2016-2021 рр. з 2,390 до 6,009, а відповідно середній строк її інкасації за цей період скоротився з 152,7 до 60,7 дня. Така тенденція свідчить про підвищення ефективності управління дебіторською заборгованістю:

скорочення термінів її інкасації, посилення контролю за розрахунками, а також запровадження більш ефективних підходів до управління грошовими потоками. Частково це також може відображати покращення платіжної дисципліни з боку контрагентів, що є особливо важливим для ІТ-компаній, орієнтованих на зовнішні ринки та дистанційну модель співпраці.

Проте, з початком повномасштабної війни спостерігається зворотна тенденція: середній термін погашення дебіторської заборгованості зріс до 100 днів у 2024 р., порівняно з 69,7 днями у 2022 р., що відображує уповільнення виконання платіжних зобов'язань контрагентами. Слід зазначити, що така тенденція є негативною в умовах сьогодення, оскільки збереження стабільності грошових надходжень є надзвичайно важливим для підтримання поточної платоспроможності та фінансової стійкості ІТ-підприємств.

Водночас тривалість обігу кредиторської заборгованості залишається стабільною (приблизно 47–55 днів), і темпи її зростання менші ніж у дебіторської. Це означає, що підприємства частково компенсують уповільнення надходжень від дебіторів шляхом використання відстрочки платежів постачальникам.

У результаті тривалість операційного циклу у 2016 – 2021 рр. стабільно скорочувалась та досягла 68,3 дня у 2021 р., що характеризує достатньо високу швидкість обігу фінансових ресурсів. Після 2022 р. тривалість операційного циклу почала зростати і у 2024 р. вже становила 113,2 дня, а тривалість фінансового циклу відповідно зросла до 57,9 дня. Це підвищує потребу в оборотному капіталі. Але водночас така динаміка свідчить про наявність у ІТ-підприємств достатнього внутрішнього фінансового ресурсу для покриття можливих касових розривів, що дозволяє підтримувати операційну діяльність без критичної залежності від короткострокових запозичень.

Для ІТ-бізнесу, що функціонує в умовах високої конкуренції, швидких технологічних змін та глобалізації, рівень прибутковості є визначальним показником ефективності діяльності та здатності ІТ-компаній фінансувати розвиток за рахунок власних ресурсів.

Аналіз фінансових результатів діяльності підприємств ІТ-сектору за 2013–2024 рр. (рис. 2.9) демонструє чітку зміну траєкторії розвитку галузі – від кризових явищ до стабільного нарощування обсягів прибутку. Зокрема, найбільш складним для галузі був період 2014 - 2015 рр, коли підприємства ІТ-сфери отримали чистий збиток (-263,8 та -585,0 млн. грн. відповідно). Проте, вже починаючи з 2016 року ситуація принципово змінюється: галузь виходить на стійкий позитивний тренд зростання прибутку до оподаткування та чистого прибутку.

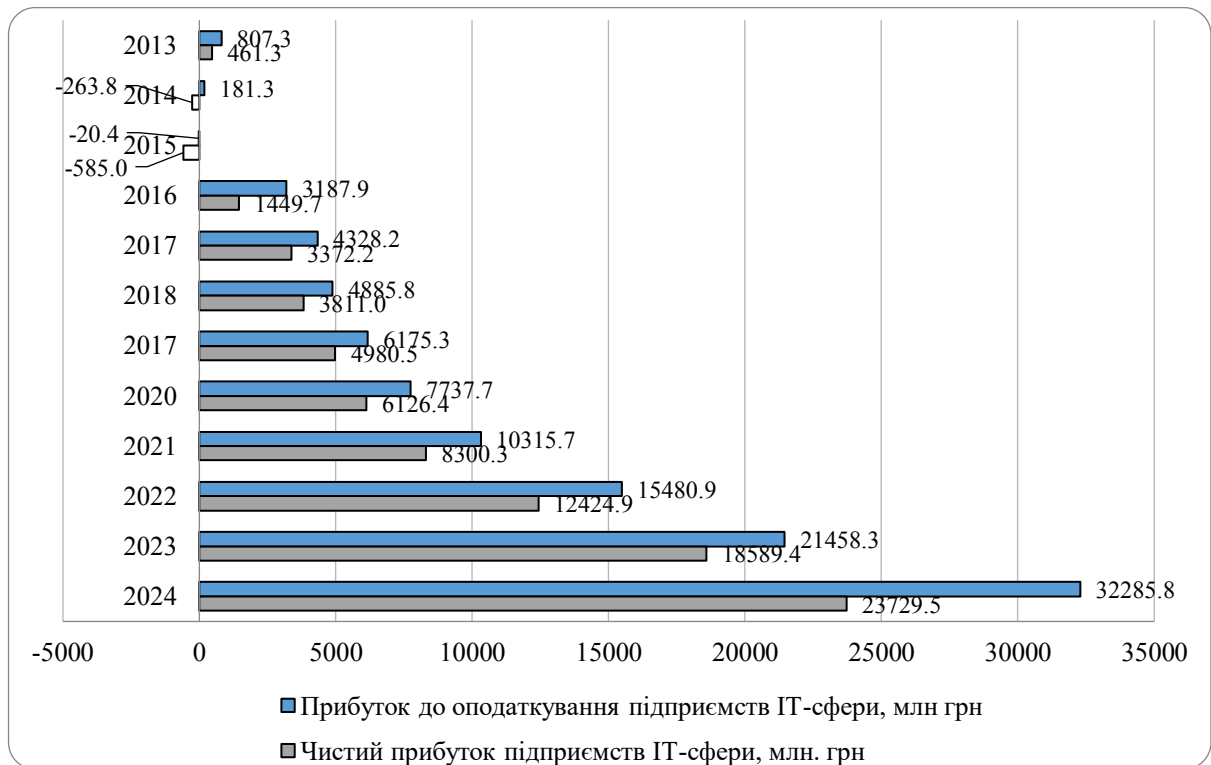


Рис. 2.9. Прибуток до оподаткування та чистий прибуток підприємств ІТ-сфери України

Джерело: складено автором за даними [141].

Особливо показовим у цьому контексті є період 2021-2024 рр., коли навіть в умовах повномасштабної війни ІТ-сектор зберіг позитивну динаміку прибутковості. У цей час суб'єкти господарювання ІТ-сфери змогли не тільки втримати фінансову спроможність, а і скористатись структурними змінами в економіці, що супроводжували кризові процеси. Прискорення цифровізації державних сервісів і бізнес-структур, стійкий попит на ІТ-продукти, різке

зростання потреб в ІТ-рішеннях у сфері оборонних технологій та кібербезпеки сформували нові ринки та напрями розвитку для вітчизняних ІТ-компаній. Це дозволило ІТ-галузі не просто виживати в умовах воєнного стану, а активно нарощувати економічний потенціал, компенсуючи загальне падіння ділової активності в інших секторах економіки [180]. У результаті роль ІТ-галузі у забезпеченні фінансової стійкості та безпеки національної економіки ще більше посилюється.

Динаміка чистої рентабельності продажу підприємств ІТ-сфери України (рис. 2.10) за 2015-2024 рр. демонструє якісну зміну ефективності галузі, поступове відновлення та послідовне зростання прибутковості після кризи 2015 року, коли показник мав від’ємне значення – 1,48 %. Уже у 2016 році підприємства змогли забезпечити позитивне значення рентабельності на рівні 2,93 %. Упродовж наступних років (2017-2021 рр.) рентабельність продажу поступово зростала. Фактично ІТ-галузь перейшла від фази відновлення до фази системного нарощування маржинальності.

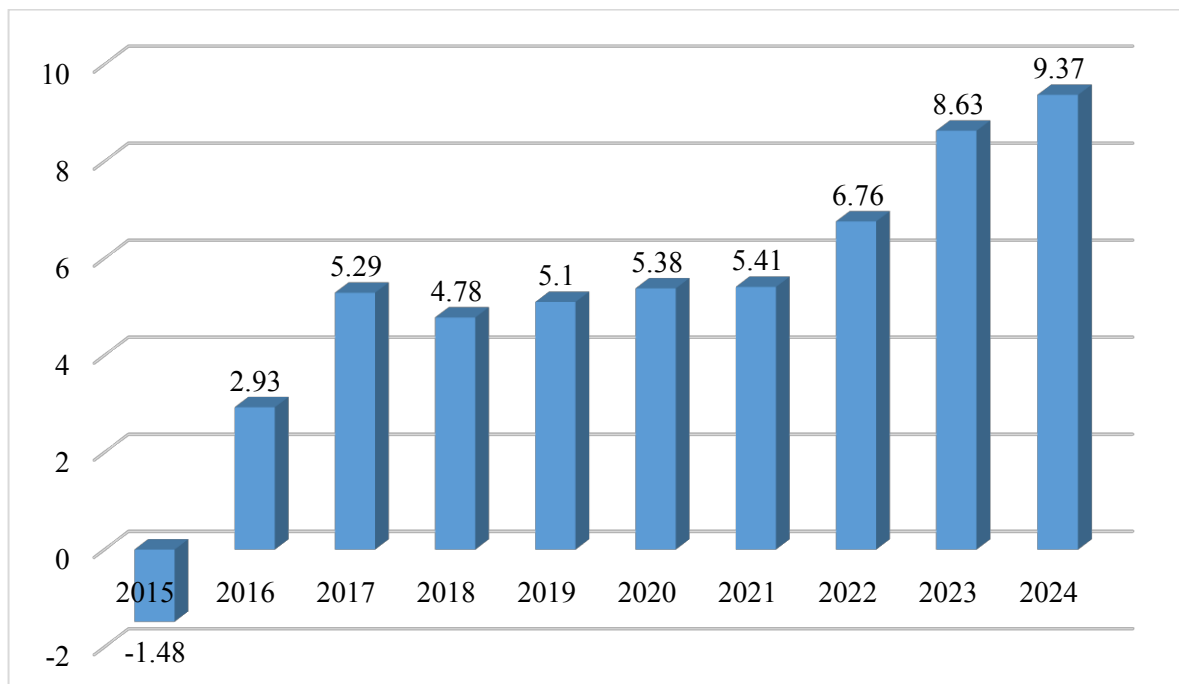


Рис. 2.10. Динаміка чистої рентабельності продажу підприємств ІТ-сфери за 2015-2024 рр.

Джерело: складено автором за даними [141].

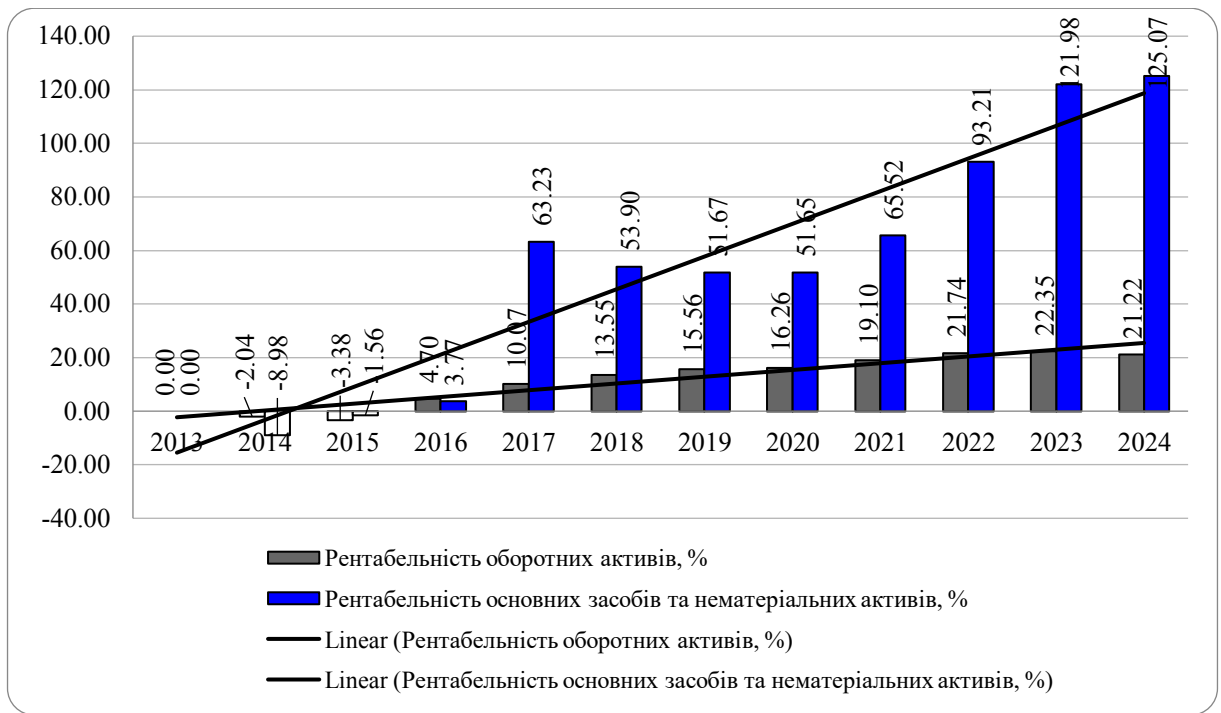
Найбільш показовою є динаміка 2022-2024 рр., коли рентабельність зросла з 6,76 % у 2022 р. до 9,37 % у 2024 р., навіть в умовах повномасштабної війни. Позитивна динаміка чистої рентабельності продажу пояснюється рядом особливостей ІТ-сектору:

- низька матеріаломісткість ІТ-бізнесу та відсутність значних витрат на основні засоби, що зменшує постійні витрати;
- експортна орієнтація ІТ-підприємств і значна частка валютної виручки, що дозволило частково нейтралізувати вплив внутрішніх макроекономічних проблем;
- гнучка структура витрат, що дає можливість коригування адміністративних та інших операційних витрат;
- переважання витрат на інтелектуальний капітал (персонал, розробку, R&D) над матеріальними витратами, створює умови для високої прибутковості операційної діяльності та формування більшої частки прибутку в структурі доходів підприємств [39].

Поглиблення оцінки прибутковості діяльності ІТ-підприємств потребує розгляду й аналізу ефективності використання окремих складових елементів активів, що дозволяє виявити, наскільки ефективно підприємства перетворюють наявні ресурси в прибуток і як саме використання різних типів активів впливає на загальну результативність господарської діяльності.

З огляду на специфіку ІТ-сфери, особливо важливо проаналізувати рентабельність оборотних активів, яка характеризує ефективність використання оборотних ресурсів у процесі операційної діяльності, а також рентабельність основних засобів та нематеріальних активів, що дає змогу оцінити результативність капіталовкладень у матеріально-технічну та інтелектуальну базу.

Аналіз динаміки рентабельності оборотних активів та рентабельності основних засобів і нематеріальних активів підприємств ІТ-сфери України у 2013-2024 рр. (рис. 2.11) демонструє суттєве зростання ефективності використання активів ІТ-галузі.



**Рис. 2.11. Динаміка показників рентабельності підприємств
ІТ-сфери України, %**

Джерело: складено автором за даними [141].

Так, рентабельність оборотних активів протягом досліджуваного періоду демонструвала поступове зростання. Якщо у 2013 - 2015 рр. значення показника були від'ємними (-2,04; -8,98 та -3,51 % відповідно), то вже з 2016 р. починається стійке зростання. У 2024 р. рентабельність оборотних активів досягла 21,22 %. Зростання цього показника корелює з підвищенням чистої рентабельності продажу та скороченням фінансового циклу і відображає тенденції прискорення обігу коштів, оптимізацію структури оборотних активів, зменшення періоду інкасації дебіторської заборгованості та зростання маржинальності операційної діяльності.

Ще більш наочною є динаміка рентабельності основних засобів та нематеріальних активів, яка зросла з 3,77 % у 2016 р. до 125,07 % у 2024 р. За відносно невеликого обсягу необоротних активів навіть помірне зростання прибутку призводить до значного підвищення їхньої рентабельності. Фактично, на кожен гривню, вкладену в основні та нематеріальні активи, формується кратно більший фінансовий результат. Переважна більшість ІТ-

компаній не має значного обсягу матеріальних активів, а виробничі потужності, транспортні засоби або нерухомість не відіграють ключової ролі в генеруванні доходу. Тоді як основна частина економічної цінності ІТ-сектору зосереджена передусім у людському капіталі, програмному забезпеченні, цифрових продуктах, ноу-хау, що не завжди повною мірою відображається у фінансовій звітності.

Унаслідок цього навіть відносно невеликий обсяг необоротних активів у поєднанні з високим прибутком формує статистично високі показники їхньої рентабельності, що треба враховувати під час інтерпретації цих показників та порівнянні ІТ-підприємств з суб'єктами господарювання традиційних галузей економіки.

Оцінка показників рентабельності власного капіталу (ROE) та рентабельності активів (ROA) підприємств України загалом за останні роки свідчить про їхню чутливість до макроекономічних потрясінь (рис. 2.12, 2.13).

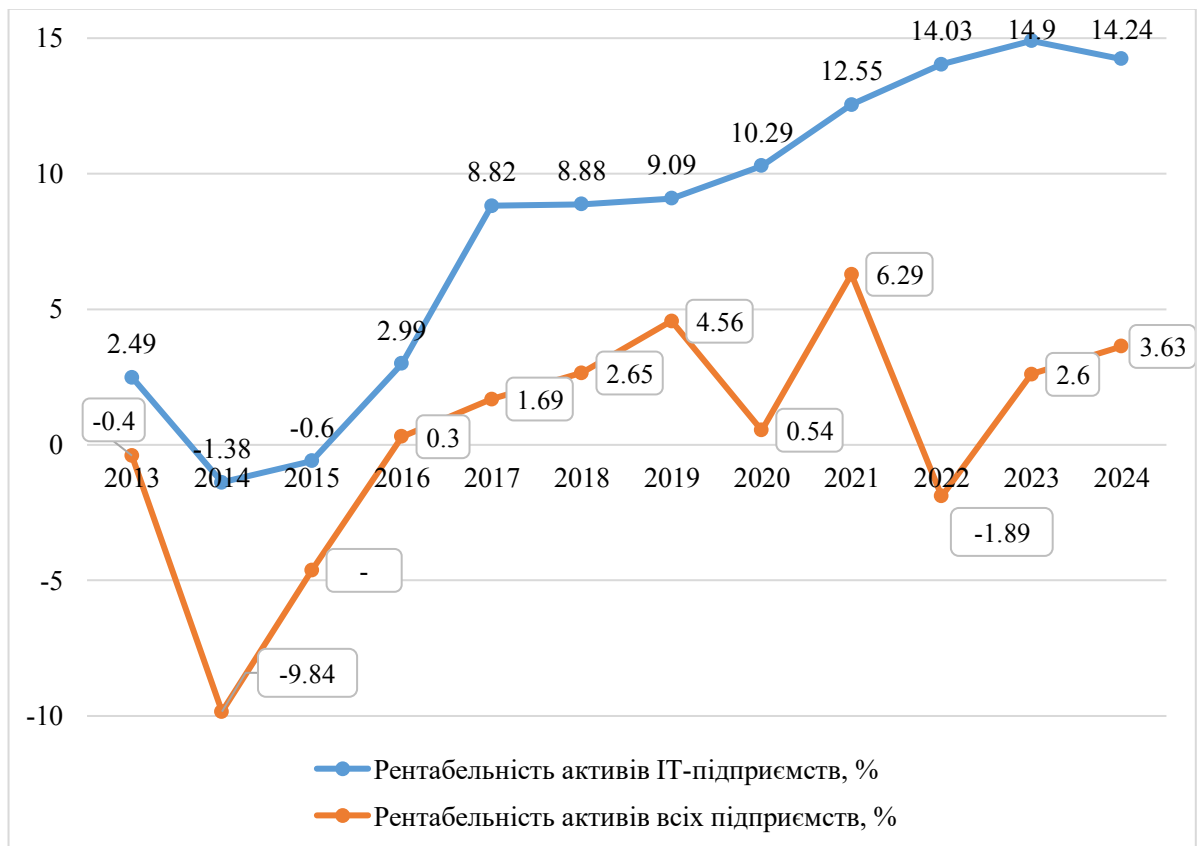


Рис. 2.12. Рентабельність активів підприємств ІТ-галузі та України

Джерело: складено автором за даними [141].

У 2022 році обидва показники навіть набули від'ємного значення. Зокрема, рентабельність власного капіталу підприємств України знизилася з 6,29 до -1,89 %, а рентабельність активів скоротилася з 21,52 до -6,95 %, що відображає масштабні деструктивні зміни в економіці, спричинені війною, руйнуванням виробничих потужностей, логістичними обмеженнями та скороченням внутрішнього попиту. Аналогічні достатньо глибокі просідання цих показників спостерігалися і у 2014 році.

На цьому фоні ІТ-сектор демонструє інші тенденції розвитку. Після кризового періоду 2013-2015 рр. ІТ-підприємства стабільно нарощують ефективність використання активів. Так, у 2023 р. ROA ІТ-сектору становив 14,9 %, у 2024 р. – 14,24 %, що суттєво перевищує середній показник по економіці (3,63 % у 2024 р.). І навіть у 2022 році, попри повномасштабну війну, ІТ-сектор України продемонстрував позитивний рівень прибутковості на відміну від традиційних секторів економіки. ІТ-компанії і на сьогодні зберігають здатність генерувати прибуток з кожної гривні активів більш ефективно, ніж інші підприємства.

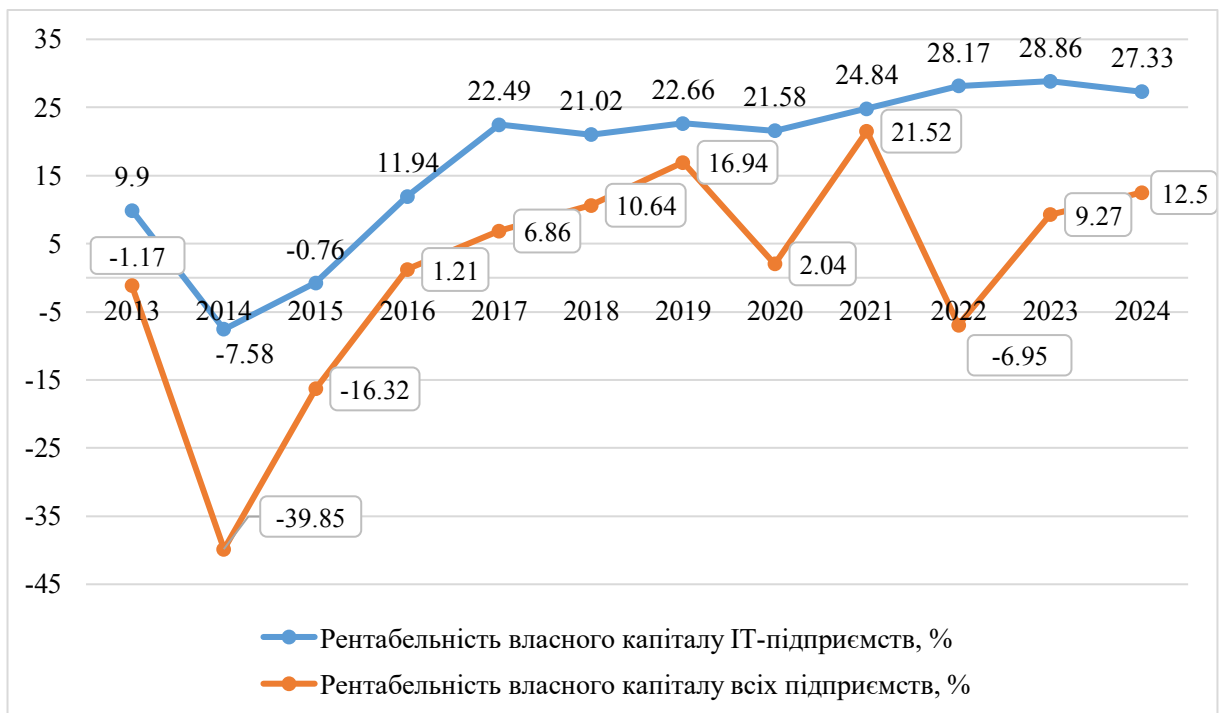


Рис. 2.13. Рентабельність власного капіталу підприємств ІТ-галузі та всіх підприємств України

Джерело: складено автором за даними [141].

Воєнний стан та макроекономічна нестабільність спричинили значні коливання рентабельності власного капіталу у загальному бізнес-секторі, що особливо помітно у 2014 році (-39,85 %) та 2022 році (-6,95 %) роках. Водночас ІТ-сектор пережив ці кризові періоди з меншими втратами. Підприємства ІТ-сфери демонструють значно вищий рівень рентабельності власного капіталу порівняно з аналогічним показником загалом по економіці України. Так, у 2024 році цей показник становив 27,33 %, тоді як середнє значення по всіх підприємствах становило лише 12,5 %. Тобто кожна гривня власного капіталу в ІТ-секторі генерує більш ніж удвічі вищу віддачу порівняно з іншим бізнесом країни.

Високий рівень рентабельності власного капіталу в ІТ-галузі є наслідком поєднання двох чинників: відносно стабільної операційної прибутковості та помірного рівня залучення власного капіталу, що знижує ризик різких коливань цього показника в кризові періоди. Лише у 2017 році обидва сектори продемонстрували синхронне зростання рентабельності власного капіталу, однак у наступні роки в економіці загалом цей показник значно коливався, тоді як по ІТ-сектору зберігалась стійка позитивна динаміка.

Узагальнюючи результати комплексного аналізу фінансового стану підприємств ІТ-сфери України, доцільно систематизувати їхні ключові відмінності порівняно з підприємствами традиційних галузей вітчизняної економіки (табл. 2.9).

Таблиця 2.9

Порівняльна оцінка параметрів фінансового стану підприємств ІТ-сфери та традиційних галузей економіки

Критерій оцінки фінансового стану	Підприємства ІТ-сфери	Підприємства традиційних галузей економіки
1	2	3
Структура капіталу	- домінування власного капіталу у структурі фінансування; - зниження коефіцієнта фінансового ризику	- висока залежність від позикового капіталу; - зниження фінансової автономії у періоди криз.

Закінчення таблиці 2.9

1	2	3
Структура зобов'язань	- переважання поточних зобов'язань при помірному рівні боргового навантаження; - відносно низька частка довгострокових зобов'язань.	- висока частка банківських кредитів; - значне довгострокове боргове навантаження
Структура активів	- переважання оборотних активів (частка необоротних активів 17–38 %); - низька капіталомісткість; - висока мобільність активів	- значна частка необоротних активів - висока капіталомісткість; - великі обсяги запасів товарно-матеріальних цінностей; - недостатня мобільність активів
Ліквідність	- стійке зростання коефіцієнтів ліквідності; - низький ризик дефіциту ліквідності; - формування запасу фінансової міцності	- погіршення платоспроможності у кризові роки; - вища волатильність ліквідності; - ризик дефіциту грошових коштів
Рентабельність	- вищий рівень ROA та ROE порівняно із середнім по економіці; - збереження позитивної рентабельності у кризові періоди (2022 р.); - висока маржинальність; - висока рентабельність необоротних активів	- помірний або низький рівень рентабельності; - у кризові роки – від'ємні значення показників рентабельності; - повільніше відновлення після криз.
Ділова активність	- скорочення тривалості фінансового циклу; - висока оборотність активів; - ефективне управління дебіторською та кредиторською заборгованістю; - швидке перетворення оборотного капіталу у грошові потоки та прибуток	- більша тривалість фінансових циклів; - нижча оборотність активів; - значна залежність від запасів і матеріальних ресурсів; - уповільнене повернення вкладених коштів.
Фактори фінансової стійкості	- висока частка інтелектуального капіталу; - експортна орієнтація; - гнучка структура витрат; - низька капіталомісткість	- висока залежність від фізичної інфраструктури; - більша залежність від внутрішнього попиту; - значні обсяги постійних витрат; - підвищена залежність від кредитних ресурсів

Джерело: складено автором.

Представлена порівняльна характеристика фінансового стану підприємств ІТ-сфери та традиційних галузей економіки підтверджує наявність суттєвих відмінностей у їхній структурі активів, капіталу та прибутковості. На відміну від підприємств традиційних секторів, ІТ-компанії

більшою мірою орієнтовані на власні джерела фінансування, мають високу мобільність активів, домінування оборотних і нематеріальних активів, а також здатні генерувати вищу норму прибутковості на одиницю вкладених ресурсів. Саме ці особливості фінансового стану суб'єктів господарювання ІТ-сектору формують специфічні передумови забезпечення їхньої фінансової безпеки.

Проведений комплексний аналіз фінансового стану підприємств ІТ-сфери України за 2013-2024 рр. показав, що їхня фінансово-господарська діяльність набула стійких рис, що забезпечують високу адаптивність до макроекономічних і геополітичних викликів. Упродовж досліджуваного періоду ІТ-підприємства продемонстрували поступове зміцнення фінансової автономії, зростання ліквідності, покращення показників ділової активності та стабільну позитивну динаміку прибутковості навіть в умовах повномасштабної війни.

Проте аналіз фінансового стану на основі окремих показників фінансової стійкості, ліквідності, ділової активності та рентабельності не дозволяє отримати повну кількісну оцінку рівня фінансової безпеки підприємств ІТ-галузі. Наявність позитивної динаміки окремих показників не завжди свідчить про системну збалансованість фінансового стану та стійкості до зовнішніх та внутрішніх загроз, не дає цілісного кількісного уявлення про рівень фінансової безпеки галузі загалом і в динаміці.

Саме тому наступним етапом дослідження є проведення інтегрального оцінювання фінансової безпеки підприємств ІТ-сфери, яка дозволить:

- узагальнити результати комплексного фінансового аналізу;
- кількісно виміряти рівень фінансової безпеки підприємств ІТ-сфери та оцінити її динаміку за відповідні періоди;
- оцінити глибину кризових спадів і швидкість відновлення галузі;
- сформувати аналітичне підґрунтя для розробки механізмів забезпечення фінансової безпеки ІТ-компаній.

Таким чином, визначення інтегрального узагальнюючого показника є логічним продовженням проведеного аналізу та дозволяє перейти від оцінки окремих параметрів фінансового стану до комплексного виміру рівня фінансової безпеки ІТ-сектору України.

2.3. Методологічні засади оцінки фінансової безпеки підприємств ІТ-сфери в умовах цифрової економіки

У сучасних умовах будь-яке підприємство функціонує як динамічна система, фінансова стійкість і рівновага якої не статична, тому виникає потреба в постійному моніторингу рівня фінансової безпеки. Це надає можливість своєчасно виявляти наявні проблеми та реагувати на них без загрози втрати платоспроможності та фінансової стійкості. Традиційні підходи та методи оцінки фінансової безпеки підприємств, що представлені в науковій літературі, розглядаються переважно для підприємств реального сектору економіки та орієнтовані на їхні особливості: фондомісткість та капіталомісткість, матеріальне виробництво, прив'язка до фізичної інфраструктури, стабільність виробничого циклу та відносно передбачувані ринкові умови. Однак ІТ-сфера має принципові відмінності, що зумовлюють необхідність адаптації методичних підходів до оцінки фінансової безпеки саме цих підприємств [148].

Такий підхід повинен враховувати як загальноекономічні принципи, так і галузеву специфіку функціонування зазначених суб'єктів господарювання в умовах цифрової економіки, а також забезпечувати інтеграцію фінансової аналітики з якісною оцінкою важливих чинників, що здійснюють істотний вплив на рівень фінансової безпеки підприємств ІТ-сфери [148].

Недостатня розробленість методичних підходів до оцінювання рівня фінансової безпеки саме в контексті відображення специфіки ІТ-сектору вимагає вдосконалення відповідної методологічної бази, що дозволить проводити якісну діагностику стану фінансової безпеки ІТ-підприємств для забезпечення їхнього сталого розвитку та адаптації до сучасних викликів та загроз цифрової економіки [148].

Дослідження та систематизація теоретико-методологічних підходів до оцінки фінансової безпеки підприємств свідчать, що у науковій літературі та на практиці сформувалась низка важливих підходів до визначення її рівня, вибір яких залежить від специфіки та сфери діяльності суб'єкта господарювання, цілей дослідження та умов зовнішнього середовища (рис. 2.14) [148].

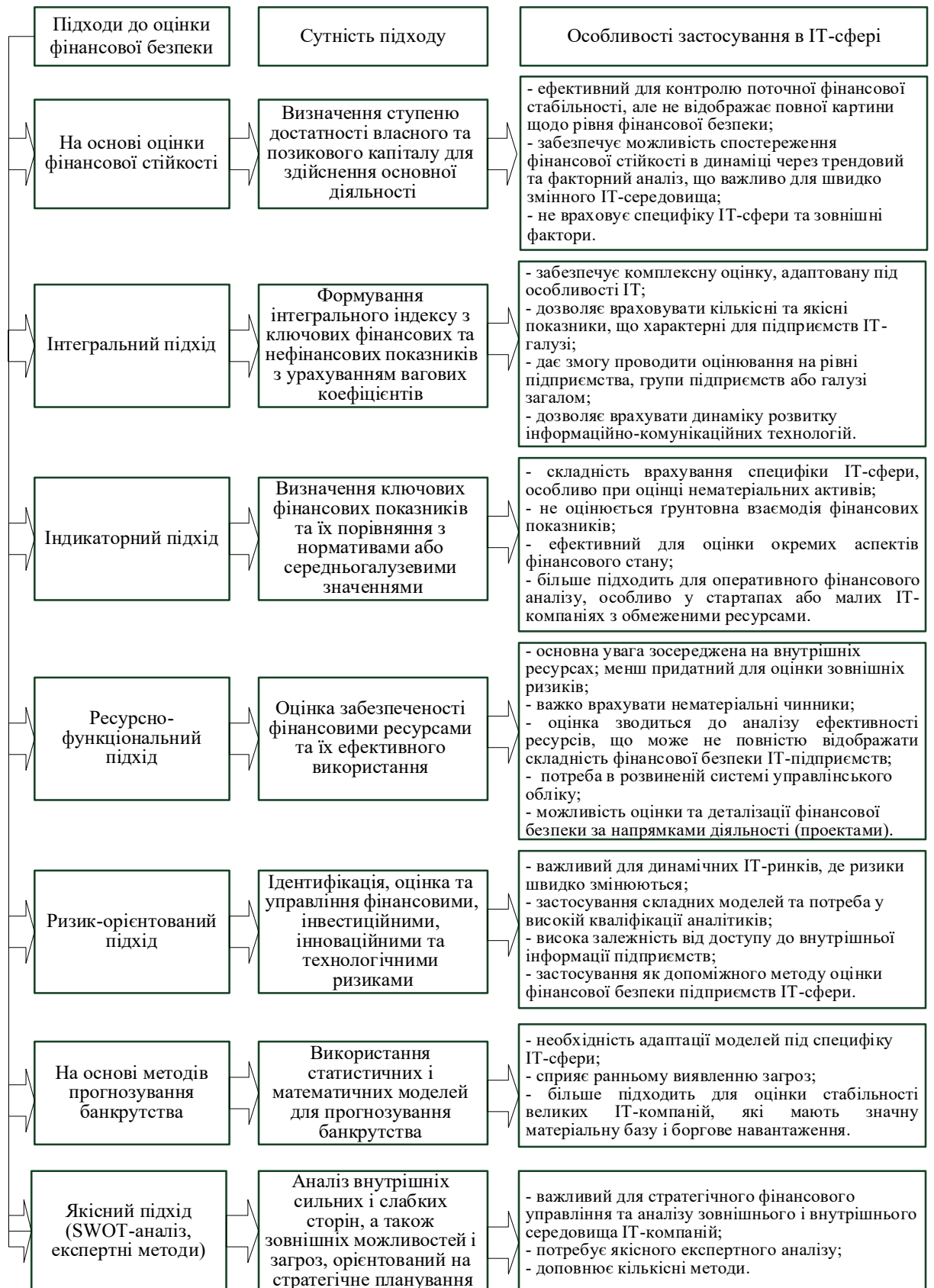


Рис. 2.14. Основні підходи до оцінки фінансової безпеки підприємств ІТ-сфери

Джерело: складено за даними [19; 35; 63; 65; 157].

Для підприємств ІТ-сфери, що мають низку унікальних характеристик, кожен із представлених методичних підходів має свої переваги та недоліки, специфічні особливості практичного застосування, а також обмеження у використанні, що впливає на точність та достовірність результатів оцінювання [148].

Розглянемо ці підходи більш детально. Дослідження свідчать, що *індикаторний підхід* відзначається простотою та швидкістю, але має певні недоліки, якщо його розглядати в галузевому контексті ІТ-сфери. Так, застосування традиційних фінансових коефіцієнтів, які визначаються на основі фінансової звітності, досить часто не повністю відображає реальну картину щодо фінансової ситуації в ІТ-компаніях, адже вагома частина цінності таких суб'єктів господарювання перебуває у сфері нематеріальних активів та визначається людським потенціалом. Тому система індикаторів має відповідати складу та важливості основних загроз фінансовій безпеці підприємства, а при визначенні порогових значень індикаторів необхідно враховувати особливості діяльності ІТ-підприємства, специфіку та умови ринку, на якому реалізується продукт чи послуга, а також інші фактори [148].

Щодо *ризик-орієнтованих підходів*, то для ІТ-компаній, які здебільшого оперують нематеріальними активами та значною мірою залежать від інтелектуальної власності, професійних компетенцій персоналу та ділової репутації, і відповідно мають специфічні ризики, їх застосування має певні обмеження. Це пов'язано, в першу чергу, з тим, що зазначені фактори важко піддаються традиційним методам кількісної оцінки, а ризики в ІТ-секторі мають більш динамічний, неструктурований та слабо прогнозований характер [148].

Крім того, ІТ-підприємства особливо вразливі до кіберзагроз, які важко піддаються точним кількісним вимірюванням і потребують застосування спеціалізованих методів моніторингу та управлінських підходів. Внаслідок цього, ризик-орієнтовані методи можуть бути використані як допоміжні інструменти, адже вони не повною мірою здатні забезпечити комплексну оцінку фінансової безпеки підприємств ІТ-сектору [148].

Метод оцінювання фінансової безпеки на основі *ресурсно-функціонального підходу* був предметом досліджень таких науковців, як О. В. Грачов, М. М. Єрмошенко, Т. Б. Кузенко та ін. Суть цього підходу полягає в окремому аналізі кожної функціональної складової фінансової безпеки з подальшим експертним узагальненням у вигляді інтегрального показника. Різні автори пропонують власну структуру функціональних компонентів і відповідних показників. Найчастіше аналіз проводиться за такими ключовими напрямками фінансової безпеки підприємства, як бюджетна, грошово-кредитна, валютна, банківська, інвестиційна, фондова та страхова [52; 92; 157].

Ресурсно-функціональний підхід в ІТ-сфері дозволяє деталізувати оцінку фінансової безпеки за напрямками діяльності (наприклад, інвестиційна та інноваційна діяльність, маркетинг тощо), що є перевагою для великих ІТ-компаній. Проте застосування таких методів ускладнено на малих підприємствах або стартапах, де управлінський облік недостатньо розвинений або де функції та напрями діяльності формально не розділені [148].

Методи прогнозування банкрутства для підприємств базуються на економіко-математичних моделях (наприклад, моделях Альтмана, Ліса, Терещенка О. О. та ін.), які враховують комплекс фінансових коефіцієнтів і показників, що відображують фінансовий стан компанії та ймовірність її банкрутства [30].

Особливістю застосування таких моделей в ІТ-сфері є необхідність їх адаптації під її специфіку, де переважають нематеріальні активи, прибутковість може бути нестабільною, а ризики мають специфічний характер (технологічні зміни, інтенсивна конкуренція). Тому традиційні моделі потрібно доповнювати якісними показниками, а також новими інструментами, такими, наприклад, як штучний інтелект і машинне навчання, що оперують великими масивами даних та враховують нелінійні залежності [191].

Якщо говорити про *SWOT-аналіз*, то він належить до якісних методів і виступає інструментом стратегічного аналізу, що базується на оцінці сильних і слабких сторін, а також можливостей і загроз для підприємства або окремого

ІТ-проєкту [30]. Якісний SWOT-аналіз є досить ефективним для ІТ-сфери, адже він доповнює кількісну оцінку рівня фінансової безпеки, забезпечуючи вивчення факторів, які важко піддаються вимірюванню, але мають суттєвий вплив на фінансову стабільність (ринкові тренди, рівень конкуренції, людський капітал, технологічні зміни тощо) [148].

На сьогодні достатньо поширеним серед науковців є *інтегральний підхід*, який дозволяє об'єднати різні показники у єдиний індекс, що відображає загальний рівень фінансової безпеки підприємства. Проте різними авторами пропонуються різні алгоритми розрахунку інтегрального показника. Більшість дослідників при визначенні інтегрального показника фінансової безпеки використовують традиційні фінансові коефіцієнти, зокрема коефіцієнти ліквідності, фінансової стійкості, показники прибутковості тощо [19; 35; 185; 215].

Деякі науковці пропонують в інтегральній оцінці застосовувати також і якісні показники. Так, на думку Л. С. Яструбецької, доцільним є доповнення кількісної оцінки фінансової безпеки підприємства якісними індикаторами, що охоплюють такі напрями, як рівень корпоративної культури, ефективність діяльності кадрової служби, служби захисту інформації, юридичного відділу та структур, відповідальних за управління фінансовою безпекою. Узагальнення результатів здійснюється шляхом об'єднання значень кількісних і якісних показників з подальшим формуванням шкали інтегрального індексу фінансової безпеки підприємства [230].

Тому адаптивні моделі визначення інтегрального показника фінансової безпеки, сформовані з урахуванням галузевої специфіки, мають більшу точність, однак потребують ретельного обґрунтування структури показників, експертного залучення та постійного оновлення відповідно до сучасних тенденцій розвитку. Саме інтегральний підхід для оцінки рівня фінансової безпеки може бути адаптований до специфіки ІТ-підприємств та дозволить поєднати фінансові індикатори з іншими параметрами розвитку, що визначають фінансову стійкість та рівновагу таких суб'єктів господарювання [148].

Отже, застосування інтегрального підходу в оцінці фінансової безпеки підприємств ІТ-сфери є найбільш доцільним з низки причин:

- комбінація кількісних і якісних показників-індикаторів надає можливість враховувати такі важливі для фінансової стійкості ІТ-компаній аспекти, як розвиток нематеріальних активів, кадровий та інноваційний потенціал, система кіберзахисту тощо;

- саме інтегральний підхід дозволяє об'єднати в єдиний узагальнюючий показник багатокomпонентну структуру фінансової безпеки, що в ІТ-секторі включає як фінансові, так і нефінансові складові та чинники: інвестиційну привабливість, інноваційну активність, технологічний розвиток та ін.;

- можливість виконання порівняльного аналізу та дослідження рівня фінансової безпеки в динаміці, що сприяє виявленню тенденцій і зіставленню результатів фінансово-господарської діяльності різних ІТ-компаній та сфер ІТ-сектору;

- адаптивність та гнучкість інтегрального підходу, який може бути модифікований відповідно до специфіки конкретного підприємства або сегмента ІТ-індустрії, забезпечуючи врахування характерних ризиків та чинників розвитку [148].

Розглянемо основні етапи проведення комплексного оцінювання рівня фінансової безпеки ІТ-компаній. При проведенні такої оцінки (рис. 2.15) на *першому етапі* формується структура фінансової безпеки, тобто визначаються складові компоненти інтегрального показника. Пропонується виділити шість ключових складових, які найповніше відображають фінансову безпеку суб'єктів господарювання ІТ-сектору: фінансова стійкість, ліквідність, прибутковість, майновий стан, ділова активність, інвестиційна привабливість [148].

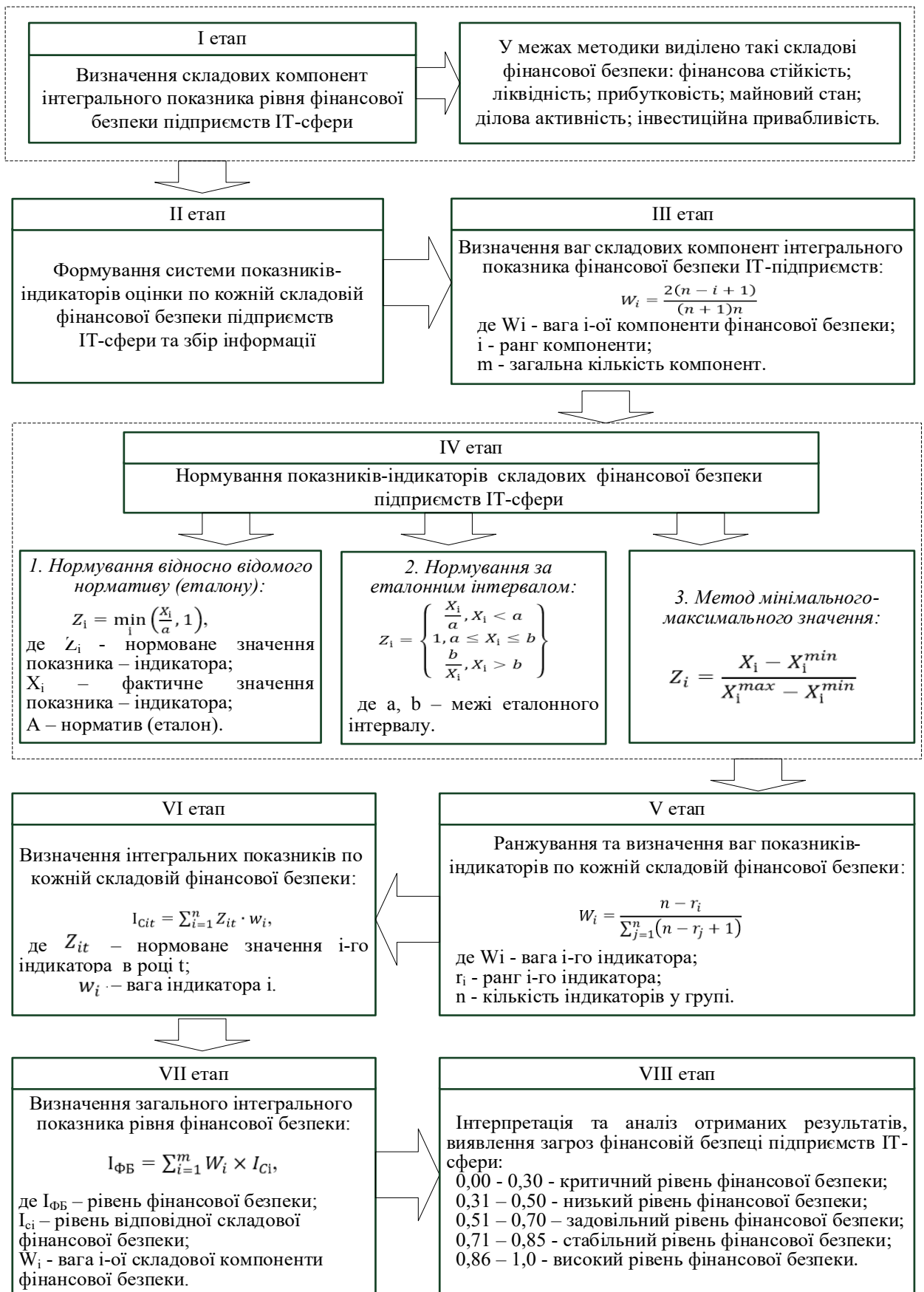


Рис. 2.15. Етапи комплексної оцінки рівня фінансової безпеки підприємств ІТ-сфери

Джерело: складено автором.

Запропонований набір складових узгоджується з науковими підходами до оцінювання фінансової безпеки, наведеними в табл. 2.10, і є результатом узагальнення сучасної теорії та практики з даного питання.

Таблиця 2.10

Порівняння підходів до визначення складових фінансової безпеки підприємств

Автори / джерело	Складові для оцінки рівня фінансової безпеки підприємств
Геєць В. М., Кизим М. О. [33]	Фінансова стійкість, ліквідність, рентабельність, ділова активність, інвестиційна привабливість
Бланк І. А. [33]	Ліквідність, платоспроможність, рентабельність, фінансова стійкість, структура капіталу
Макарчук І. М., Малишко В. В., Яременко Л. М. [111]	Прибутковість, ліквідність, майновий стан, інвестиційна привабливість, ділова активність
Кракос Ю. Б., Разгон Р. О. [87]	Оцінки ефективності управління, оцінки платоспроможності та фінансової стійкості, ділової активності, ринкової стійкості, інвестиційної привабливості
Ільяшенко О.В., Біломістна І. І. [11]	Фінансова стійкість
Полтнініна О. П. [161]	Структура капіталу, ділова активність, платоспроможність та ліквідність, рентабельність, фінансова стійкість
Хижняк Ю. О. Хижняк Ю. О. [215]	Майновий стан, ліквідність, фінансова незалежність, ділова активність, ефективність діяльності
Яструбецька Л. [230]	Ліквідність та платоспроможність, ділова активність, фінансова стійкість, майновий стан, прибутковість

Джерело: систематизовано автором.

Вибір зазначених шести складових обґрунтовується наступним:

- фінансова стійкість відображає здатність підприємства підтримувати рівновагу між власними та залученими ресурсами, зберігати платоспроможність і незалежність від зовнішніх джерел фінансування у довгостроковій перспективі. Для ІТ-компаній, які функціонують у середовищі високих інноваційних ризиків та постійного залучення зовнішніх інвестицій, дослідження цієї складової є основою для прийняття рішень щодо збереження фінансової незалежності та захисту від потенційних фінансових загроз;

- ліквідність характеризує спроможність підприємства оперативно перетворювати активи на грошові кошти для виконання поточних зобов'язань. В умовах динамічного ІТ-ринку та частих змін кон'юнктури, цей показник

критично важливий для моніторингу стабільності операційної діяльності, платоспроможності та швидкої реакції на ринкові виклики;

- прибутковість в ІТ-секторі визначає здатність підприємства генерувати власний капітал, формувати фінансові ресурси, здійснювати фінансування інновацій, протидіяти фінансовим ризикам, підтримувати інвестиційну привабливість та забезпечувати податкову стабільність;

- майновий стан підприємства характеризує структуру та якість його активів. Показники майнового стану не лише дають змогу оцінити поточний стан активів ІТ-підприємства, визначити ступінь їх оновлення і модернізації та виявити слабкі місця, а й оцінити довгостроковий потенціал забезпечення фінансової стабільності та здатності суб'єкта господарювання протистояти викликам і загрозам;

- ділова активність дозволяє оцінити ефективність операційної діяльності та раціональність використання ресурсів ІТ-підприємств, стійкість до ринкових коливань, фінансову гнучкість, конкурентоспроможність та темпи розвитку бізнесу загалом;

- інвестиційна привабливість характеризує здатність ІТ-підприємств забезпечувати власне фінансування і ефективно залучення зовнішніх інвестицій та венчурного капіталу для масштабування бізнесу, виходу на нові ринки та впровадження інноваційних продуктів і технологій.

Отже, на нашу думку, для оцінювання фінансової безпеки ІТ-підприємств на основі інтегрального показника доцільним є:

- включення індикаторів, що відображають інноваційно-інвестиційний потенціал ІТ-компаній, зокрема у складових ділової активності та інвестиційної привабливості;

- переважна роль показників ліквідності та фінансової стійкості, як ключових характеристик фінансової незалежності та платоспроможності суб'єктів господарювання;

- оцінку майнового стану з урахуванням вагової частки нематеріальних активів і прав інтелектуальної власності, що формують інноваційний потенціал ІТ-компанії [148].

Такий вибір обґрунтовується також тим, що в нинішніх умовах господарювання ІТ-підприємств, які функціонують у високотехнологічному та інноваційно динамічному середовищі, лише класичні індикатори фінансового стану не здатні повною мірою відобразити реальний рівень фінансової безпеки. Тому також повинні бути враховані показники, що характеризують кадровий потенціал, інноваційну активність, інвестиційну привабливість тощо [148].

Отже, запропонований перелік складових забезпечує комплексний, науково обґрунтований та адаптивний підхід до оцінки рівня фінансової безпеки підприємств ІТ-сектору. Він дозволяє охопити як внутрішні фінансові параметри, так і зовнішні ринкові та інвестиційні фактори, що поєднує універсальні критерії та галузеву специфіку, дозволяючи отримати релевантні результати [148].

Другим етапом комплексної оцінки рівня фінансової безпеки підприємств ІТ-сфери є формування системи показників-індикаторів для кожної з визначених складових. На цьому етапі здійснюється збір інформації та визначення показників, що дозволяють оцінити рівень фінансової безпеки підприємств ІТ-сфери. Тут важливим є обрання для кожної складової фінансової безпеки тих індикаторів, які найбільш повно характеризують функціонування підприємств ІТ-галузі [148].

Для комплексної оцінки рівня фінансової безпеки ІТ-підприємств застосовуються як уніфіковані, найбільш поширені у фінансово-економічному аналізі та доступні для широкого використання показники, так і ті, що більш повно характеризують специфіку діяльності таких суб'єктів господарювання (рис. 2.16) [148].

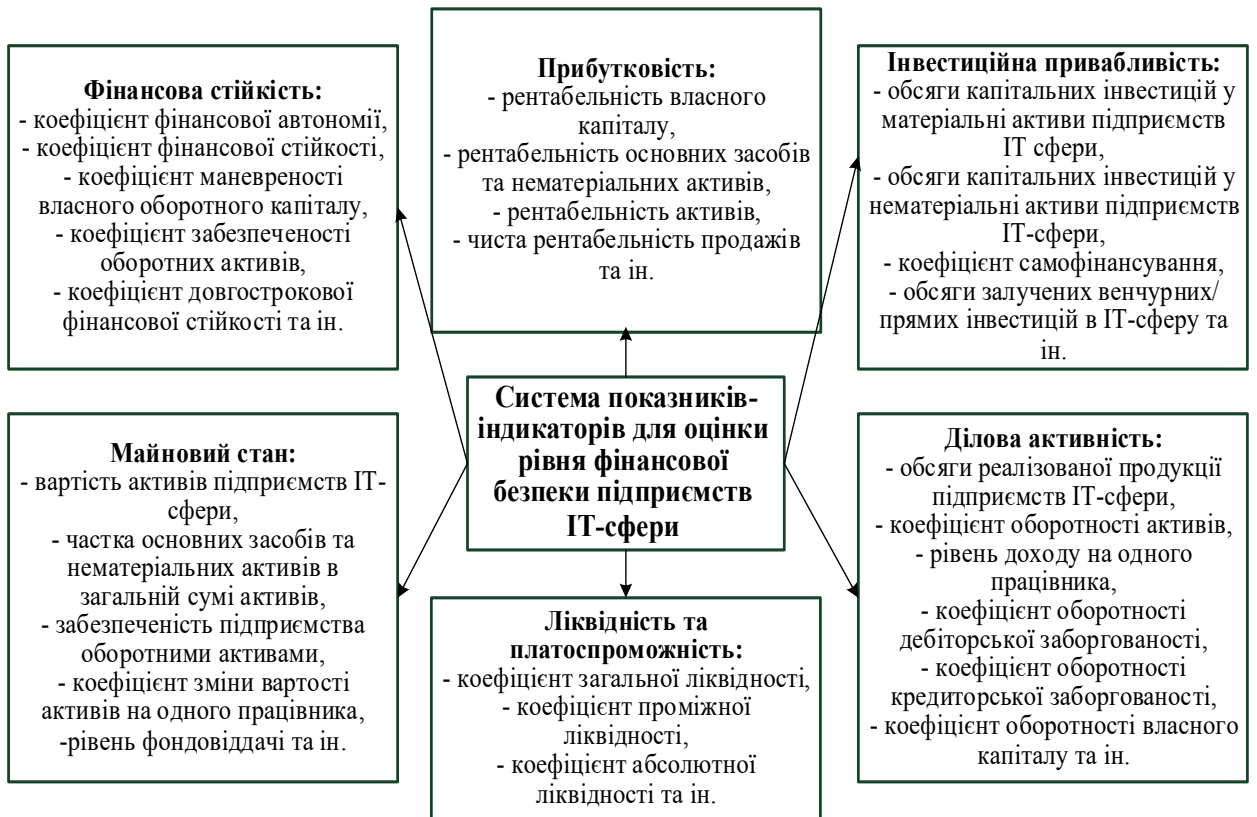


Рис. 2.16. Показники-індикатори для оцінки рівня фінансової безпеки підприємств ІТ-сфери

Джерело: складено автором на основі [19; 35; 63; 230].

Варто відзначити, що вибір показників для дослідження здійснювався відповідно до таких методологічних принципів:

- репрезентативність – у систему включено найбільш суттєві показники, які комплексно характеризують стан кожної складової фінансової безпеки підприємств ІТ-сектору. Відбір індикаторів ґрунтувався на аналізі офіційних статистичних джерел, сучасних наукових праць та галузевих досліджень провідних ІТ-кластерів України;

- достовірність – обрані індикатори мають вагоме значення у фінансово-економічній діагностиці підприємств, широко застосовуються в міжнародній та вітчизняній практиці, а також адекватно відображають реальний стан і динаміку відповідної складової фінансової безпеки;

- інформаційна доступність – для розрахунку показників використано офіційні статистичні дані Державної служби статистики України, Національного банку України, а також аналітичні звіти профільних ІТ-асоціацій та кластерів, що забезпечує відкритість джерел, можливість повторного розрахунку показників та порівнянність результатів у часовій динаміці;

- галузева релевантність – обрані показники враховують специфіку функціонування ІТ-сфери.

Проте перелік показників може бути розширений залежно від завдань дослідження або доступності вихідних даних. Однак нами в межах дисертаційної роботи вибір було зосереджено на тих показниках, які є уніфікованими, найбільш поширеними у фінансово-економічному аналізі та доступними для широкого використання (додаток А, табл. А.1). Так, первинні статистичні дані для визначення необхідних показників-індикаторів щорічно публікуються на офіційному сайті Державної служби статистики України та систематизуються за видами економічної діяльності відповідно до класифікатора КВЕД, що забезпечує можливість їх регулярного оновлення та порівняння в динаміці.

Використання динамічних рядів цих показників дозволяє не лише здійснити розрахунок інтегрального рівня фінансової безпеки ІТ-підприємств, а й провести оцінку його змін у часі та проаналізувати фактори впливу, а також визначити останні тенденції та закономірності.

Отже, процес формування системи індикаторів складається з двох етапів:

- попередній відбір показників на основі аналізу наукових джерел, методичних підходів до оцінювання фінансової безпеки, а також доступності статистичної інформації;

- галузева адаптація, у межах якої виключаються показники, що не мають суттєвого впливу на фінансову безпеку підприємств ІТ-сфери, та додаються індикатори, релевантні для цифрової економіки та ІТ-сфери. Зокрема, варто враховувати такі специфічні показники, як швидкість обігу нематеріальних активів, частка витрат на R&D у загальній структурі витрат, рівень залучення інвестицій та інші [148].

Такий підхід дозволяє забезпечити баланс між універсальністю системи оцінювання та галузевою специфікою, що, у свою чергу, сприяє підвищенню

точності визначення інтегрального рівня фінансової безпеки ІТ-підприємств і забезпеченню релевантності управлінських рішень у контексті цифрової трансформації економіки [148].

Розраховані та визначені показники-індикатори для оцінки рівня фінансової безпеки підприємств ІТ-сфери України за 2019-2023 рік представлені в табл. 2.11.

На третьому етапі комплексної оцінки рівня фінансової безпеки підприємств ІТ-сфери здійснюється визначення вагових коефіцієнтів для кожної зі складових інтегрального показника. Інтегральний підхід хоч і забезпечує більшу системність, але може дати спотворені результати за неправильного вибору ваг для складових компонентів інтегрального показника, особливо якщо ваги не адаптовані до галузі. Наприклад, велика вага майнових показників у структурі інтегрального, для ІТ-підприємств може знизити загальний рівень фінансової безпеки, навіть якщо підприємство є прибутковим, інноваційним та інвестиційно привабливим [148].

З огляду на складність прямого кількісного вимірювання впливу кожної складової на загальний рівень фінансової безпеки, доцільним є використання експертних методів, які дозволяють інтегрувати знання та практичний досвід у більш формалізовану модель [148].

Для визначення ваги кожної складової компоненти інтегрального показника рівня фінансової безпеки підприємств ІТ-сфери доцільно застосовувати метод ранжування з використанням формули Фішберна. Цей метод дозволяє перетворити якісну оцінку значущості кожної складової у кількісні вагові значення шляхом ранжування складових за ступенем їхньої важливості для фінансової безпеки ІТ-підприємств, а ваги відповідно розраховуються на основі позиції кожної складової в ранжованому списку за формулою [148]:

$$Wi = \frac{2(n-i+1)}{(n+1)n},$$

де Wi – вага i -ої компоненти фінансової безпеки;

i – ранг компоненти;

m – загальна кількість компонентів.

Таблиця 2.11

Показники-індикатори для оцінки рівня фінансової безпеки підприємств ІТ-сфери України за 2019-2024 рік

Компоненти фінансової безпеки	Індикатори для підприємств ІТ-сфери	2019	2020	2021	2022	2023	2024
Майновий стан	Вартість активів підприємств ІТ-сфери, млн грн	54819,9	59552,3	66113,1	88536,7	124765,5	159589,2
	Частка основних засобів та нематеріальних активів в загальній сумі активів	0,205	0,209	0,194	0,156	0,134	0,133
	Забезпеченість підприємства оборотними активами	0,6291	0,6862	0,6964	0,7709	0,7861	0,7868
	Коефіцієнт зміни вартості активів на одного працівника	1,277	0,918	0,996	1,104	1,301	1,372
	Рівень фондовіддачі	1,782	1,911	2,322	2,077	1,726	1,586
Інвестиційна привабливість	Обсяги капітальних інвестицій у матеріальні активи підприємств ІТ сфери, млн грн	2816,07	2332,74	3068,28	2277,98	2772,71	4041,5
	Обсяги капітальних інвестицій у нематеріальні активи підприємств ІТ-сфери, млн грн	892,63	614,3	1419,41	861,27	2172,0	2878,4
	Коефіцієнт самофінансування	0,639	0,916	0,563	0,841	0,922	0,683
	Обсяги залучених венчурних/прямих інвестицій в ІТ-сферу, млн дол.	673,9	533,5	779,6	826	228,8	462
Фінансова стійкість	Коефіцієнт фінансової автономії	0,401	0,477	0,505	0,498	0,516	0,521
	Коефіцієнт фінансової стійкості	0,669	0,911	1,022	0,993	1,067	1,088
	Коефіцієнт маневреності власного оборотного капіталу	0,197	0,452	0,474	0,605	0,746	0,752
	Коефіцієнт забезпеченості оборотних активів	0,126	0,314	0,344	0,391	0,490	0,498
	Коефіцієнт довгострокової фінансової стійкості	0,450	0,529	0,543	0,530	0,599	0,605
Прибутковість	Рентабельність власного капіталу, %	22,66	21,58	24,84	28,17	28,86	27,33
	Рентабельність основних засобів та нематеріальних активів, %	51,67	51,65	65,52	93,21	121,98	125,07
	Рентабельність активів, %	9,09	10,29	12,55	14,03	14,9	14,24
	Чиста рентабельність продажів, %	5,1	5,38	5,41	6,76	8,63	9,37
Ліквідність	Коефіцієнт загальної ліквідності	1,144	1,457	1,524	1,642	1,960	1,990
	Коефіцієнт проміжної ліквідності	1,08	1,38	1,44	1,56	1,84	1,86
	Коефіцієнт абсолютної ліквідності	0,24	0,30	0,31	0,27	0,28	0,27
Ділова активність	Обсяги реалізованої продукції підприємств ІТ-сфери, млрд грн	97,57	113,90	160,42	184,68	67,16	250,38
	Коефіцієнт оборотності активів	1,998	1,990	2,443	2,379	2,019	1,781
	Рівень доходу на одного працівника (продуктивність праці)	424,8	444,1	493,7	546,1	634,9	800,7
	Коефіцієнт оборотності дебіторської заборгованості	5,308	5,150	6,009	5,234	4,135	3,649
	Коефіцієнт оборотності кредиторської заборгованості	6,678	6,792	7,781	7,641	6,816	6,594
	Коефіцієнт оборотності власного капіталу	4,870	4,519	4,967	4,745	3,969	3,432

Джерело: розраховано автором на основі [141; 153].

В умовах цифрової економіки функціонування ІТ-підприємств визначається високою залежністю від стабільності фінансових потоків, здатності до адаптації до умов технологічних змін і гнучкого управління ресурсами. Відповідно, ранжування складових фінансової безпеки нами здійснено на основі аналізу впливу кожної з них на здатність підприємства забезпечувати стійкий розвиток, мінімізувати ризики та підтримувати фінансову стійкість та рівновагу в довгостроковій перспективі:

- ранг 1 – фінансова стійкість обрана як пріоритетна складова, оскільки для ІТ-підприємств, які часто залучають фінансування для масштабування, важливим є оптимальне співвідношення власного та позикового капіталу, здатність підтримувати платоспроможність та уникати надмірного боргового навантаження, а високий рівень фінансової стійкості сприяє стійкому інноваційному розвитку;

- ранг 2 – ліквідність є другою за значущістю, оскільки своєчасне виконання фінансових зобов'язань, безперервність розрахунків із контрагентами та наявність достатніх ліквідних активів визначають стабільність операційної діяльності. В ІТ-галузі, де швидкі розрахунки та короткі операційні цикли є нормою, достатня ліквідність запобігає зривам проєктів через брак оборотних коштів;

- ранг 3 – прибутковість є показником ефективності використання ресурсів, що прямо впливає не тільки на стабільність функціонування, а й на можливість фінансування інноваційних проєктів та розширення бізнесу. У висококонкурентному середовищі ІТ-ринку прибутковість не лише відображає поточну ефективність підприємства, але й формує базу для майбутніх інвестицій та розробок;

- ранг 4 – майновий стан відображає структуру та якість активів підприємства. Хоча в ІТ-секторі матеріальні активи відіграють меншу роль, ніж у традиційних галузях, збереження та ефективне використання основних засобів (серверного обладнання, дата-центрів, офісної інфраструктури) та особливо нематеріальних активів є важливою умовою безперебійного надання ІТ-послуг;

- ранг 5 – ділова активність характеризує інтенсивність використання ресурсів та швидкість обороту капіталу. Для ІТ-підприємств високий рівень

ділової активності свідчить про ефективне управління операційною діяльністю, проектами та людським капіталом, проте вона розглядається як похідна від фінансової стійкості, ліквідності та прибутковості;

- ранг 6 – інвестиційна привабливість посідає останнє місце в ієрархії пріоритетів, оскільки для стабільно функціонуючих ІТ-підприємств вона є радше наслідком, ніж причиною фінансової безпеки. Водночас вона залишається стратегічним фактором, що визначає можливості залучення додаткових фінансових ресурсів для масштабування та виходу на нові ринки.

Таким чином, наведене ранжування враховує як базові елементи фінансової стійкості, що необхідні для забезпечення безперервності діяльності, так і стратегічні складові, які впливають на довгострокову фінансову стійкість та безпеку підприємств ІТ-сфери.

Після проведення розрахунків отримаємо наступні вагові показники для складових фінансової безпеки підприємств ІТ-сфери (табл. 2.12).

Таблиця 2.12

Вагові показники компонентів фінансової безпеки підприємств

Компоненти фінансової безпеки	Вага
Фінансова стійкість (I_{FC})	0,286
Ліквідність (I_L)	0,238
Прибутковість (I_P)	0,191
Майновий стан (I_{MC})	0,143
Ділова активність (I_{DA})	0,095
Інвестиційна привабливість (I_{IP})	0,047

Джерело: розраховано автором.

Відповідно до цього інтегральний показник рівня фінансової безпеки підприємств ІТ-сфери будемо визначати за формулою:

$$I_{FB} = 0,286 \cdot I_{FC} + 0,238 \cdot I_L + 0,191 \cdot I_P + 0,143 \cdot I_{MC} + 0,095 \cdot I_{DA} + 0,047 \cdot I_{IP}.$$

Після формування системи показників-індикаторів наступним кроком є їх нормування (*четвертий етап*), що необхідно для інтеграції різнорідних за економічним змістом і розмірністю параметрів у єдиний інтегральний показник. Нормування дозволяє забезпечити порівнянність усіх показників у межах однієї шкали, нейтралізувати вплив одиниць виміру та масштабів,

унеможливити домінування окремих індикаторів у складі інтегрального показника та підвищити об'єктивність результатів інтегральної оцінки [148].

Ураховуючи різний економічний зміст та можливу наявність еталонних значень, допустимих інтервалів і фактичного діапазону коливань показників, доцільно застосовувати *три підходи до нормування*:

1. Нормування відносно відомого нормативу (еталону):

$$Z_i = \min_i \left(\frac{X_i}{a}, 1 \right),$$

де Z_i - нормоване значення показника-індикатора;

X_i – фактичне значення показника-індикатора;

a – норматив (еталон) [148].

Цей метод використовується для показників, які мають чітко визначені нормативні значення, закріплені в науковій літературі, національних стандартах, методичних рекомендаціях Міністерства фінансів України, НБУ або МСФЗ, що дозволяє об'єктивно оцінювати відхилення фактичних значень від нормативних й уникати штучного завищення інтегрального показника в разі перевищення нормативу.

2. Нормування за еталонним інтервалом $[a; b]$:

$$Z_i = \begin{cases} \frac{X_i}{a}, & X_i < a \\ 1, & a \leq X_i \leq b \\ \frac{b}{X_i}, & X_i > b \end{cases}$$

де a, b – межі еталонного інтервалу.

Цей метод застосовується для показників, де немає єдиного нормативу, але існує рекомендований діапазон допустимих значень. Таке нормування дозволяє врахувати як надто низькі, так і надто високі значення, які мають негативний вплив на фінансову безпеку.

3. Метод мінімального-максимального значення:

$$Z_i = \frac{X_i - X_i^{\min}}{X_i^{\max} - X_i^{\min}}.$$

Використовується у випадках, коли відсутні як нормативи, так і еталонні інтервали, але є достатній обсяг статистичних даних для визначення мінімального та максимального значень індикатора у виборці. Це забезпечує ефективність його використання в динамічному аналізі показників за певні часові періоди.

Вибір нормативних значень коефіцієнтів фінансової стійкості (табл. 2.13) здійснено виходячи із галузевої специфіки ІТ-сектору, для якого, на відміну від традиційних промислових підприємств, характерним є функціонування в середовищі з нерівномірними та циклічними грошовими потоками. За таких умов ключовими вимогами до фінансової стійкості ІТ-підприємств є достатній рівень власного капіталу, що забезпечує можливість оперативного маневрування фінансовими ресурсами, а також збалансована структура джерел фінансування.

Таблиця 2.13

**Нормативні значення показників фінансової стійкості
для підприємств ІТ-сфери**

Коефіцієнти фінансової стійкості	Норматив
Коефіцієнт фінансової автономії	0,6
Коефіцієнт фінансової стійкості	1,2
Коефіцієнт маневреності власного оборотного капіталу	0,4
Коефіцієнт забезпеченості оборотних активів	0,5
Коефіцієнт довгострокової фінансової стійкості	0,6

Джерело: складено автором за [67].

Тому нормативи коефіцієнтів фінансової стійкості визначено з урахуванням адаптації до умов ІТ-галузі, де підвищена боргова залежність і недостатність власного оборотного капіталу можуть суттєво підвищувати ризики втрати фінансової безпеки.

Оскільки більшість витрат ІТ-компаній пов'язані із заробітною платою, орендою, підтримкою інфраструктури тощо, такі підприємства потребують стабільних обсягів ліквідних активів для забезпечення безперервної операційної діяльності. Тому запропоновані нормативні інтервали показників ліквідності (табл. 2.14) відповідають оптимальним значенням для підприємств, які

працюють в умовах швидкого обороту короткострокових зобов'язань та високої залежності від строків погашення дебіторської заборгованості.

Такі інтервали характеризують достатній рівень грошових коштів, що дозволяє уникати касових розривів і формувати резерв ліквідності для мінімізації ризиків неплатоспроможності. Крім того, обрані нормативи відображають збалансоване співвідношення між необхідністю підтримки високої поточної платоспроможності та ефективним використанням оборотного капіталу, що є важливою умовою забезпечення фінансової безпеки підприємств ІТ-сектору.

Таблиця 2.14

Нормативні значення показників ліквідності для підприємств ІТ-сфери

Коефіцієнти ліквідності	Еталонний інтервал
Коефіцієнт загальної ліквідності	[1,6; 2,2]
Коефіцієнт проміжної ліквідності	[1,3; 1,8]
Коефіцієнт абсолютної ліквідності	[0,25; 0,4]

Джерело: складено автором за [67; 106].

Після відбору релевантних показників-індикаторів для кожної зі складових фінансової безпеки, що було здійснено у межах другого етапу, *на n'ятому етапі* здійснюється їх ранжування за ступенем значущості та визначення вагових коефіцієнтів для подальшої інтеграції складової в загальний індекс (інтегральний показник) [148].

Не всі показники мають однаковий вплив на відповідну складову фінансової безпеки, тому для забезпечення об'єктивності оцінювання доцільно визначити їх відносну вагу. З цією метою використано метод експертного ранжування з подальшим застосуванням формули Фішберна, яка дозволяє перетворити ранги індикаторів на кількісні вагові коефіцієнти:

$$W_i = \frac{n - r_i}{\sum_{j=1}^n (n - r_j + 1)},$$

де W_i – вага і-го індикатора;

r_i - ранг і-го індикатора;

n - кількість індикаторів в групі [148].

Цей підхід надає можливість враховувати експертну думку щодо впливовості окремих показників, забезпечити гнучкість та адаптацію до специфіки ІТ-сектору та формалізувати суб'єктивні оцінки у кількісні дані, які будуть використані на наступних етапах інтегрального аналізу. Результати нормування показників-індикаторів по кожній складовій компоненті фінансової безпеки та їхніх вагових коефіцієнтів наведено в табл. Б.1 додатку Б.

Після нормування індикаторів та визначення їхніх ваг наступним *шостим етапом* є обчислення інтегрального показника для відповідної складової фінансової безпеки підприємств ІТ-сфери (табл. 2.15), який дозволяє провести узагальнену оцінку кожної з них:

$$I_{Cit} = \sum_{i=1}^n Z_{it} \cdot w_i ,$$

де Z_{it} – нормоване значення i -го індикатора в році t ;

w_i – вага індикатора i [148].

Таблиця 2.15

**Інтегральні значення складових фінансової безпеки
підприємств ІТ-сфери**

Рік	$I_{\text{ФС}}$	$I_{\text{Л}}$	$I_{\text{П}}$	$I_{\text{МС}}$	$I_{\text{ДА}}$	$I_{\text{ПП}}$
2019	0,538	1,000	0,045	0,302	0,254	0,417
2020	0,785	1,000	0,096	0,274	0,276	0,502
2021	0,839	0,991	0,406	0,358	0,650	0,458
2022	0,846	0,953	0,746	0,514	0,637	0,654
2023	0,920	0,829	0,961	0,671	0,292	0,466
2024	0,930	0,820	0,892	0,800	0,524	0,556

Джерело: розраховано автором.

На основі отриманих вагових коефіцієнтів та інтегральних показників за кожною складовою фінансової безпеки *на сьомому етапі* визначається загальний інтегральний показник рівня фінансової безпеки підприємств за формулою:

$$I_{\text{ФБ}} = \sum_{i=1}^m W_i \cdot I_{Ci} ,$$

де $I_{\text{ФБ}}$ – рівень фінансової безпеки;

I_{Ci} – рівень відповідної складової фінансової безпеки;

W_i – вага i -ої складової компоненти фінансової безпеки [148].

Таким чином, з огляду на специфіку ІТ-сфери, адаптація класичних підходів до оцінювання фінансової безпеки ІТ-підприємств на основі інтегрального показника передбачає:

- включення індикаторів, що відображають інноваційно-інвестиційний потенціал та здатність до масштабування, зокрема у складових ділової активності та інвестиційної привабливості;
- посилення ролі ліквідності та фінансової стійкості, як ключових характеристик фінансової незалежності та платоспроможності суб'єктів господарювання;
- оцінку майнового стану з урахуванням вагової частки нематеріальних активів і прав інтелектуальної власності, що формують інноваційний потенціал ІТ-компанії тощо [148].

З метою якісної інтерпретації інтегрального показника фінансової безпеки підприємств ІТ-сектору доцільно застосовувати шкалу Харрінгтона, адаптовану під ІТ-галузь. В умовах швидких цифрових трансформацій та високої динаміки ринку ІТ-послуг зміни фінансово-економічних показників мають значно швидший вплив на фінансову безпеку ІТ-підприємств ніж в традиційних секторах економіки. Крім того, вітчизняні ІТ-компанії здебільшого працюють на зовнішні ринки, що дещо знижує чутливість їхнього фінансового стану до негативного впливу внутрішніх економічних факторів, але, водночас підвищує залежність фінансово-господарської діяльності від глобальної кон'юнктури та геополітичних ризиків. Тому порогові значення шкали оцінки рівня фінансової безпеки були зміщені в бік більш жорстких вимог до її рівнів (табл. 2.16) [148].

Варто зауважити, що у межах кожної складової фінансової безпеки (зокрема, інвестиційної привабливості, ділової активності або майнового стану) окрім кількісних показників, можуть бути застосовані якісні параметри, які не піддаються прямому вимірюванню, але мають істотний вплив на загальний рівень фінансової стійкості. Так, у межах складової «Інвестиційна

привабливість» для ІТ-підприємств доцільно використовувати якісні показники, що відображають нематеріальні, репутаційні, стратегічні та управлінські аспекти, які суттєво впливають на рішення інвесторів [148].

Таблиця 2.16

Адаптована шкала Харрінгтона оцінки рівня фінансової безпеки підприємств ІТ-сектору

Інтервал інтегрального показника І_{ФБ}	Рівень фінансової безпеки	Характеристика
0,00-0,30	Критичний	Підприємство перебуває у фінансово нестабільному стані, високий ризик неплатоспроможності, можлива втрата ліквідності.
0,31-0,50	Низький	Рівень безпеки є незадовільним, спостерігаються проблеми з ліквідністю, прибутковістю або капіталізацією.
0,51-0,70	Задовільний	Фінансовий стан підприємства перебуває під контролем, однак характеризується нестійкістю, що створює потенційні ризики за умов зовнішніх викликів або загроз.
0,71-0,85	Стабільний	Підприємство має достатній рівень фінансової безпеки, основні ризики мінімізовані.
0,86-1,00	Високий	Підприємство демонструє ефективну модель управління фінансами, має високу фінансову стійкість, гнучкість та інвестиційну привабливість.

Джерело: складено автором на основі [109; 89; 36].

Майновий стан ІТ-підприємств охоплює не лише матеріальні активи, але й цифрову інфраструктуру, інтелектуальні продукти та систему інформаційної безпеки. Тому до якісних показників для оцінки майнового стану ІТ-підприємств можна віднести, наприклад, оцінку ступеня захисту інтелектуальної власності, рівень безпеки активів та інформаційних ресурсів, доступність цифрових платформ і сервісів тощо [148].

Аналогічно, у разі потреби, до якісних характеристик складової «Ділова активність» можна додатково включити не тільки показники, що характеризують обсяг і швидкість обороту ресурсів, а й показники динаміки розвитку бізнесу, інноваційної активності, потенціалу масштабування тощо [148].

Таким чином, сформована система індикаторів не є фіксованою, а може бути розширена відповідно до аналітичних завдань, доступності даних та

технологічної зрілості ІТ-компанії, що забезпечує високу релевантність, глибину та точність оцінки фінансової безпеки підприємств у динамічному, інноваційно активному цифровому середовищі [148].

У табл. 2.17 представлені отримані інтегральні значення оцінки рівня фінансової безпеки підприємств ІТ-сфери України у 2019-2023 рр.

Таблиця 2.17

**Інтегральні значення рівня фінансової безпеки
підприємств ІТ-сфери України**

Рік	Інтегральний показник фінансової безпеки	Зміна до попереднього року	Рівень фінансової безпеки
2019	0,487	-	Низький
2020	0,570	+0,083	Задовільний
2021	0,689	+0,119	Задовільний
2022	0,776	+0,087	Стабільний
2023	0,789	+0,013	Стабільний
2024	0,822	+0,033	Стабільний

Джерело: розраховано автором.

Результати інтегральної оцінки рівня фінансової безпеки підприємств ІТ-сфери України за 2019–2024 рр. свідчать про стійку динаміку її зростання, що відображає як загальні макроекономічні тенденції, так і специфіку функціонування ІТ-галузі в умовах цифрової економіки та зростаючої зовнішньої нестабільності.

Упродовж 2019 – 2021 рр. інтегральний показник фінансової безпеки зріс з 0,487 до 0,689, що за шкалою Харрінгтона відповідало переходу від низького до задовільного рівня фінансової безпеки. Причинами таких змін стали насамперед: зростання експорту ІТ-послуг (щорічно понад 20% у валютному еквіваленті); підвищення прибутковості діяльності ІТ-компаній, активізація ділової активності (особливо за певними напрямками та сферами діяльності) та зростання фінансової автономії ІТ-підприємств. Цей період характеризувався формуванням запасу фінансової міцності, що дозволив ІТ-підприємствам швидко адаптуватися до подальших кризових викликів.

У 2022 році позитивний тренд зростання інтегрального показника (до 0,776) зберігся, однак темпи його приросту уповільнились. Це відбулось насамперед через повномасштабну війну, внаслідок чого порушились усталені економічні зв'язки, різко знизилась інвестиційна активність та зросли зовнішні ризики та загрози, що негативно вплинуло на фінансовий стан ІТ-компаній. Водночас відсутність різкого погіршення інтегрального значення рівня фінансової безпеки підтверджує здатність ІТ-сектору підтримувати платоспроможність та відносну фінансову стійкість навіть в умовах високої турбулентності зовнішнього середовища.

У 2023–2024 роках інтегральний показник фінансової безпеки ІТ-підприємств продовжив зростати (до 0,822), однак темпи його приросту суттєво сповільнились, що свідчить про перехід галузі до більш помірного фінансово-економічного розвитку. Зазначена динаміка відображає закріплення досягнутого рівня фінансової безпеки за рахунок збереження ключових фінансових параметрів, тоді як подальше зростання обмежується уповільненням приростів окремих складових, насамперед інвестиційної активності порівняно з довоєнним періодом.

Порівняльний аналіз складових інтегрального показника показав, що ключовими драйверами зростання фінансової безпеки ІТ-підприємств виступають фінансова стійкість та майновий стан, інтегральні значення яких стабільно зростають протягом досліджуваного періоду. Зокрема, інтегральний показник фінансової стійкості зріс з 0,538 у 2019 р. до 0,930 у 2024 р., що свідчить про посилення ролі власного капіталу. Ліквідність та прибутковість, значення яких упродовж досліджуваного періоду суттєво зросли, також істотно впливають на формування належного рівня фінансової безпеки ІТ-сектору.

Найбільш вразливими складовими до впливу зовнішніх викликів та загроз стали ділова активність та інвестиційна привабливість, значення яких суттєво зменшувались під впливом дестабілізуючих факторів в останні досліджувані роки. Так, рівень ділової активності у 2023 р. різко скоротився до 0,292, а інвестиційної привабливості – до 0,466 і лише частково відновився у

2024 році. Саме ці складові мали найбільший вплив на зниження загального інтегрального рівня фінансової безпеки підприємств ІТ-сфери у 2023-2024 рр.

Така ситуація є цілком закономірною та логічною. Посилення безпекових ризиків та зростання загальної невизначеності економічного середовища негативно позначились на інвестиційній привабливості та діловій активності ІТ-підприємств. Також обмеженість обсягів інвестиційних ресурсів, що залучаються в ІТ-сектор протягом останніх років підтверджує важливу роль венчурного і прямого інвестування для підтримання динамічного зростання, інноваційного розвитку та забезпечення належного рівня фінансової безпеки суб'єктів ІТ-бізнесу.

Таким чином, розраховані інтегральні показники фінансової безпеки є релевантними та відображають реальний стан ІТ-сфери України за досліджуваний період. Узагальнюючи результати інтегральної оцінки, можна констатувати, що фінансова безпека підприємств ІТ-сфери України формується як динамічна система, здатна підтримувати фінансову стійкість і платоспроможність за рахунок високої прибутковості, ліквідності, переважання нематеріальних активів у структурі ресурсів, експортної орієнтації галузі тощо.

Разом з тим, досягнутий рівень фінансової безпеки залишається чутливим до впливу внутрішніх та зовнішніх викликів і загроз, а збереження його позитивної динаміки в середньо- та довгостроковій перспективі потребує розробки дієвих механізмів забезпечення фінансової безпеки ІТ-підприємств, управління фінансовими ризиками, стимулювання інвестиційної активності, посилення інституційної підтримки розвитку ІТ-галузі тощо.

Висновки до другого розділу

1. Досліджено сучасний стан та тенденції розвитку підприємств ІТ-сфери України і встановлено, що впродовж 2014-2021 рр. вітчизняний ІТ-сектор демонстрував стійке зростання, збільшення кількості суб'єктів господарювання та посилення своєї ролі в національній економіці. Попри

негативні зміни у 2022 р. під впливом повномасштабної війни, уже з 2023 р. ІТ-галузь виявила ознаки поступового відновлення та адаптації, що свідчить про її відносно високий рівень гнучкості, здатність до швидкої перебудови бізнес-процесів і збереження економічної активності в умовах воєнних та макроекономічних викликів.

2. Встановлено, що важливою тенденцією розвитку вітчизняної ІТ-галузі є не лише зміни її внутрішньої структури та поступове зростання кількості продуктивних ІТ-компаній, а і зміцнення макроекономічного значення ІТ-сектору як джерела валютних надходжень, експортного потенціалу та стабільних податкових платежів. Обґрунтовано, що навіть в умовах війни ІТ-сфера зберегла вагомий внесок у формування експортної виручки країни, продемонструвала здатність генерувати стабільні податкові надходження до державного та місцевих бюджетів, а також залишилася інвестиційно привабливим сегментом економіки. Це свідчить про поступове зміцнення системоутворюючої ролі ІТ-галузі в національній економіці та її стратегічне значення для фінансової стійкості держави.

3. За результатами комплексного аналізу фінансового стану підприємств ІТ-сфери України виявлено, що вони мають низку суттєвих відмінностей порівняно з підприємствами традиційних галузей економіки. Доведено, що для ІТ-компаній характерними є висока мобільність активів, вищі показники рентабельності, переважання оборотних активів у структурі майна, відносно низька капіталомісткість, домінування власного капіталу у структурі джерел фінансування, незначні обсяги позикового капіталу і переважання в його структурі поточних зобов'язань. Сукупність цих характеристик свідчить про достатньо високу фінансову гнучкість ІТ-підприємств, яка є однією з головних передумов їхньої фінансової стійкості в умовах кризи й воєнних потрясінь.

4. Визначено, що фінансовий стан підприємств ІТ-сфери упродовж досліджуваного періоду характеризувався нерівномірною динамікою окремих складових, однак загалом оцінюється як відносно стабільний. Встановлено, що навіть в умовах макроекономічної нестабільності, пандемії та повномасштабної війни ІТ-підприємства зберегли достатньо високі показники

ліквідності, прибутковості та фінансової автономії, хоча чутливість окремих параметрів фінансового стану до зовнішніх ризиків та загроз була неоднаковою. Це дало підстави зробити висновок, що фінансова безпека ІТ-підприємств формується як багатокomпонентна динамічна система, у якій різні складові мають різну швидкість реагування на кризові явища та неоднакову тенденцію до відновлення.

5. Обґрунтовано, що використання лише окремих показників фінансового стану не забезпечує цілісного уявлення про реальний рівень фінансової безпеки підприємств ІТ-сфери. У зв'язку з цим доведено доцільність застосування інтегрального підходу, який дозволяє поєднати кількісні та якісні параметри, врахувати галузеву специфіку ІТ-бізнесу та здійснювати динамічний і порівняльний аналіз рівня фінансової безпеки. Встановлено, що саме такий підхід є найбільш релевантним для ІТ-сфери, оскільки дає змогу враховувати не лише традиційні фінансові індикатори, а й обсяги нематеріальних активів, інноваційний потенціал, інвестиційну привабливість, кадрову складову та інші чинники, що мають принципове значення для фінансової стійкості підприємств ІТ-сектору в умовах цифрової економіки.

6. Розроблено методичний підхід до комплексної оцінки рівня фінансової безпеки підприємств ІТ-сфери, який ґрунтується на використанні інтегрального показника та враховує галузеві особливості функціонування ІТ-компаній. Запропоновано здійснювати оцінювання за шістьма основними складовими – фінансовою стійкістю, ліквідністю, прибутковістю, майновим станом, діловою активністю та інвестиційною привабливістю, що дає змогу перейти від аналізу окремих фінансових показників до комплексного оцінювання рівня фінансової безпеки. Практичне застосування запропонованого підходу створює аналітичну основу для виявлення глибини кризових явищ, оцінки темпів відновлення ІТ-сектору та подальшого обґрунтування механізмів та заходів забезпечення фінансової безпеки підприємств ІТ-сфери.

Основні результати дослідження опубліковані в таких наукових роботах [65; 148; 261; 235].

РОЗДІЛ 3

КОНЦЕПТУАЛЬНІ ЗАСАДИ РОЗВИТКУ СИСТЕМИ ФІНАНСОВОЇ БЕЗПЕКИ ІТ-ПІДПРИЄМСТВ

В УМОВАХ СТАНОВЛЕННЯ ЦИФРОВОЇ ЕКОНОМІКИ

3.1. Оцінка та характеристика загроз формування системи фінансової безпеки підприємств ІТ-сфери

Аналіз стану вітчизняного ІТ-сектору показав його стрімкий розвиток після кризових 2014-2015 рр. І навіть впродовж останніх п'яти років, в умовах війни, підвищеної макроекономічної та політичної нестабільності, галузь зберігає стійкість і спроможність до розвитку попри численні негативні зовнішні фактори. Починаючи з 2020 р. суб'єкти господарювання ІТ-сфери були змушені безперервно адаптуватися до нових реалій: спочатку до пандемії COVID-19 та її наслідків, а згодом – до виживання і подальшого зростання в умовах повномасштабної війни. Звісно, що ці фактори значною мірою змінювали діяльність ІТ-компаній, впливаючи на їхні бізнес-моделі, організацію праці, підходи до фінансового управління, стратегічні пріоритети розвитку тощо.

У процесі формування системи фінансової безпеки підприємств ІТ-сфери одним із ключових завдань є своєчасне виявлення тих чинників, які здатні порушити їхню фінансову стійкість або поставити під загрозу довгостроковий фінансово-економічний розвиток. Щоб вибудувати цілісну логіку управління фінансовою безпекою будь-якого суб'єкта господарювання, необхідно чітко розмежувати базові категорії безпекознавства – «виклик», «ризик» та «загроза».

У науковій літературі зазначено, що ці поняття тісно пов'язані між собою, але не є тотожними. Дослідники з питань безпекознавства [41; 83; 119] підкреслюють, що виклик – це насамперед сигнал про зміну умов функціонування підприємства. Він може мати як позитивний, так і

негативний потенціал залежно від того, чи здатен суб'єкт господарювання вчасно адаптуватися, переорієнтувати ресурси, переглянути підходи до управління тощо.

Як зазначає Бойко І. В., виклик сам по собі не є деструктивним фактором, а лише відображенням наявної ситуації. Наявність викликів безпосередньо ніяк не впливає на фінансову безпеку суб'єкта господарської діяльності [14]. Виклик створює ситуацію, яка вимагає реакції, і в разі її відсутності може трансформуватися в ризики й загрози.

В умовах цифрової економіки до ключових викликів фінансово-економічного розвитку ІТ-підприємств та забезпечення їхньої фінансової безпеки можна віднести:

- надзвичайно швидкі темпи розвитку новітніх технологій і технологічних змін;
- зростання рівня кіберзагроз в операційній діяльності та фінансовій сфері ІТ-підприємств;
- посилення залежності бізнес-процесів ІТ-сектору від рівня розвитку цифрової інфраструктури;
- посилення глобальної конкуренції на ринку ІТ-послуг;
- розширення масштабів цифровізації корпоративного управління та операційної діяльності;
- дефіцит працівників із сучасними цифровими компетенціями;
- підвищення вимог до прозорості та швидкості фінансових операцій тощо.

Кожен із цих викликів не є небезпекою сам по собі, однак за відсутності адекватної реакції перетворюється на джерело потенційних фінансових втрат.

Поняття «ризик» у працях вітчизняних та зарубіжних авторів традиційно пов'язується з імовірністю відхилення фактичних результатів діяльності від запланованих, причому акцент робиться саме на можливості негативних наслідків [31]. Ризик розглядають як міру невизначеності, що супроводжує фінансово-господарську діяльність підприємства та може проявлятися у вигляді додаткових витрат ресурсів, недоотримання доходів і прибутку,

погіршення показників ліквідності, платоспроможності чи фінансової стійкості [18]. Важливо, що на стадії ризику деструктивні події ще не відбулися, але є певна ймовірність їх настання.

Категорія «загроза» характеризує вищий ступінь визначеності та наближеності потенційно небезпечних подій. Науковці характеризують загрози фінансовій безпеці як наявне чи потенційно можливе явище або чинник, яке створює небезпеку для реалізації фінансових інтересів підприємства [53]. Або як вплив дестабілізаційних чинників на фінансовий стан підприємства, який може призвести до потенційних або реальних збитків [119]. Тобто, на відміну від ризику, що відображає потенційну ймовірність небажаних відхилень, загроза має чітко окреслене джерело, напрям впливу та прогнозовані наслідки – від погіршення структури капіталу і втрати ліквідності до блокування доступу до фінансових ресурсів чи компрометації фінансової інформації.

У сучасних дослідженнях фінансової безпеки підприємств пропонується розглядати виклик, ризик і загрозу як логічну послідовність ескалації деструктивних впливів. Спочатку підприємство стикається з викликом – новими умовами чи тенденціями в зовнішньому або внутрішньому середовищі. Якщо цей виклик не враховано в управлінських рішеннях, він трансформується в ризики – ймовірність виникнення негативних фінансових наслідків. І вже на наступному етапі, коли окреслюється конкретне джерело небезпеки і сценарій розвитку подій, формується загроза, реалізація якої здатна спричинити фактичні економічні збитки та порушити фінансову стійкість підприємства [181; 159].

З урахуванням проведеного узагальнення вважаємо доцільним у контексті фінансової безпеки підприємств ІТ-сфери:

- виклики розглядати як нові умови й тенденції цифрової економіки, що змінюють параметри фінансово-господарської діяльності та потребують адаптації системи фінансового управління;

- ризики – як ймовірність виникнення негативних фінансових наслідків у діяльності ІТ-підприємства внаслідок дії дестабілізаційних чинників в умовах невизначеності;

- загрози – як конкретизовані деструктивні чинники, реалізація яких здатна призвести до фінансових втрат, зниження платоспроможності чи порушення фінансової стійкості підприємства (рис. 3.1).

Таке трактування дозволяє розглядати систему фінансової безпеки ІТ-підприємств як динамічну, що спрямована не лише на нейтралізацію вже наявних загроз, а й на своєчасне врахування нових викликів та активне управління ризиками.

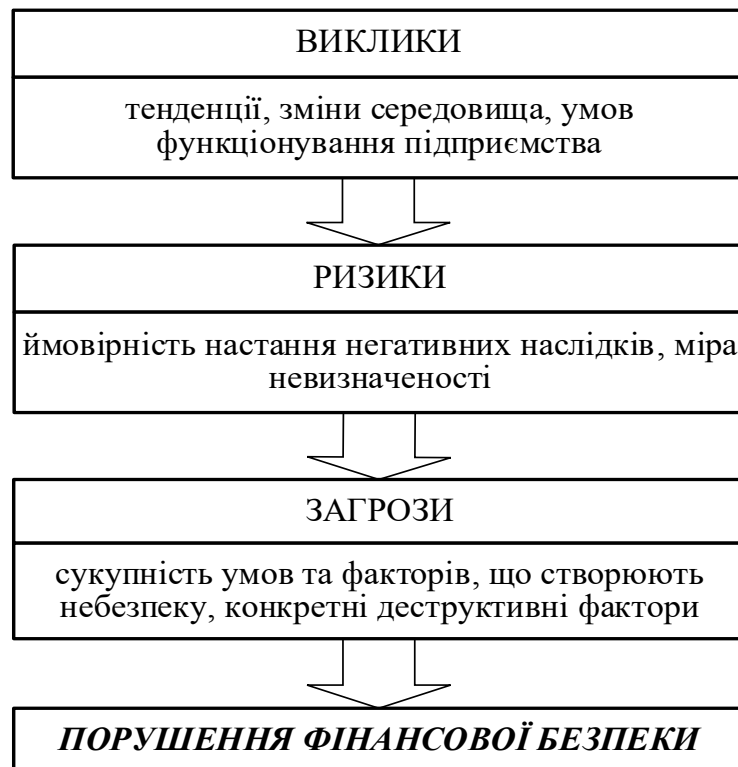


Рис. 3.1. Взаємозв'язок категорій «виклики», «ризик», «загроза»

Джерело: складено автором за [69; 83; 159].

Комплексний аналіз фінансової безпеки ІТ-підприємств передбачає чітке розмежування зовнішніх та внутрішніх дестабілізаційних чинників, а також уточнення характеру їхнього впливу на фінансову стійкість і безпеку суб'єктів господарювання. У межах цього дослідження зовнішні чинники інтерпретуються переважно як загрози фінансовій безпеці, оскільки вони

формується поза межами підприємства, мають екзогенний характер і обмежені можливості управлінського впливу з боку самого суб'єкта господарювання. Тому в дисертаційній роботі під загрозами фінансовій безпеці ІТ-підприємств пропонується розуміти передусім зовнішні дестабілізаційні чинники, що виникають під впливом макроекономічного, політичного, технологічного та соціального середовища. Їх систематизація за моделлю PEST дозволить дослідити всебічний характер впливу на фінансову безпеку вітчизняних ІТ-підприємств.

Натомість внутрішні дестабілізаційні чинники доцільно розглядати переважно як ризики, оскільки вони є наслідком особливостей фінансово-господарської діяльності ІТ-підприємств, структури їхніх ресурсів, організації операційної діяльності та якості управлінських фінансових рішень. На відміну від зовнішніх загроз, внутрішні ризики можуть бути ідентифіковані, оцінені та мінімізовані в межах системи фінансового менеджменту суб'єкта господарювання, що визначає здатність підприємства реагувати та адаптуватися до змін регуляторного й ринкового середовища.

Більшість науковців [119; 159; 17] наголошують, що нестабільність політичної системи та недостатня ефективність інституційних механізмів захисту економічних інтересів бізнесу підвищують рівень загроз для підприємств та стримують інвестиційну активність. Не є винятком і підприємства ІТ-сектору. На сьогодні *політичні загрози* фінансовій безпеці підприємств вітчизняної ІТ-сфери насамперед пов'язані з політичною нестабільністю та військовими діями, регуляторними змінами у сфері ІТ, нестійкістю інституційного середовища, а також валютними та фінансовими обмеженнями НБУ.

В умовах сьогодення серед зовнішніх політичних загроз саме повномасштабна війна є тим чинником, який найбільшою мірою дестабілізує систему фінансової безпеки підприємств ІТ-сфери України. Її вплив проявляється через формування комплексу економічних, інфраструктурних, репутаційних і технологічних загроз, що істотно ускладнюють функціонування вітчизняної ІТ-галузі.

Як показав проведений у попередньому розділі аналіз, до 2022 року ІТ-галузь України демонструвала активне зростання, стрімку інтеграцію у глобальні ринки та нарощення експортного потенціалу. Однак повномасштабна збройна агресія росії проти України змінила архітектуру фінансових ризиків та загроз, з якими стикаються вітчизняні ІТ-компанії.

Так, воєнно-політичні загрози фінансовій безпеці ІТ-підприємств проявляються насамперед через фізичне знищення їхніх матеріальних активів та об'єктів критичної інфраструктури, а також вимушене припинення або обмеження діяльності компаній у прифронтових регіонах і на окупованих територіях. Удари по енергетичній інфраструктурі та телекомунікаційних мережах, перебої з енергопостачанням і зв'язком створюють прямі загрози для безперервності операційної діяльності ІТ-компаній, виконання контрактів та, відповідно, стабільності отримуваних доходів і грошових потоків.

За результатами досліджень Світового банку, у 2022 р. близько 18 % українських компаній різних галузей зазнали прямого фізичного пошкодження активів, а доступ до фінансових ресурсів, логістики та ринків збуту значно ускладнився [268; 269]. Також сукупні потреби у відновленні та реконструкції за роки повномасштабної війни оцінюються щонайменше у 524 млрд дол. США на наступне десятиліття [273], що підкреслює довгостроковість наслідків воєнно-політичних ризиків для економіки країни та фінансової безпеки суб'єктів господарювання.

Крім того, погіршення безпекової ситуації впливає на поведінку іноземних замовників. Вони переглядають умови співпраці, скорочують бюджети та обсяги замовлень або тимчасово зупиняють проекти, що загрожує нестабільністю контрактів, зменшенням доходів та зниженням інвестиційної привабливості вітчизняних ІТ-компаній [140].

Враховуючи експортну орієнтацію українського ІТ-сектору, суттєвий вплив на рівень його фінансової безпеки здійснюють встановлені державою умови валютно-фінансового регулювання та ведення зовнішньоекономічної діяльності. З початком повномасштабної війни НБУ був змушений

запровадити жорсткі валютні обмеження з метою недопущення відтоку капіталу й підтримання стабільності національної фінансової системи. Такі заходи включали адміністративні обмеження на транскордонні платежі та рух капіталу, встановлення граничних строків розрахунків за експортно-імпортними операціями та ін. [228]. Хоча такі інструменти мали стабілізаційний ефект на макрорівні, на рівні підприємств вони ускладнили їм взаємодію з іноземними партнерами та інвесторами.

Для ІТ-компаній найбільш чутливими стали обмеження щодо репатріації дивідендів та виплат за зовнішніми позиками. У результаті підприємства зіткнулися з проблемами у проведенні міжнародних розрахунків, управлінні валютною виручкою та плануванні грошових потоків. Крім того, відсутність можливості своєчасного виведення доходів створює додаткові бар'єри для залучення іноземного капіталу. Усе це підвищує інвестиційні ризики для іноземних інвесторів, негативно впливає на інвестиційну привабливість ІТ-компаній і, як наслідок, призводить до зростання вартості капіталу та обмеження доступу до кредитних ресурсів і венчурних інвестицій для суб'єктів господарювання ІТ-сфери.

Водночас поряд із внутрішніми валютними обмеженнями, посилюється і зовнішній репутаційний тиск. Як зазначають Ковтуненко Ю.В., Дукіна Д.М., для сервісних ІТ-компаній ускладнюється доступ до міжнародних фінансових сервісів, відкриття рахунків та проведення розрахунків із нерезидентами, що фактично прирівнює український ІТ-бізнес до високоризикових юрисдикцій [77].

Протягом тривалого періоду частина впроваджених валютних обмежень залишалася чинною, обмежуючи можливості реалізації довгострокових інвестиційних проєктів. І лише у 2024 р. НБУ розпочав поетапну лібералізацію валютного регулювання. Передусім це стосувалося пом'якшення правил репатріації доходів та перегляду валютних лімітів для підприємств [136]. А на початку 2025 р. НБУ запровадив черговий пакет послаблень, у тому числі й механізм «інвестиційного ліміту», який дозволив компаніям здійснювати

окремі валютні операції в межах коштів, залучених від іноземних інвесторів до статутного капіталу підприємств [135]. Проте навіть попри певне пом'якшення режиму валютного контролю, значна частина обмежень продовжує діяти, що ускладнює фінансово-економічну діяльність ІТ-підприємств, які працюють на зовнішні ринки.

Також фінансова стійкість ІТ-підприємств значною мірою залежить від того, наскільки стабільним і передбачуваним залишається інституційне середовище. Саме в цій площині особливо відчутними стають слабкість державних інститутів, непослідовність політичних рішень, недостатня якість державного управління та зниження довіри бізнесу до інституційної системи.

Відповідно до індексів якості врядування Світового банку, Україна традиційно належить до країн із рівнем політичної стабільності нижчим за середньосвітовий. І хоча в довоєнний період спостерігалась поступова позитивна динаміка за окремими індикаторами інституційної спроможності, зокрема у сфері ефективності державного управління та якості регуляторного середовища [274], для бізнесу інституційне середовище й надалі залишалося нестійким і недостатньо передбачуваним. З початком повномасштабної війни ці проблеми лише посилилися, що призвело до зростання невизначеності економіко-правових умов ведення ІТ-бізнесу та підвищення загального рівня політичної нестабільності.

Додатковим проявом нестійкості інституційного середовища залишаються високі корупційні ризики. Для ІТ-сектору корупційні ризики проявляються не стільки через прямі корупційні впливи, скільки через загальну регуляторну та правову невизначеності, надмірну бюрократизацію та ускладнення економіко-правових умов ведення підприємницької діяльності та взаємодії з іноземними партнерами. У таких умовах для ІТ-підприємств зростають витрати на юридичний супровід, а сам ІТ-бізнес стає більш залежним від інституційних рішень і адміністративних бар'єрів.

Водночас важливим кроком з боку українського уряду в напрямку підтримки вітчизняної ІТ-галузі стало запровадження у 2021 р. спеціального правового режиму «Дія.City», закріпленого Законом України «Про стимулювання розвитку цифрової економіки в Україні» [171]. Його впровадження було спрямоване на формування більш передбачуваних умов функціонування ІТ-бізнесу, підвищення інвестиційної привабливості галузі та зміцнення довіри з боку контрагентів.

Разом із тим, обмеженість бюджетних ресурсів, пріоритетність оборонних і соціальних видатків, а також значні потреби у фінансуванні відновлення зруйнованої інфраструктури, істотно звужують можливості реалізації комплексних державних програм підтримки ІТ-галузі. За таких умов навіть позитивні ініціативи з боку держави не здатні повною мірою компенсувати загальну нестійкість інституційного середовища, що зберігає для підприємств ІТ-сфери високий рівень залежності від політичних рішень і загальної інституційної стабільності.

Однією із суттєвих зовнішніх політичних загроз фінансовій безпеці підприємств ІТ-сфери в сучасних умовах є регуляторна нестабільність. Вона проявляється в частих змінах правил ведення бізнесу, податкового та трудового законодавства, а також у непередбачуваності державних рішень в умовах воєнного стану. Слід зауважити, що нестабільність інституційного середовища формує загальний політико-правовий контекст функціонування бізнесу, тоді як регуляторна нестабільність в ІТ-сфері є його безпосереднім проявом на рівні правил, норм і процедур, з якими щоденно стикаються ІТ-підприємства. Саме тому вона безпосередньо трансформується у ризики, пов'язані з підвищенням невизначеності господарської діяльності ІТ-компаній.

Важливо зазначити, що податкова політика держави має для вітчизняних ІТ-підприємств подвійний вплив: з одного боку, вона відкриває нові можливості для розвитку бізнесу, а з іншого – може формувати додаткові загрози для його фінансової безпеки. Одним із найбільш помітних кроків у напрямку підтримки галузі стало створення більш сприятливих умов для

функціонування ІТ-бізнесу в рамках спеціального правового режиму «Дія.City» [265], що передбачає особливі умови оподаткування доходів ІТ-компаній та спеціалістів (зниження ставки податку на доходи фізичних осіб ІТ-спеціалістів до 5 %, запровадження податку на виведений капітал за ставкою 9 % тощо) [155]. Також у межах режиму «Дія.City» було впроваджено нові форми організації трудових відносин (гіг-контракти), що сприяло формуванню більш гнучкого правового поля функціонування ІТ-компаній [265].

Отже, загалом запровадження режиму «Дія.City» було спрямоване на підвищення прогнозованості податкового навантаження для резидентів, зміцнення довіри з боку інвесторів та іноземних контрагентів, а також на детінізацію ІТ-бізнесу через стимулювання більш прозорих моделей ведення діяльності та оформлення трудових відносин [44].

Проте на практиці позитивний ефект від функціонування «Дія.City» частково нівелюється частими змінами податкового законодавства через війну. Зокрема, підвищення ставки військового збору до 5 % наприкінці 2024 р., зміни у сфері оподаткування ФОП та загальне зростання фіскального навантаження на фонд оплати праці збільшують операційні витрати ІТ-компаній [107]. За оцінками галузевих експертів, податкові зміни останніх років стали одним із чинників оптимізації витрат та загального перегляду бізнес-моделей окремих ІТ-компаній [258].

У таких умовах неможливість прогнозування податкового навантаження в довгостроковій перспективі посилює невизначеність управлінських рішень і спонукає бізнес до пошуку альтернативних варіантів функціонування, у тому числі й через релокацію частини операцій або юридичних структур за кордон [77]. Крім того, резиденти «Дія.City» мають щорічно підтверджувати свій статус, що створює додаткове адміністративне та фінансове навантаження, особливо для ІТ-підприємств малого та середнього бізнесу.

На сьогодні окремим проявом регуляторної нестабільності в умовах воєнного стану є невизначеність, пов'язана з мобілізаційними процесами та механізмами бронювання працівників ІТ-галузі. За оцінками 2024–2025 рр.,

близько 75 % ІТ-компаній мають у штаті мобілізованих спеціалістів [271]. За відсутності чітких та стабільних механізмів бронювання це створює високий рівень невизначеності як для самих ІТ-компаній, так і для іноземних замовників, які побоюються раптового припинення реалізації проєктів у разі мобілізації ключових розробників. У результаті ускладнюється планування кадрової політики, зростають ризики втрати спеціалістів, зменшується здатність ІТ-компаній виконувати довгострокові контракти.

Зовнішні *економічні загрози* фінансовій безпеці підприємств ІТ-сфери охоплюють комплекс дестабілізаційних макроекономічних чинників, до яких насамперед належать сповільнення темпів економічного зростання, інфляційні ризики, валютна нестабільність та девальвація, зниження зовнішнього попиту на ІТ-послуги, а також обмежений доступ до кредитних та інвестиційних ресурсів.

Протягом 2014–2024 рр. макроекономічна ситуація в Україні характеризувалась високим рівнем нестабільності, що проявлялося у значних коливаннях ключових макроекономічних показників (ВВП, рівень інфляції, валютний курс та ін.), що було наслідком одночасного впливу внутрішніх структурних проблем та зовнішніх потрясінь, насамперед пов'язаних із коронокризою та повномасштабною війною.

Після рекордного падіння ВВП більше ніж на 20 % у 2022 р. вже у 2023 р. спостерігалось певне пожвавлення економічної активності, а темпи зростання становили близько 12 % (рис. 3.2). Однак у 2024 р. економічне відновлення дещо втратило динаміку, а зростання ВВП сповільнилось до 5,2 %, що вказує на його нестійкий характер та високу залежність від негативного впливу зовнішніх і внутрішніх факторів.

За таких умов для ІТ-компаній посилюється економічна невизначеність, що ускладнює стратегічне фінансове планування та формування довгострокових інвестиційних програм. Зміни загальноекономічної ситуації безпосередньо впливають на попит на цифрові послуги, рівень ділової активності та поведінку іноземних замовників, які залишаються ключовими споживачами українських ІТ-послуг.

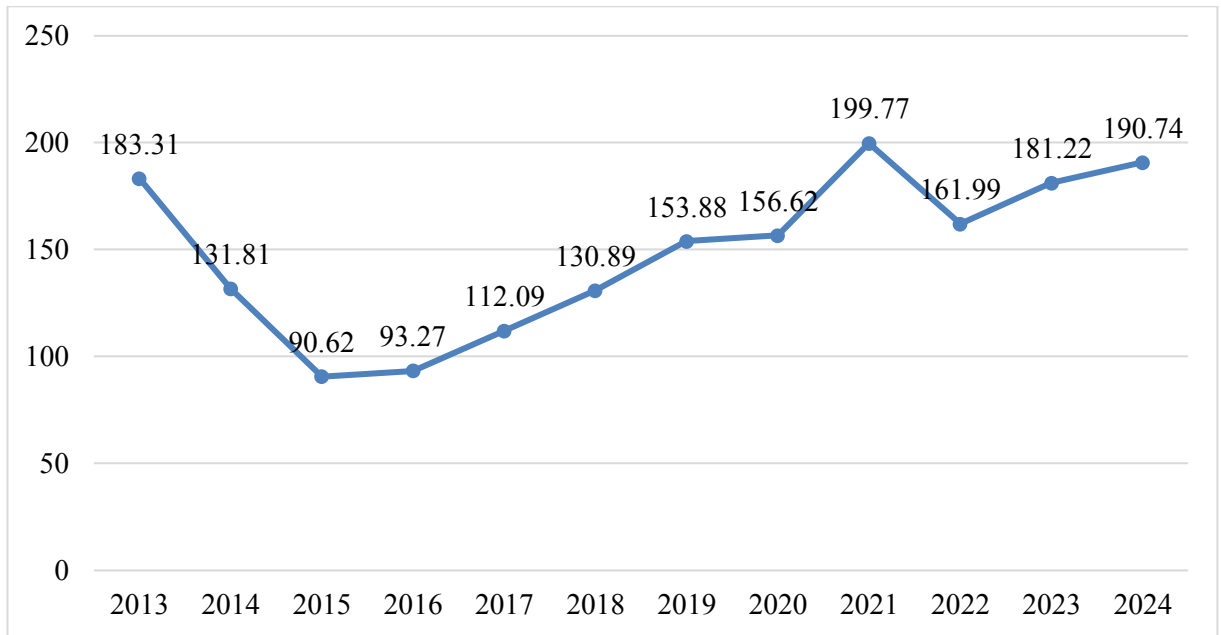


Рис. 3.2. ВВП України, млрд дол. США

Джерело: [61].

Серед макроекономічних чинників найбільш дестабілізаційний вплив на фінансову безпеку ІТ-підприємств мають інфляційні процеси та валютна нестабільність. При чому в умовах воєнної економіки ці чинники набувають довгострокового характеру й формують стійкі загрози для ІТ-бізнесу.

Як свідчать статистичні дані, індекс споживчих цін в Україні протягом останніх років характеризується нерівномірною динамікою (рис. 3.3).

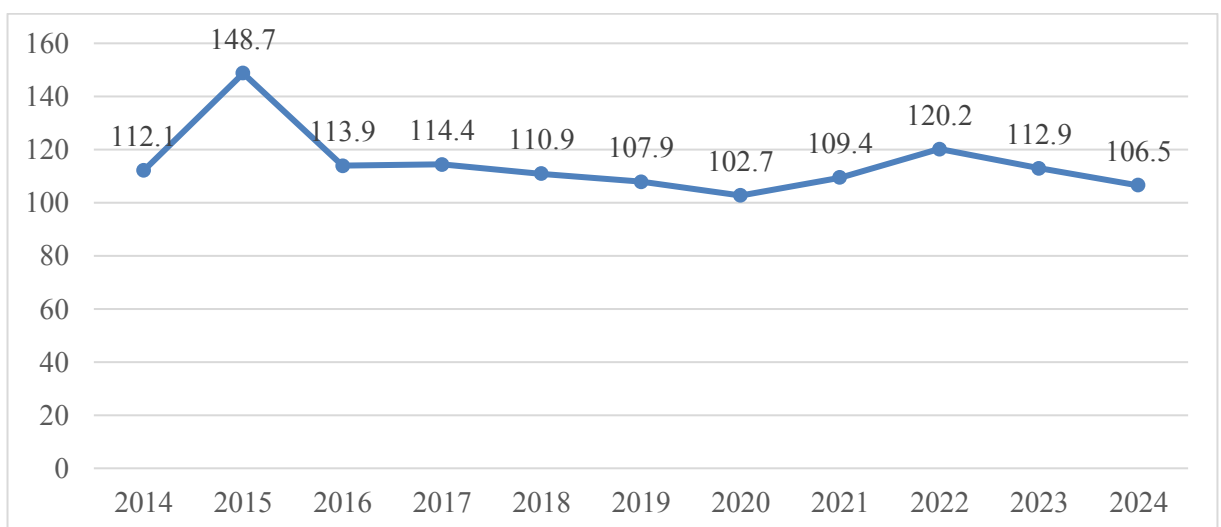


Рис. 3.3. Динаміка індексу споживчих цін в Україні, %

Джерело: [61; 153].

На інфляційні процеси в різні роки по-різному впливали як особливості монетарної політики НБУ, так і внутрішні структурні дисбаланси економіки, коливання світових цін і наслідки воєнних дій. Так, періоди різкого прискорення інфляції в умовах економічної кризи 2014–2015 рр. та у 2022 р. – з початком повномасштабної війни, змінювалися фазами відносної цінової стабілізації. І навіть у періоди уповільнення інфляції її наслідки продовжували впливати на економічну поведінку суб'єктів господарювання, формуючи середньо- та довгострокові інфляційні ризики.

Для ІТ-сектору інфляція насамперед означає зростання операційних витрат та підвищення собівартості ІТ-послуг. Особливо відчутним є вплив інфляції на витрати на оплату праці, які складають переважну частину операційних витрат ІТ-підприємств. Так, коли у 2024-2025 рр. номінальні зарплати ІТ-спеціалістів зросли на 10-15 %, їх реальний дохід через інфляцію скоротився на 10-25 % рис. 3.4 [140]. Безумовно, зниження реальної купівельної спроможності працівників змушує ІТ-підприємства коригувати фонд оплати праці з метою утримання висококваліфікованих кадрів та забезпечення кадрової стабільності. Як наслідок, посилюється фінансовий тиск на бізнес, знижується реальна прибутковість діяльності та ускладнюється прогнозування витрат.

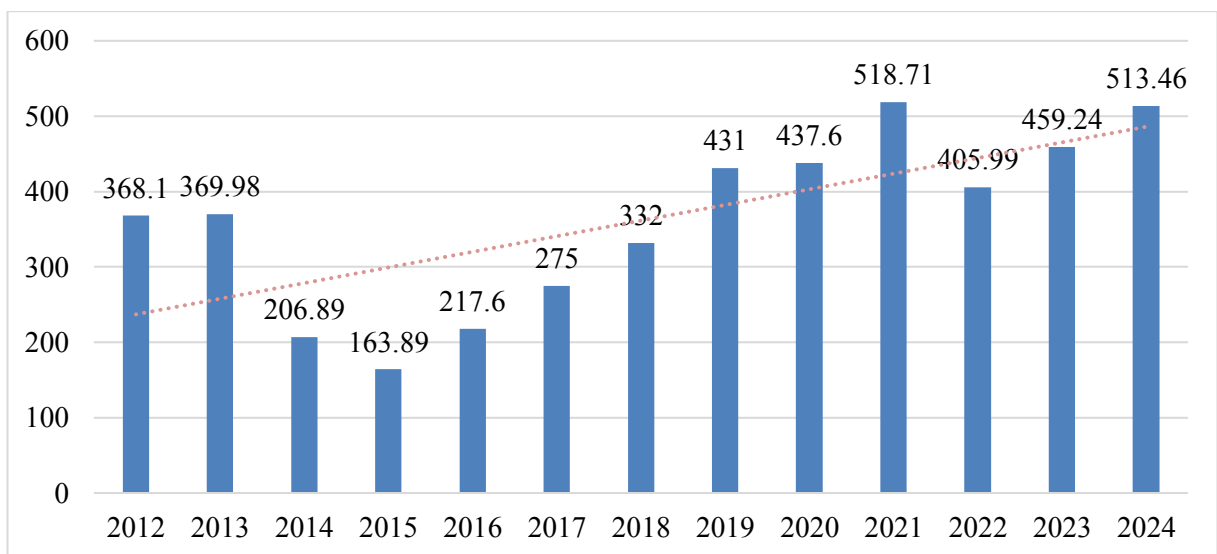


Рис. 3.4. Середня заробітна плата, дол. США

Джерело: [61; 153].

Особливо вразливими до таких процесів залишаються малі ІТ-підприємства, фінансові можливості яких щодо формування резервів є досить обмеженими. Для сервісних ІТ-компаній ситуація ускладнюється ще й тим, що нестабільність кадрових витрат поєднується з невизначеністю щодо обсягів майбутніх контрактів, що змушує їх постійно переглядати бюджети, моделі ціноутворення та структуру команд [77].

Поряд з інфляцією суттєвий дестабілізаційний вплив на фінансову безпеку ІТ-підприємств здійснюють коливання валютного курсу. Девальвація гривні (рис. 3.5), як, наприклад, у 2022 р., з одного боку, тимчасово підвищила цінову конкурентоспроможність експортноорієнтованих ІТ-компаній, однак з іншого – посилила валютні ризики.

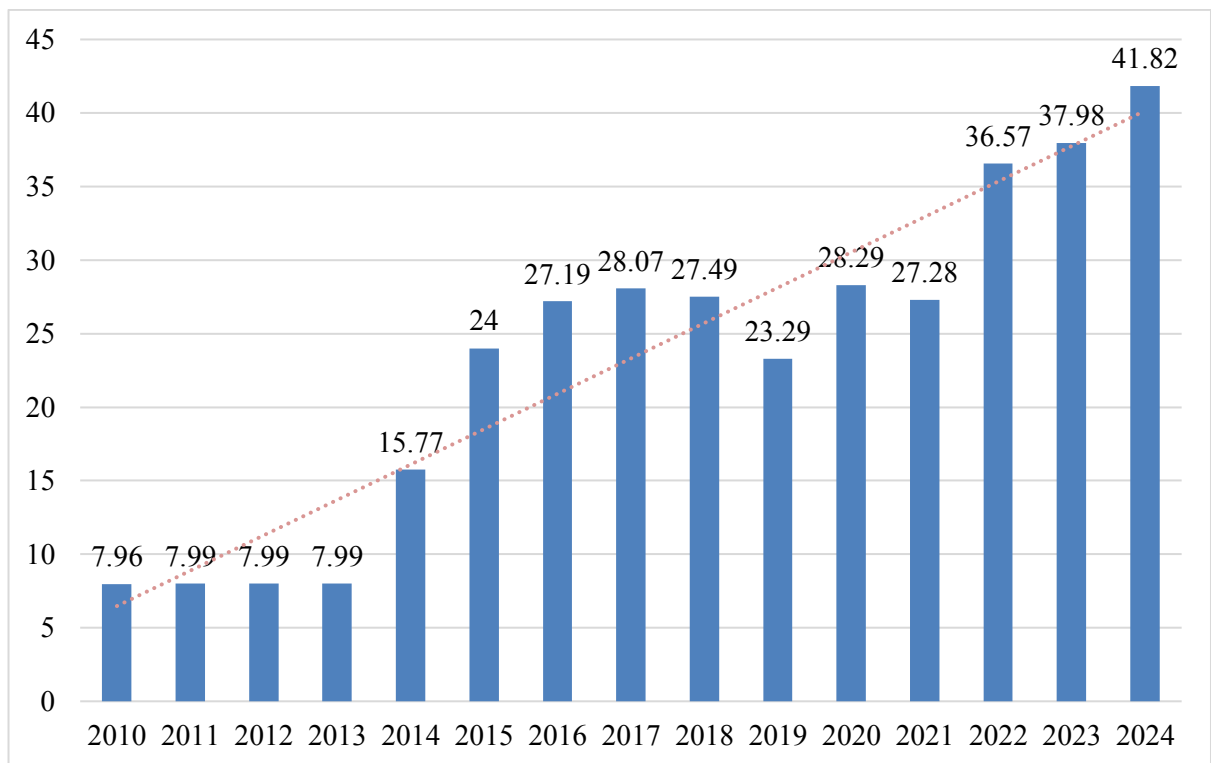


Рис. 3.5. Динаміка курсу гривні щодо дол. США

Джерело: [153].

Враховуючи те, що значна частина вітчизняних ІТ-компаній отримують доходи в іноземній валюті, тоді як основні витрати формуються в національній, валютна нестабільність ускладнює оцінку фактичної вартості доходів і витрат підприємств, посилює ризики курсових різниць і викривлює фінансові

показники. Управління ліквідністю та фінансове планування в таких умовах потребують більшої гнучкості, постійного коригування бюджетних показників і врахування валютних ризиків у процесі ухвалення фінансових рішень.

Крім того, девальвація гривні призводить до зростання вартості імпортного обладнання, програмного забезпечення, хмарних сервісів та інших цифрових інструментів, які використовуються в діяльності ІТ-компаній. Це збільшує операційні витрати ІТ-компаній, особливо для малих і середніх ІТ-підприємств, які мають обмежені можливості хеджування валютних ризиків.

Враховуючи високу інтегрованість ІТ-сектору України в міжнародні ринки, можемо констатувати, що фінансова безпека ІТ-підприємств значною мірою залежить від зовнішньоекономічного середовища, рівня міжнародної співпраці та довіри, а також стабільності попиту на вітчизняні ІТ-продукти з боку іноземних замовників. Для більшості українських ІТ-компаній експорт ІТ-послуг залишається основним джерелом валютних надходжень, а отже – і чинником підвищеної чутливості до міжнародних політичних, економічних і безпекових ризиків.

Проте повномасштабна війна суттєво ускладнила умови міжнародної взаємодії українських ІТ-підприємств і призвела до скорочення зовнішнього попиту на ІТ-продукти та послуги. За даними IT Ukraine Association, у 2022–2024 рр. обсяги нових контрактів з іноземними замовниками зменшились на 20-30 % порівняно з піковими значеннями 2021 р. [194]. Водночас змінилась структура контрактів, а саме зросла частка короткострокових угод і пілотних проєктів замість довгострокових контрактів, що посилює нестабільність доходів ІТ-компаній.

Додатковим чинником зниження зовнішнього попиту стало посилення вимог іноземних клієнтів до кіберстійкості та безперервності наданих послуг українськими ІТ-компаніями. І хоча американські та європейські компанії з початком повномасштабної війни переважно продовжували співпрацю за вже чинними контрактами, значна частина потенційних замовників утримується

від укладання нових через ризики невиконання зобов'язань та можливі перебої в роботі команд. Для окремих ІТ-компаній це призвело до втрати 80 % потенційних замовлень [184].

Водночас загострюється конкуренція на глобальному ринку ІТ-послуг з боку країн із більш стабільним політико-правовим середовищем (Польщі, Індії, держав південно-східної Азії). Переорієнтація частини іноземних замовників на інші країни посилює ціновий тиск на українські ІТ-компанії, ускладнює залучення нових клієнтів, що, відповідно, негативно впливає на доступ до міжнародних фінансових ресурсів та інвестиційні можливості розвитку ІТ-бізнесу.

Не менш важливою економічною загрозою для фінансової безпеки ІТ-підприємств є обмежений доступ до кредитних та інвестиційних ресурсів. Однак упродовж останніх років можливості залучення кредитних ресурсів та інших альтернативних джерел фінансування для вітчизняного ІТ-сектору суттєво звузилися. Якщо до 2021 року кредитне середовище для українського бізнесу залишалось відносно сприятливим: облікова ставка поступово знижувалась, а банківські кредити ставали доступнішими, то з початком повномасштабної війни ситуація кардинально змінилася (рис. 3.6). У червні 2022 р. НБУ був змушений підвищити облікову ставку до 25 %, щоб стримати девальвацію та захистити гривневі активи. Унаслідок цього банківські кредити для бізнесу суттєво подорожчали і стали малодоступними. Навіть у 2024 р. при пом'якшенні монетарної політики НБУ, вартість кредитів залишалася високою, тоді як валютні кредити були доступні переважно експортоорієнтованим компаніям зі стабільною валютною виручкою [234; 209].

Ситуацію додатково ускладнює проблема непрацюючих кредитів у банківській системі. У червні 2024 року їхня частка становила 34,6 %, а у корпоративному секторі – 40,7 % [234], що змушувало банки суттєво обмежувати кредитну пропозицію.

Крім того, державні програми субсидування, насамперед «5–7–9%», фактично стали одним із небагатьох каналів доступу малого та середнього бізнесу до фінансування. Наприкінці 2024 р. частка таких кредитів сягнула

33,7 % у чистому гривневому корпоративному портфелі [234]. Отже, можемо констатувати, що банківське кредитування без державної підтримки наразі перебуває у стані стагнації.

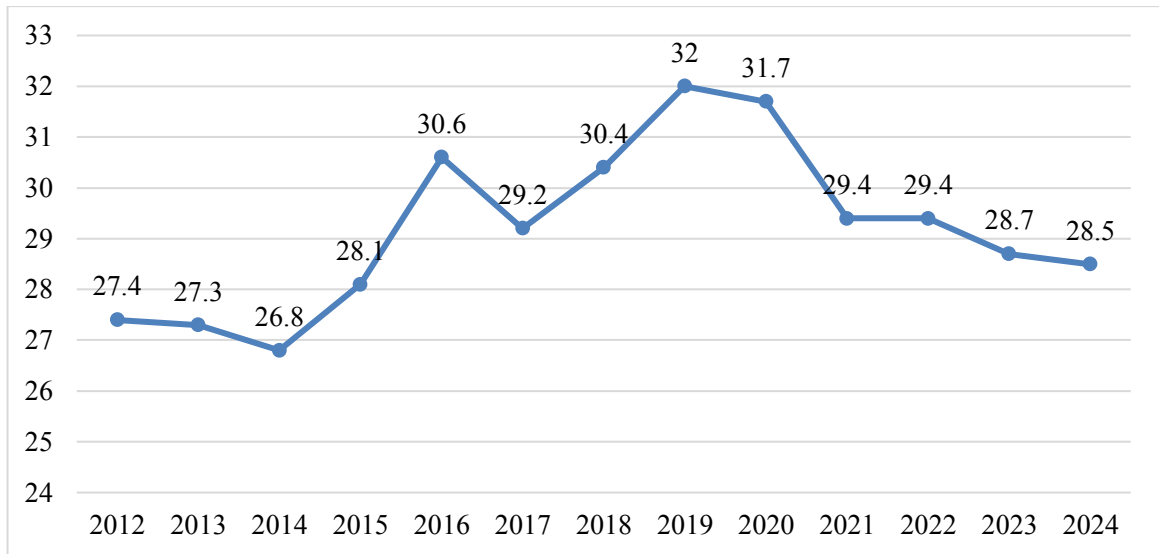


Рис. 3.6. Відсоткова ставка за кредитами для юридичних осіб, %
Джерело: [153].

Для ІТ-компаній проблема доступу до фінансування проявляється не лише у високій вартості банківських кредитів. Як засвідчує Устинов Я., отримання банківських кредитів для ІТ-бізнесу пов'язане з необхідністю відповідати критеріям прийнятності та надавати заставу, що є особливо проблематичним для невеликих та менш розвинених ІТ-компаній. Крім того, погашення кредиту разом із відсотками може негативно впливати на грошові потоки компанії, особливо на початкових етапах її розвитку. За таких умов основним джерелом фінансування стартапів в Україні часто залишаються власні кошти засновників, що саме по собі свідчить про наявність проблеми з доступом до зовнішнього фінансування ІТ-проектів [209].

Обмеженість доступу до капіталу для ІТ-підприємств посилюється також недостатнім розвитком альтернативних джерел фінансування. Попри зростання ролі венчурного капіталу, прямих іноземних інвестицій та інших інструментів фінансування, їх доступність для широкого кола вітчизняних ІТ-компаній залишається недостатньою. Це означає, що для багатьох

підприємств, особливо малих і стартап-компаній, зовнішнє фінансування або є дорогим, або вимагає виконання умов, які вони не можуть забезпечити [209].

Для підприємств ІТ-сфери це має особливо відчутні наслідки, оскільки саме доступ до капіталу визначає можливості фінансування R&D, модернізацію технологічної інфраструктури, посилення кіберзахисту чи запуску нових продуктів. Особливо вразливими в цих умовах залишаються малі та середні ІТ-компанії, для яких банківське кредитування фактично стало недосяжним, а альтернативні джерела фінансування – обмеженими. Проблему поглиблює недостатній розвиток фінансової інфраструктури. В Україні досі відсутній повноцінний фондовий ринок та майже не працюють механізми фінансових гарантій.

Таким чином, обмежений доступ до кредитних ресурсів і капіталу перетворюється на системну економічну загрозу фінансовій безпеці ІТ-підприємств, що проявляється у:

- дефіциті інвестиційних ресурсів для масштабування продуктів та інноваційного розвитку;
- зростанні вартості капіталу та фінансового навантаження на операційну діяльність;
- відкладенні модернізації технологічної інфраструктури та інвестицій у кіберстійкість;
- підвищенні ризиків втрати ліквідності та платоспроможності.

Зовнішні *технологічні загрози* фінансовій безпеці підприємств ІТ-сфери формуються під впливом стрімких технологічних змін, посилення кіберзагроз, зростання вимог до цифрової стійкості та необхідності постійного оновлення технологічної бази. Для ІТ-компаній такі чинники мають особливо важливе значення, оскільки саме технологічне середовище визначає їхню конкурентоспроможність, здатність забезпечувати безперервність діяльності, виконувати контрактні зобов'язання та підтримувати належний рівень захисту даних. За таких умов технологічні загрози безпосередньо трансформуються у фінансові та операційні ризики, що впливають на витрати, доходи, рентабельність та фінансову стійкість ІТ-бізнесу.

Однією з найбільш небезпечних технологічних загроз для фінансової безпеки ІТ-підприємств України на сьогодні є стрімке зростання кількості та складності кібератак, значна частина яких здійснюється з боку держави-агресора. Після 2022 р. кіберпростір фактично перетворився на «цифровий фронт», де об'єктами атак стають не лише державні інформаційні ресурси та критична інфраструктура, а і приватний бізнес.

За офіційними даними лише у 2024 р. в Україні було зафіксовано 4315 кіберінцидентів, що на 70 % більше, ніж у 2023 р. (2541 кіберінцидент). У 2025 році негативна тенденція посилюється: станом на березень кількість атак сягнула 1384, що на 50 % більше, ніж за аналогічний період минулого року [183].

Зростання кіберзлочинності має прямі фінансові наслідки для ІТ-бізнесу. Навіть один серйозний кіберінцидент може призвести до зриву контрактів, втрати даних, зростання репутаційних ризиків та суттєвих витрат на відновлення інфраструктури. У таких умовах ІТ-компанії змушені постійно удосконалювати системи кіберзахисту, додатково залучати фахівців з кібербезпеки, оновлювати захисні програмні рішення та здійснювати постійний моніторинг ризиків [129].

Зазначені процеси, безперечно, супроводжуються помітним зростанням відповідних витрат ІТ-підприємств, що підтверджується динамікою вітчизняного ринку кібербезпеки, обсяги якого за останні вісім років зросли у чотири рази. Якщо у 2016 році його обсяг становив 32 млн дол., то у 2020 – 70 млн дол., а у 2024 році – вже 138 млн дол. [129].

Також війна завдала значної шкоди телекомунікаційним та енергетичним мережам, а також іншій цифровій інфраструктурі. За оцінками спеціалістів, з початку війни прямі збитки для цифрової інфраструктури сягнули 1,2 млрд дол. [58], а сукупні втрати для українського ІТ-сектору станом на 2024 р. оцінюються у 19,3 млрд дол. [54]. Такі масштаби втрат свідчать про системний характер технологічних загроз для фінансової безпеки галузі.

Пошкодження енергетичної та телекомунікаційної інфраструктури, ракетні атаки на енергетичні об'єкти, тривалі відключення світла створюють для ІТ-компаній прямі ризики припинення або збоїв операційної діяльності

(нестабільність доступу до інтернету, перебої в роботі дата-центрів, зриви дедлайнів по проєктах, вимушені простоя команди тощо).

У відповідь на ці виклики ІТ-компанії змушені здійснювати незаплановані інвестиції в автономне енергозабезпечення, Starlink, резервні канали зв'язку та ін. Хоча такі заходи дозволяють частково знизити операційні ризики, вони водночас створюють додаткове фінансове навантаження, що особливо відчутно для малих і середніх ІТ-підприємств.

Як було зазначено вище, важливою особливістю діяльності підприємств ІТ-галузі є швидкі темпи технологічних змін та динамічність розвитку цифрових технологій, з якими безпосередньо пов'язане їх функціонування. Поява нових програмних продуктів та технологій, автоматизація бізнес-процесів, активне застосування інструментів штучного інтелекту та хмарних технологій потребують постійних інвестицій у модернізацію та оновлення виробничо-технологічної бази ІТ-підприємств та професійних компетенцій персоналу.

Проте з початком повномасштабної війни значна частина компаній була вимушена переорієнтувати фінансові ресурси на підтримку безперервності операційної діяльності, кіберзахист та інші безпекові заходи. У результаті уповільнюються темпи інноваційної активності, підвищуються ризики технологічного відставання вітчизняного ІТ-сектору та знижується його конкурентоспроможність на міжнародному ринку. У короткостроковій перспективі це проявляється у втраті привабливості українських ІТ-компаній для іноземних замовників, а в довгостроковій – у втраті частини ринків, зниженні рентабельності та обмеженні потенціалу розвитку.

Крім того, відкладені інвестиції в оновлення матеріально-технічної бази в майбутньому можуть перетворитись у значні капіталовкладення, необхідні для термінової модернізації ІТ-продуктів і технологічної інфраструктури, що додатково підвищує фінансове навантаження на ІТ-підприємства.

Окремим джерелом технологічних ризиків є залежність українських ІТ-компаній від зовнішніх цифрових платформ, міжнародних провайдерів хмарних сервісів та ін. У мирний час така залежність сприяла інтеграції

вітчизняного ІТ-бізнесу у глобальний цифровий простір, однак в умовах війни вона стає чинником його додаткової вразливості. Особливо небезпечними стають ситуації, коли підприємство критично залежить від одного провайдера, що робить його фінансово вразливим до будь-яких змін умов співпраці.

Окремим сучасним викликом для сервісних ІТ-компаній є стрімкий розвиток інструментів штучного інтелекту, які здатні автоматизувати частину типових завдань і, відповідно, зменшувати потребу в певних категоріях виконавців. Унаслідок цього для частини сервісних ІТ-компаній зростають ризики втрати частини клієнтів та необхідності додаткових інвестицій у технологічне оновлення й підвищення кваліфікації персоналу [258].

У системі зовнішніх загроз фінансовій безпеці ІТ-підприємств України вагоме місце посідають *соціальні загрози*, оскільки саме людський капітал залишається ключовим стратегічним ресурсом та головною конкурентною перевагою вітчизняної ІТ-галузі. Для ІТ-бізнесу фінансова стійкість значною мірою залежить від здатності зберігати кадровий потенціал, підтримувати його професійний розвиток і забезпечувати стабільність трудових відносин.

В умовах повномасштабної війни соціальні ризики для ІТ-підприємств істотно загострилися. І навіть попри те, що багато ІТ-компаній змогли адаптуватися, вимушена міграція фахівців, зростаючий дефіцит кадрів, трансформація ринку праці та поглиблення диспропорцій у підготовці спеціалістів залишаються тими загрозами, які ускладнюють операційну діяльність, підвищують ризики невиконання контрактних зобов'язань та призводять до зростання операційних витрат ІТ-підприємств.

Однією з найпомітніших соціальних загроз для ІТ-сфери стала вимушена міграція населення та відтік трудових ресурсів за кордон. У період 2022-2025 рр. Україна зіткнулася з безпрецедентним відтоком трудових ресурсів. Станом на липень 2025 року близько 5,7 млн українців залишаються за кордоном [232], а кількість ІТ-фахівців за межами країни у 2025 році оцінюється у 58 тис. осіб. І хоча це на 10 % менше, ніж у 2024 р., ризик остаточної втрати цих кадрів залишається доволі високим [205].

Ситуацію погіршує ще й той факт, що зростає відтік молоді за кордон. Попри наявність в Україні значної кількості закладів вищої освіти, що здійснюють підготовку за технічними та комп'ютерними спеціальностями, дедалі більше абітурієнтів обирають навчання за кордоном. У 2025 році ця тенденція ще більше посилилась після послаблення правил виїзду для молоді, що створює ризики скорочення майбутнього кадрового резерву для ІТ-сфери. За таких умов проблема набуває не лише поточного, а і стратегічного характеру, адже йдеться вже не просто про нестачу окремих фахівців, а про поступове послаблення механізмів відтворення людського капіталу в галузі.

Окремого аналізу потребують демографічні зміни. Тут серйозною загрозою стає поступове зростання середнього віку українських ІТ-спеціаліста. З одного боку, це свідчить про професійну зрілість галузі, але з іншого – вказує на обмежений приплив молодих талантів, що у перспективі загрожують дефіцитом молодих кадрів.

Додатковий тиск на фінансову безпеку ІТ-компаній створює трансформація самого ринку праці. Погіршення зовнішньої кон'юнктури, скорочення попиту на ІТ-послуги на міжнародних ринках і зменшення обсягів нових замовлень змушують компанії переглядати кадрову політику. У таких умовах вони змушені заморожувати або навіть знижувати зарплати, проводити оптимізацію чисельності працівників та скорочувати інвестиції в розвиток персоналу. Такі процеси підвищують ризики втрати ключових спеціалістів.

Паралельно з цим ще більше посилюється вже набута тенденція до зміни форматів організації праці. Зростає частка дистанційної, гібридної та проєктної зайнятості. З одного боку, це підвищує гнучкість ІТ-компаній, але з іншого – ускладнює управління персоналом, підвищує витрати та посилює ризики недотримання термінів та вимог до якості виконання контрактів. Частина компаній уже зіткнулася з необхідністю перегляду у зв'язку з цим фінансових планів [140].

Освітні дисбаланси в ІТ-сфері проявляються в невідповідності компетентностей випускників потребам ІТ-бізнесу, фрагментації освітніх програм і недостатній практико-орієнтованій підготовці молодих фахівців. Особливо це помітно на тлі зміщення попиту від базових напрямів веброзробки до компетенцій, що пов'язані з аналізом великих даних, штучним інтелектом, хмарними технологіями та автоматизацією [28]. Однак не всі освітні заклади встигають переорієнтовувати свої освітні програми відповідно до цієї динаміки, а отже, посилюються ризики невідповідності між темпами підготовки кадрів і зміною потреб ІТ-ринку.

Для підприємств ІТ-сфери така ситуація має цілком відчутні фінансові наслідки. Недостатня кількість фахівців із сучасними компетенціями посилює конкуренцію за кадри, вимагає підвищення витрат на оплату праці та потребує від ІТ-компаній додаткового інвестування в навчання та перекваліфікацію персоналу.

Нові виклики в умовах війни та повоєнного відновлення виникають у зв'язку з інтеграцією ветеранів у трудові колективи. На сьогодні 35 % компаній уже мають ветеранів у штаті, що вимагає впровадження програм психологічної підтримки, реабілітації та адаптації робочих процесів [205]. Відповідно, виникають нові управлінські та фінансові виклики для ІТ-підприємств, неефективне подолання яких може призводити до зростання плинності кадрів, негативно впливати на продуктивність праці та фінансові результати діяльності.

Нарешті, соціальні загрози для ІТ-бізнесу посилюються і через нерівномірність розвитку цифрової інфраструктури в регіонах. У малих містах і сільській місцевості зберігаються проблеми з якістю інтернету, доступом до ІТ-освіти, цифровими сервісами. Це стримує розвиток локальних ринків праці, обмежує можливості для створення регіональних ІТ-хабів і знижує конкурентоспроможність невеликих регіональних ІТ-компаній.

Отже, проведений аналіз дозволяє систематизувати ключові зовнішні загрози фінансовій безпеці підприємств ІТ-сфери за компонентами PEST-аналізу, із виокремленням їх змістовних характеристик та основних напрямів впливу на фінансову безпеку підприємств (табл. В.1, додаток В).

На основі проведеної систематизації можемо констатувати, що найбільш деструктивний вплив на фінансову безпеку підприємств ІТ-сфери в сучасних умовах мають воєнно-політичні, макроекономічні, валютно-регуляторні та технологічні загрози, які одночасно впливають на стабільність грошових потоків, інвестиційну активність і безперервність операційної діяльності ІТ-компаній.

Варто зазначити, що спроможність ІТ-підприємства протистояти зовнішнім загрозам і негативним впливам значною мірою залежить від його внутрішнього фінансового стану та наявних можливостей. Вирішальне значення при цьому мають фінансовий потенціал підприємства, ефективність системи фінансового контролінгу та здатність своєчасно реагувати на зміни зовнішнього середовища. Саме якість фінансового управління визначає, наскільки підприємство здатне мінімізувати негативний вплив зовнішніх дестабілізаційних чинників і знижувати вразливість до кризових ситуацій.

Тому аналіз зовнішніх загроз доцільно доповнити дослідженням внутрішніх ризиків фінансової безпеки, що формуються в процесі фінансово-господарської діяльності ІТ-підприємств та, на відміну від зовнішніх чинників, мають переважно керований характер і можуть бути оцінені та нейтралізовані системою фінансового менеджменту.

У цьому дослідженні внутрішні ризики фінансової безпеки підприємств ІТ-сфери, з урахуванням галузевої специфіки, вважаємо за доцільне систематизувати за напрямками їхнього впливу та можливостями своєчасного виявлення і мінімізації. Зважаючи на це, пропонуємо виокремити фінансові, інвестиційні, кадрові, управлінські, операційні та інформаційно-технологічні ризики (рис. 3.7), які формуються в процесі фінансово-господарської діяльності ІТ-підприємства та безпосередньо впливають на рівень його фінансової безпеки.

З метою узагальнення результатів проведеного аналізу внутрішніх ризиків і зовнішніх загроз фінансовій безпеці підприємств ІТ-сфери України, а також з урахуванням результатів аналізу їхнього фінансового стану та інтегральної оцінки рівня фінансової безпеки, здійснених у другому розділі дисертації, вважаємо доцільним тепер провести SWOT-аналіз системи фінансової безпеки вітчизняних ІТ-підприємств (табл. 3.1).

Внутрішні ризики фінансової безпеки підприємств ІТ-сфери		
	Характеристика	Фінансові наслідки
Фінансові	<ul style="list-style-type: none"> - нестабільність грошових потоків унаслідок проєктного характеру діяльності та нерівномірності надходжень виручки; - висока концентрація доходів на обмеженій кількості ключових клієнтів; - недостатність власних фінансових ресурсів для фінансування розвитку; - неефективне використання фінансових і нематеріальних ресурсів; - перевищення фактичних витрат над запланованими у межах окремих ІТ-проєктів. 	<ul style="list-style-type: none"> - порушення ліквідності; - виникнення касових розривів та підвищення ризику втрати платоспроможності; - зменшення виручки та рентабельності; - зниження фінансової стійкості; - обмеження інноваційної активності; - зниження прогнозованості фінансових результатів та складність фінансового планування; - уповільнення оборотності активів.
Кадрові	<ul style="list-style-type: none"> - втрата ключових ІТ-спеціалістів; - зростання витрат на персонал; - висока плинність кадрів; - відставання професійних навичок персоналу від темпів технологічних змін; - недостатній рівень розвитку цифрових компетентностей персоналу. 	<ul style="list-style-type: none"> - зниження продуктивності праці; - втрата інтелектуального капіталу; - зростання операційних витрат; - скорочення доходів та зменшення прибутковості через зниження якості ІТ-послуг; - зростання собівартості ІТ-продуктів.
Інформаційно-технологічні	<ul style="list-style-type: none"> - недостатній рівень кіберзахисту даних та внутрішніх інформаційних систем; - вразливість до шахрайських схем у цифровому середовищі; - низький рівень якості управління внутрішньою інформаційною безпекою; - застарілі технологічні рішення та програмне забезпечення; - недостатність інвестицій у R&D та модернізацію. 	<ul style="list-style-type: none"> - прямі фінансові втрати внаслідок кіберінцидентів; - штрафи та фінансові втрати, пов'язані з репутаційними збитками; - втрата конкурентних позицій; - скорочення доходів.
Інвестиційні	<ul style="list-style-type: none"> - зниження інвестиційної привабливості в умовах високої невизначеності; - зниження довіри інвесторів через інциденти з даними та порушення інформаційної безпеки; - неефективний відбір та реалізація інвестиційних проєктів; - зниження рівня довіри інвесторів до фінансової стійкості та прозорості діяльності ІТ-підприємства; - обмеженість внутрішніх фінансових ресурсів для співфінансування інвестиційних проєктів. 	<ul style="list-style-type: none"> - ускладнення доступу до венчурного та прямого фінансування; - перевищення фактичних інвестиційних витрат та недоотримання запланованого прибутку; - відтермінування або згортання інвестиційних проєктів.
Управлінські	<ul style="list-style-type: none"> - недостатня ефективність системи фінансового управління та внутрішнього контролю; - відсутність системного підходу до ідентифікації, оцінювання та управління фінансовими ризиками; - недостатнє застосування цифрових інструментів у системі фінансового управління; - формальний або несистемний характер політик управління цифровими ризиками (доступи, резервування, реагування) 	<ul style="list-style-type: none"> - помилки при здійсненні фінансового планування та прогнозування; - неефективне використання фінансових та нематеріальних ресурсів; - зниження оперативності та якості фінансових управлінських рішень; - підвищення загальної фінансової вразливості підприємства.

Рис. 3.7 Систематизація внутрішніх ризиків фінансової безпеки підприємств ІТ-сфери

Джерело: складено автором на основі [194; 209; 37].

SWOT-аналіз системи фінансової безпеки підприємств ІТ-сфери України

Сильні сторони	Слабкі сторони
<ul style="list-style-type: none"> - високий рівень ліквідності та платоспроможності; - короткий операційний та фінансовий цикл; - низька капіталомісткість та домінування нематеріальних активів; - гнучкість структури операційних витрат та можливість їх оперативного коригування; - стійке зростання прибутковості ІТ-підприємств; - швидке відновлення рентабельності після 2022 р.; - достатньо високий запас фінансової міцності; - переважання власних джерел фінансування та низька залежність від позикового капіталу; - стійка позитивна динаміка інтегрального показника фінансової безпеки; - експортна орієнтація ІТ-сектору; - високий рівень мобільності ІТ-бізнесу та оперативна адаптація до змін зовнішнього середовища. 	<ul style="list-style-type: none"> - висока залежність від зовнішніх ринків збуту та валютної виручки; - висока чутливість фінансових результатів до макроекономічних і валютних ризиків; - зниження інвестиційної активності та обмежений доступ до венчурного і прямого фінансування в умовах війни; - уповільнення темпів зростання інтегрального показника фінансової безпеки у 2023–2024 рр.; - структурні дисбаланси між складовими фінансової безпеки, зокрема низький рівень інвестиційної привабливості; - вразливість до кадрових ризиків (релокація, відтік спеціалістів, зростання витрат на персонал); - уповільнення оборотності активів та ефективності використання фінансових ресурсів у порівнянні з довоєнним періодом.
Можливості	Загрози
<ul style="list-style-type: none"> - поглиблення цифрової трансформації економіки та зростання глобального попиту на ІТ-послуги, зокрема у сферах FinTech, кібербезпеки, оборонного сектору, GovTech та ін.; - поглиблення інтеграції України до цифрового та економічного простору ЄС, що відкриває доступ до нових ринків, програм фінансування та інституційної підтримки ІТ-підприємств; - потенційне відновлення інвестиційної активності у перспективі за умови стабілізації безпекової ситуації та розвитку державних програм підтримки ІТ-бізнесу; - використання внутрішнього фінансового потенціалу та накопиченого запасу фінансової міцності для диверсифікації продуктів і ринків збуту; - використання цифрових фінансових інструментів, аналітики даних і автоматизованих систем управління для підвищення якості фінансового планування та контролю на ІТ-підприємствах. 	<ul style="list-style-type: none"> - тривалий воєнний стан та пов'язані з ним макроекономічні (нестабільність валютного курсу, інфляційний тиск, скорочення інвестицій), а також кадрові та демографічні ризики (мобілізація, відтік кадрів); - посилення кіберзагроз і ризиків втрати даних, інтелектуальної власності та репутаційних активів, що мають прямі фінансові наслідки для ІТ-підприємств; - регуляторна та податкова невизначеність, зміни у податковому, валютному та трудовому законодавстві, що ускладнюють фінансове планування та управління ризиками; - обмеження доступу до довгострокових фінансових ресурсів та зростання вартості капіталу в умовах підвищених ризиків; - посилення глобальної конкуренції на міжнародних ІТ-ринках та зростання цінової конкуренції; - ризик скорочення обсягів зовнішніх контрактів та перегляду умов співпраці з іноземними замовниками в умовах глобальної нестабільності.

Джерело: складено автором.

Проведений SWOT-аналіз підтверджує, що фінансова безпека підприємств ІТ-сфери України формується на перетині достатньо сильного внутрішнього фінансового потенціалу та високої чутливості до зовнішніх загроз. Наявність стійкої ліквідності, прибутковості та накопиченого запасу фінансової міцності створює передумови для збереження фінансової стійкості навіть в умовах війни та економічної нестабільності. Водночас уповільнення темпів зростання інтегрального показника фінансової безпеки та зниження інвестиційної активності обмежують можливості подальшого посилення фінансової безпеки без відповідних управлінських механізмів та рішень різних рівнів.

Тому забезпечення фінансової безпеки вітчизняних підприємств ІТ-сфери в сучасних умовах потребує не фрагментарних рішень, а формування цілісного механізму, здатного забезпечити своєчасну ідентифікацію дестабілізуючих чинників, оцінювання їх впливу та розробку управлінських фінансових рішень щодо мінімізації негативних наслідків. Це обумовлює необхідність обґрунтування теоретико-методичних засад механізму забезпечення фінансової безпеки ІТ-підприємств, що буде детально розглянуто в наступному підрозділі дисертаційної роботи.

3.2. Формування механізму забезпечення фінансової безпеки підприємств ІТ-сфери

Глобалізація ринків, цифрова трансформація економіки, посилення конкуренції, воєнні ризики, валютна нестабільність та зміна моделей зайнятості формують нову конфігурацію загроз для збереження фінансової стійкості суб'єктів ІТ-бізнесу, що було детально розглянуто в підрозділі 3.1. За таких умов забезпечення фінансової безпеки дедалі більше набуває рис динамічного процесу, що потребує постійного моніторингу, аналізу та адаптації фінансових управлінських рішень до змін зовнішнього і внутрішнього середовища функціонування ІТ-підприємства.

Особливості діяльності ІТ-підприємств, зумовлюють обмеженість застосування універсальних підходів до забезпечення їхньої фінансової безпеки. Для таких підприємств характерні підвищені фінансові та кіберризики, швидка зміна умов формування грошових потоків і висока чутливість фінансових результатів до зовнішніх викликів та загроз.

Аналіз наукових праць [204; 224], присвячених проблемі забезпечення фінансової безпеки підприємств свідчить, що в сучасних дослідженнях фінансова безпека підприємств дедалі частіше розглядається з позицій гнучкості та адаптивності, що зумовлено ускладненням фінансових процесів на підприємствах і зростанням ролі зовнішніх ризиків. Так, більшість наукових підходів ґрунтується на використанні системи фінансових показників, регулярному моніторингу фінансового стану та перегляді фінансових рішень відповідно до змін середовища функціонування.

Проте зазначені підходи не враховують галузеву специфіку діяльності підприємств ІТ-сектору та їхніх проблем із забезпеченням фінансової безпеки. В умовах сьогодення ІТ-компанії стикаються з унікальними операційними й фінансовими викликами, що пов'язані з особливостями їхньої фінансово-господарської діяльності. Тому для ІТ-підприємств постає потреба подальшого розвитку наявних підходів до забезпечення фінансової безпеки в напрямку посилення їх комплексності, а також інтеграції цифрових технологій, сучасних фінансових рішень і превентивних заходів у межах єдиного механізму.

Високі темпи цифровізації розширюють можливості та інструментарій фінансового аналізу, прогнозування та контролю, що не тільки визначають нові підходи до управління фінансовими ресурсами, ризиками, капіталом та грошовими потоками суб'єктів господарювання ІТ-сфери, а і створюють передумови для переходу від реактивного реагування на фінансові загрози до превентивного забезпечення фінансової безпеки. Для ІТ-підприємств такий підхід є особливо важливим, оскільки для таких суб'єктів господарювання в разі виникнення ризиків і загроз фінансові втрати можуть бути миттєвими, що створює серйозні негативні наслідки для їхньої ліквідності, платоспроможності та безперервності діяльності.

У цьому контексті виникає необхідність формування адаптивного механізму забезпечення фінансової безпеки ІТ-підприємств, у межах якого інтегруються сучасна інформаційно-аналітична база, цифрові інструменти оцінювання та прогнозування ризиків і загроз, а також фінансові рішення превентивного характеру, спрямовані на підтримання фінансової та кіберстійкості в умовах динамічного зовнішнього середовища [86; 124].

У науковій літературі під терміном «механізм» прийнято розглядати сукупність форм, методів, підходів, прийомів, які використовуються для досягнення певної мети. Так, у «Великому тлумачному словнику сучасної української мови» поняття «механізм» визначається як внутрішня будова, система чого-небудь, сукупність станів і процесів, з яких складається певне явище...» [23].

В економічних дослідженнях поняття «механізм» здебільшого трактується як сукупність взаємопов'язаних елементів, методів і інструментів, що забезпечують реалізацію управлінських впливів і досягнення поставлених фінансово-економічних цілей [99]. Такий підхід дозволяє розглядати механізм не лише як формалізований інструментарій, а як цілісну систему впливу на фінансові процеси підприємства. Отже, у нашій роботі під терміном механізм розуміється сукупність методів, форм, інструментів та важелів, які разом із системою забезпечення використовуються для досягнення поставленої мети.

З огляду на це механізм забезпечення фінансової безпеки ІТ-підприємств у цьому дослідженні характеризується як сукупність взаємопов'язаних елементів, методів, інструментів, важелів і цифрових технологій, що реалізуються в межах відповідної системи забезпечення і спрямовані на випереджальне виявлення ризиків і загроз для підтримання фінансової стійкості, збалансованості грошових потоків та кіберстійкості ІТ-підприємств в умовах динамічного зовнішнього середовища.

Таким чином, метою механізму забезпечення фінансової безпеки ІТ-підприємств є формування умов для стійкого та безперервного функціонування таких суб'єктів господарювання шляхом комплексного

превентивного впливу на фінансові ризики і загрози, а також адаптації фінансових управлінських рішень до цифрових викликів та змін внутрішнього і зовнішнього середовища.

Ефективність реалізації зазначеного механізму зумовлена застосуванням комплексного підходу, який передбачає узгоджене використання фінансових, інформаційних і цифрових інструментів у межах системи економічної безпеки підприємства. У цьому контексті фінансова безпека виступає ключовою складовою економічної безпеки, оскільки саме фінансові ресурси, грошові потоки та фінансові результати забезпечують стабільність і відтворювальні можливості підприємства [12].

Відповідно до поставленої мети, основними завданнями механізму забезпечення фінансової безпеки ІТ-підприємства є:

- визначення ключових фінансових показників фінансової безпеки підприємств [7];
- виявлення ризиків та оцінка пов'язаних із ними можливих небезпек та загроз [7];
- здійснення контролю та оцінювання результативності функціонування системи фінансової безпеки [7];
- розробка та реалізація превентивних і захисних заходів, спрямованих на мінімізацію ризиків та недопущення фінансових втрат;
- забезпечення стабільності й безперервності грошових потоків, підтримання ліквідності та платоспроможності;
- діагностика стану кібербезпеки;
- захист фінансових, інформаційних, цифрових і нематеріальних активів;
- забезпечення інформаційно-аналітичної підтримки фінансових управлінських рішень;
- активне використання підприємствами сучасних цифрових технологій для покращення ефективності операцій та зменшення негативного впливу фінансових ризиків і загроз [257];

- моніторинг нових цифрових технологій та продуктів;
- гармонізація фінансової стратегії та політики підприємства з цифровими викликами сучасності.

Цілком логічно, що механізм забезпечення фінансової безпеки ІТ-підприємств функціонує в структурі фінансового менеджменту, а його важливою особливістю є розмежування стратегічного та оперативного рівнів фінансового впливу, що дозволяє підвищити обґрунтованість управлінських фінансових рішень і забезпечити узгодженість довгострокових і поточних цілей фінансового розвитку підприємства.

Стратегічний рівень механізму спрямований на формування відповідної фінансової стратегії ІТ-підприємства, забезпечення довгострокової фінансової стійкості та рівноваги, оптимізацію структури капіталу, диверсифікацію джерел фінансування та доходів, а також підвищення інвестиційної привабливості. У межах стратегічного рівня превентивний підхід у забезпеченні фінансової безпеки реалізується через формування фінансових резервів, політики диверсифікації, сценарне моделювання розвитку та завчасне врахування основних ризиків і загроз.

Оперативний рівень передбачає забезпечення ліквідності та платоспроможності, регулювання грошових потоків, витрат і фінансових ризиків, що виникають у процесі поточної фінансово-господарської діяльності ІТ-підприємства. Його реалізація передбачає ухвалення поточних фінансових рішень на основі актуальної інформаційно-аналітичної бази та постійного моніторингу ключових фінансових показників, що забезпечує оперативність реагування на зміну фінансових умов і ризиків.

Превентивна складова на оперативному рівні проявляється в ранньому виявленні відхилень фінансових показників, своєчасному коригуванні грошових потоків і витрат, а також у застосуванні інструментів запобігання фінансовим втратам. Для ІТ-підприємств, особливого значення в умовах цифрової економіки набуває здатність до гнучкого перерозподілу фінансових ресурсів і мінімізації ризиків у режимі, наближеному до реального часу.

Погоджуючись із думкою Назаренко Я., Теслюк Н., слід зазначити, що у процесі забезпечення фінансової безпеки важливо знаходити баланс між короткостроковими цілями, такими як підтримання ліквідності, і довгостроковими перспективами, що передбачають розвиток бізнесу. Надмірна концентрація на короткострокових вигодах може призвести до втрати стратегічних можливостей, тоді як ігнорування поточних проблем може зумовити кризові ситуації [133].

На рис. 3.8 представлено структурну модель складових механізму забезпечення фінансової безпеки ІТ-підприємств, яка дозволяє окреслити його змістовне наповнення. Запропонована схема відображає не лише структурні елементи механізму забезпечення фінансової безпеки ІТ-підприємств, а й логіку його функціонування в умовах динамічного зовнішнього середовища та цифрової трансформації.

З урахуванням специфіки діяльності ІТ-підприємств, кіберстійкість у межах механізму розглядається як невід’ємна складова фінансової безпеки, оскільки порушення цифрової інфраструктури безпосередньо впливає на безперервність діяльності, стабільність грошових потоків та фінансові результати суб’єктів ІТ-бізнесу, а не лише на інформаційну безпеку в її класичному розумінні.

Реалізація механізму забезпечення фінансової безпеки ІТ-підприємств ґрунтується на сукупності принципів, що визначають логіку його функціонування та взаємодію основних елементів:

- системності – механізм забезпечення фінансової безпеки розглядається як цілісна система взаємопов’язаних елементів, що охоплює фінансові методи, ризики, інструменти, важелі та цифрові технології. Реалізація цього принципу забезпечує узгодженість дій у межах механізму та комплексний вплив на фінансову стійкість ІТ-підприємства;

- адаптивності – своєчасне виявлення загроз, здатності суб’єкта підприємництва ефективно долати негативний вплив цих загроз, а також корегування методів та заходів із фінансової безпеки для забезпечення його стабільного розвитку [176];

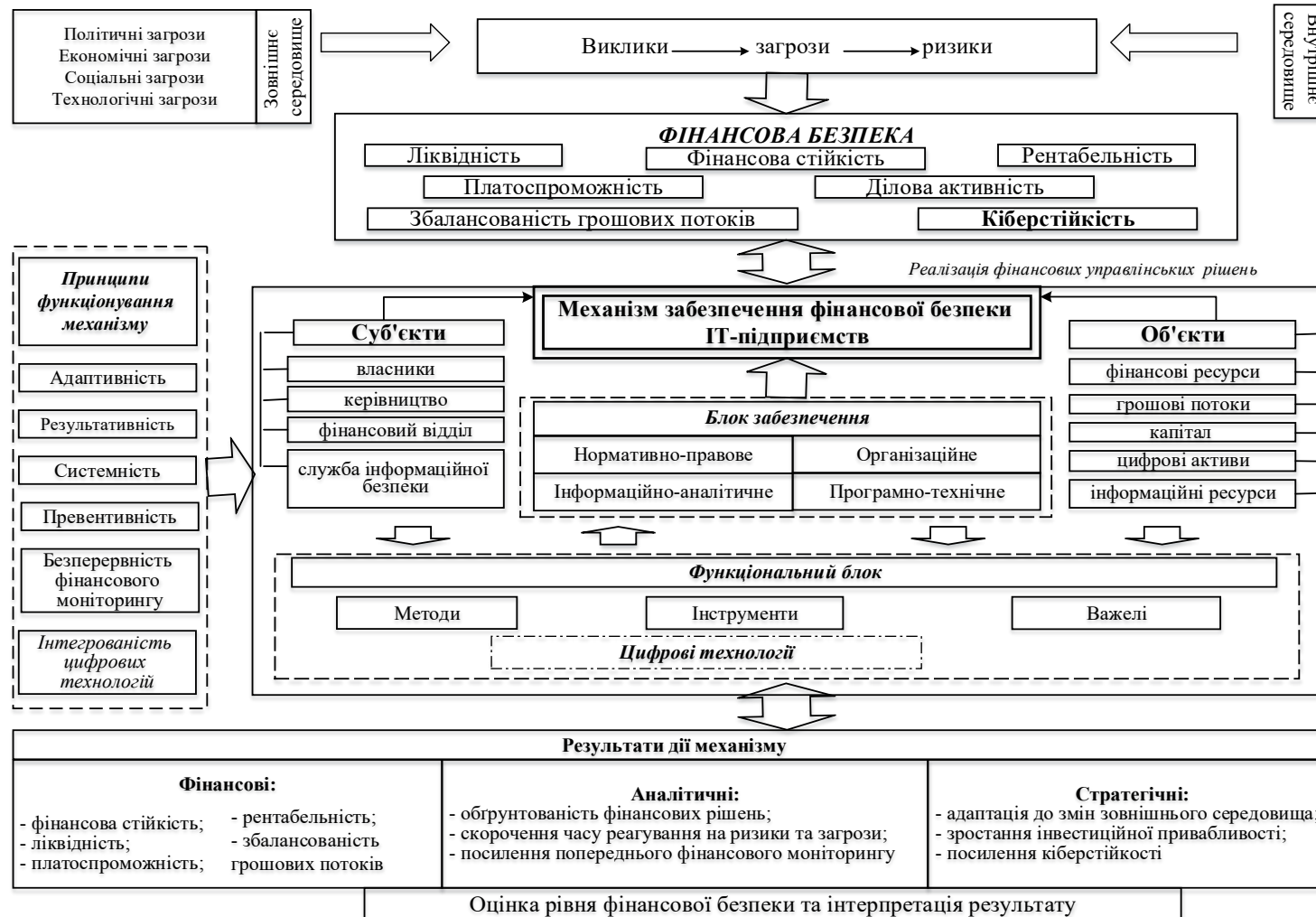


Рис. 3.8. Структурно-функціональна модель адаптивного механізму забезпечення фінансової безпеки ІТ-підприємств

Джерело: складено автором на основі [7; 91; 121; 134; 221].

- превентивності – забезпечення фінансової безпеки орієнтується не лише на реагування на існуючі загрози, а насамперед на їх раннє виявлення, прогнозування та мінімізацію;

- безперервності фінансового моніторингу – механізм передбачає постійне відстеження ключових фінансових показників, грошових потоків і ризиків, що забезпечує своєчасне ухвалення коригувальних фінансових рішень [121];

- інтегрованість цифрових технологій – цифрові технології інтегруються в усі елементи механізму фінансової безпеки та забезпечують автоматизацію аналізу, прогнозування і контролю фінансових параметрів, що сприяє підвищенню точності фінансових розрахунків і рівня кіберстійкості ІТ-підприємств;

- результативності – функціонування механізму спрямоване на досягнення цільового рівня фінансової безпеки, що проявляється у збереженні фінансової стійкості, ліквідності, платоспроможності та здатності підприємства до сталого розвитку в умовах цифрової економіки.

Зважаючи на визначені принципи функціонування механізму, доцільно окреслити його об'єкти та суб'єкти, які формують зміст фінансового впливу в межах забезпечення фінансової безпеки ІТ-підприємств. Суб'єктами виступають власники та керівництво підприємства, служба інформаційної безпеки, фінансові підрозділи, які здійснюють формування, реалізацію та коригування фінансових рішень і заходів у межах функціонування механізму забезпечення фінансової безпеки.

До об'єктів механізму забезпечення фінансової безпеки ІТ-підприємств варто віднести фінансову та управлінську інформацію, фінансові ресурси, грошові потоки, прибуток, капітал підприємства, цифрові активи, інвестиції, а також інтелектуальні ресурси. Зазначені об'єкти формують фінансову основу діяльності ІТ-підприємства та визначають рівень його фінансової стійкості, платоспроможності та здатності до розвитку в умовах цифрової економіки.

Взаємодія суб'єктів і об'єктів у межах механізму реалізується через виконання відповідних функцій, до яких доцільно віднести:

- інформаційну – формування та підтримка інформаційно-аналітичної бази системи фінансової безпеки ІТ-підприємств, у тому числі із застосуванням цифрових технологій для оцінювання, прогнозування та обґрунтування фінансових управлінських рішень;
- оцінювальну – комплексний аналіз фінансового стану та оцінку рівня фінансової безпеки ІТ-підприємства з урахуванням ризиків і загроз;
- регуляторну – коригування ключових фінансових параметрів діяльності ІТ-підприємства з метою підтримання фінансової стійкості, ліквідності та збалансованості грошових потоків [12];
- контрольну – яка реалізується у здійсненні контролю за доходами, витратами, фінансовою документацією, а також за виконанням чинних нормативно-правових актів під час фінансових операцій [176];
- організаційну – формування організаційної структури забезпечення фінансової безпеки підприємства, визначення центрів відповідальності для виконання задач та координації дій у межах механізму [134];
- прогнозну – прогнозування фінансових ризиків і загроз, оцінювання можливих фінансових наслідків їх виникнення та формування превентивних заходів забезпечення фінансової безпеки.

Основна увага при формуванні системи фінансової безпеки ІТ-підприємств приділяється забезпечувальному блоку, що включає нормативно-правове, організаційне, інформаційно-аналітичне та програмно-технічне забезпечення. Його функціонування визначає можливості ефективної реалізації методів, інструментів і важелів фінансового впливу в межах механізму забезпечення фінансової безпеки ІТ-підприємств.

Нормативно-правове забезпечення механізму охоплює сукупність зовнішніх і внутрішніх нормативних актів, що визначають умови фінансово-господарської діяльності ІТ-підприємства та формують правові межі реалізації фінансових рішень. До нього належать законодавчі та підзаконні акти, стандарти й норми, які регулюють підприємницьку діяльність, фінансові відносини, оподаткування, валютні операції, а також питання захисту

інформації та цифрових активів. У практичному вимірі нормативно-правове забезпечення визначає допустимі межі фінансових операцій ІТ-підприємства, вимоги до структури фінансової звітності, порядку здійснення валютних операцій, оподаткування експортних доходів, а також умови використання та захисту цифрових і нематеріальних активів.

Важливу роль у складі нормативно-правового забезпечення відіграють внутрішні положення та регламенти ІТ-підприємства, що стосуються фінансового планування, бюджетування, управлінського обліку, фінансового контролінгу, контролю грошових потоків і формування фінансових резервів, а також процедур реагування на ризики. Внутрішня нормативна база забезпечує захист конфіденційної фінансової інформації, визначає відповідальність за фінансові порушення та прояви шахрайства, сприяє узгодженості фінансової стратегії з вимогами зовнішнього середовища та зниженню ризиків і загроз у процесі поточної господарської діяльності.

Як зазначено в [7] розробка внутрішньої нормативно-методичної бази стає важливим аспектом для забезпечення сталої фінансової безпеки, зокрема визначення рекомендованих значень індикаторів та їхніх межових значень з урахуванням конкретного рівня безпеки. Спрямованість на створення системи оцінки рівня фінансової безпеки дозволить ефективніше контролювати фінансовий стан підприємства, розробляти адекватні ситуації на ринку підходи до адаптації моніторингу при формуванні механізму.

Організаційне забезпечення механізму визначає внутрішню організацію процесів реалізації фінансових рішень, спрямованих на забезпечення фінансової безпеки ІТ-підприємства. Воно охоплює розподіл функцій і відповідальності між власниками, керівництвом, фінансовими підрозділами та службою інформаційної безпеки, а також визначення процедур взаємодії між ними у процесі формування, реалізації та контролю фінансових рішень.

У межах організаційного забезпечення визначається порядок координації фінансового планування, бюджетування, фінансового контролінгу та управління ризиками, а також відповідальність за моніторинг рівня

фінансової безпеки та реалізацію превентивних заходів. Чітка організаційна регламентація дозволяє забезпечити своєчасне реагування на внутрішні й зовнішні ризики та мінімізувати ймовірність несистемних або несвоєчасних фінансових рішень.

Важливого значення в сучасних умовах набуває рівень цифрових компетенцій персоналу, задіяного в реалізації механізму фінансової безпеки, оскільки недостатня цифрова грамотність обмежує можливості використання фінансово-аналітичних інструментів, автоматизованих систем, що підвищує ризики ухвалення неефективних фінансових рішень.

З урахуванням специфіки ІТ-підприємств організаційне забезпечення передбачає узгодження фінансових процесів із проєктним характером їхньої діяльності, гнучкими формами зайнятості та активним використанням цифрових інструментів, що сприяє підвищенню адаптивності механізму фінансової безпеки в умовах динамічного зовнішнього середовища.

Інформаційно-аналітичне забезпечення механізму створює підґрунтя для збирання, обробки та інтерпретації інформації, необхідної для оцінювання рівня фінансової безпеки та обґрунтування фінансових управлінських рішень. Воно охоплює сукупність фінансових і нефінансових показників, аналітичних методів, інформаційних потоків і процедур, що використовуються для моніторингу фінансового стану, грошових потоків, ризиків і загроз тощо.

У межах інформаційно-аналітичного забезпечення здійснюється аналіз динаміки ключових фінансових параметрів, виявлення відхилень від цільових показників, оцінювання впливу внутрішніх і зовнішніх факторів, а також формування прогнозних і сценарних оцінок. Це створює передумови для своєчасного коригування фінансових інструментів і підвищення обґрунтованості фінансових рішень у процесі забезпечення фінансової безпеки.

Інформаційно-аналітична підсистема повинна містити якісні і кількісні параметри використання фінансових ресурсів, операційні та фінансові плани (бюджети) та формуватися на підставі даних бухгалтерського, управлінського

та статистичного обліку і звітності, а також світових, загальнодержавних та галузевих показників [176], що забезпечує формування повної, достовірної та релевантної інформаційної бази для підготовки аналітичних матеріалів, рекомендацій і фінансово-економічних висновків.

Для ІТ-підприємств ефективне інформаційно-аналітичне забезпечення сприяє переходу від реактивного до превентивного підходу в забезпеченні фінансової безпеки, а також підвищенню адаптивності механізму в умовах динамічного зовнішнього середовища.

Акумуляування значних обсягів різної інформації у процесі забезпечення фінансової безпеки зумовлює підвищені вимоги до якості її структурування, аналітичної обробки та своєчасного оновлення, що визначає тісний зв'язок інформаційно-аналітичного забезпечення з програмно-технічними засобами механізму.

Отже, *програмно-технічне забезпечення* механізму створює технічні та технологічні передумови для реалізації інформаційно-аналітичних процедур у процесі забезпечення фінансової безпеки ІТ-підприємства. Воно охоплює сукупність програмних продуктів, інформаційних систем, цифрових платформ і технічних засобів, що забезпечують автоматизацію збору, обробки, зберігання та передачі фінансової інформації.

У межах програмно-технічного забезпечення реалізується підтримка фінансового обліку, бюджетування, контролю грошових потоків, аналізу фінансових показників і ризиків, а також інтеграція даних з різних інформаційних джерел. Це дозволяє підвищити оперативність фінансового аналізу, зменшити інформаційні асиметрії та забезпечити безперервність аналітичного супроводу фінансових рішень.

Для ІТ-підприємств програмно-технічне забезпечення має особливе значення з огляду на цифрову природу бізнесу, високу залежність від інформаційних систем та ризики втрати або викривлення фінансових даних. Надійність, захищеність і безперервність функціонування програмно-

технічної інфраструктури безпосередньо впливають на фінансову стійкість, стабільність грошових потоків, а особливо на рівень кіберстійкості підприємства, що робить цей елемент важливою складовою забезпечувального блоку механізму фінансової безпеки підприємств ІТ-сфери.

Таким чином, нормативно-правове й організаційне забезпечення створюють інституційну основу механізму фінансової безпеки ІТ-підприємств, тоді як інформаційно-аналітичне та програмно-технічне забезпечення формують його динамічну складову, що забезпечує адаптивність, превентивний характер управління та оперативне реагування на фінансові ризики й загрози в умовах цифрової економіки.

Сукупна дія зазначених складових забезпечувального блоку створює інтегроване середовище реалізації механізму фінансової безпеки ІТ-підприємств, у межах якого фінансові рішення формуються на основі своєчасної, достовірної та аналітично опрацьованої інформації з урахуванням цифрових ризиків і викликів.

У дослідженнях методичний апарат забезпечення фінансової безпеки трактується неоднозначно, що зумовлено різними рівнями аналізу, цілями дослідження та галузевою специфікою. У межах цього дослідження в основу структуризації методів, інструментів і важелів покладено функціонально-процесний підхід, відповідно до якого будується механізм забезпечення фінансової безпеки ІТ-підприємств. Згідно з цим підходом методи згруповано залежно від їх ролі в оцінюванні та регулюванні рівня фінансової безпеки, а також превентивному реагуванні на ризики і загрози. Інструменти в межах механізму застосовуються для практичної реалізації відповідних фінансових рішень, тоді як важелі - для здійснення цілеспрямованого фінансового впливу на ключові параметри діяльності суб'єктів господарювання ІТ-сфери (табл. 3.2).

**Методи, інструменти та важелі реалізації механізму забезпечення
фінансової безпеки підприємств ІТ-сфери**

1. Методи забезпечення фінансової безпеки ІТ-підприємств		
Категорія методів	Методи	Призначення
Методи діагностики та фінансового аналізу	горизонтальний та вертикальний аналіз, коефіцієнтний аналіз, порівняльний аналіз, факторний аналіз, індикаторний метод; інтегральний метод; ідентифікація ризиків і загроз; методи прогнозування банкрутства; експертно-аналітичні методи	Оцінка фінансового стану ІТ-підприємства, визначення рівня фінансової безпеки, ідентифікація ризиків і загроз, формування аналітичної бази.
Методи фінансового регулювання та стабілізації	фінансове планування і бюджетування; методи управління грошовими потоками; інвестування та кредитування; методи управління структурою джерел фінансування; методи управління витратами; страхування ризиків	Забезпечення фінансової стійкості, ліквідності, платоспроможності та досягнення цільового рівня фінансової безпеки
Методи адаптації та превентивного реагування	фінансове прогнозування; трендовий аналіз; економіко-статистичні методи; сценарне моделювання; стрес-тестування; постійний фінансовий моніторинг; оперативне коригування фінансових параметрів	Підвищення адаптивності механізму забезпечення фінансової безпеки та формування системи превентивного реагування на фінансові ризики і загрози.
2. Інструменти забезпечення фінансової безпеки ІТ-підприємств		
Категорія інструментів	Інструменти	Призначення
Аналітичні інструменти	система фінансових показників і KPI; інтегральні індекси фінансової безпеки; управлінська, фінансова звітність; фінансові аналітичні дашборди	Забезпечення оцінки та моніторингу рівня фінансової безпеки
Планово-регулятивні інструменти	фінансові плани та бюджети; cash-flow-плани; фінансові ліміти; резервні фонди; сценарні бюджети	Реалізація фінансових управлінських рішень і регулювання грошових потоків
Ризикорієнтовані інструменти	ризик-карти; стрес-тестування; сценарний аналіз; страхування фінансових ризиків; хеджування валютних ризиків	Мінімізація впливу ризиків і загроз
Цифрові фінансові інструменти	ERP-системи; BI-системи; автоматизовані системи бюджетування і фінансового контролю; цифрові платформи фінансового аналізу тощо	Автоматизація, підвищення оперативності та точності фінансових розрахунків
Інструменти кіберзахисту фінансових даних	системи захисту інформації; контроль доступу; резервне копіювання; моніторинг кіберзагроз	Забезпечення цілісності та конфіденційності фінансових даних

1	2	3
3. Важелі фінансового впливу		
Фінансово-економічні	податки та податкові пільги; кредити; відсоткові ставки за кредитами; дивідендна політика, пільгові кредити; курси валют; інвестиції	Регулювання фінансових результатів і структури капіталу
Стимулюючі	оплата праці; система бонусів; премії; участь у прибутку	Стимулювання ефективного використання фінансових і інтелектуальних ресурсів
Обмежувальні	штрафні санкції; фінансові обмеження; ліміти витрат	Зменшення фінансових ризиків і перевитрат
Інституційні	законодавча база, норми, державні пільги; гранти; субсидії; програми підтримки ІТ-сектору, гарантії інвесторам, податкові стимули для інноваційної діяльності	Підвищення фінансової стійкості в умовах нестабільності

Джерело: систематизовано автором на основі [7; 66; 121; 134; 176; 225].

До методів реалізації механізму забезпечення фінансової безпеки ІТ-підприємств належить сукупність фінансово-аналітичних, регулятивних та адаптивних методів, застосування яких спрямоване не лише на оцінювання фінансового стану і рівня фінансової безпеки, а й на підтримання та коригування ключових фінансових параметрів діяльності підприємства в умовах цифрової економіки.

Так, методи діагностики та фінансового аналізу формують аналітичну основу механізму й застосовуються для оцінювання фінансового стану ІТ-підприємств, визначення рівня їхньої фінансової безпеки та ідентифікації внутрішніх і зовнішніх ризиків і загроз. До цієї групи належать як традиційні методи фінансового аналізу, так і методи визначення рівня фінансової безпеки (індикаторні, інтегральні, ризикоорієнтовані та ін.) [66].

Методи фінансового регулювання спрямовані на підтримання належного рівня фінансової безпеки, стійкості, ліквідності та платоспроможності ІТ-підприємств шляхом впливу на грошові потоки, витрати, структуру капіталу, джерела фінансування тощо [66].

Застосування методів адаптації та превентивного реагування забезпечує гнучкість і динамічність механізму фінансової безпеки в умовах мінливого зовнішнього середовища й високої невизначеності та дозволяє своєчасно

реагувати на зміну умов функціонування ІТ-підприємств [66]. Прогнозування, сценарне моделювання, стрес-тестування і постійний фінансовий моніторинг дозволяють завчасно виявляти потенційні загрози та коригувати фінансові рішення до моменту настання негативних впливів.

Таким чином, комплексне використання методів діагностики, фінансового регулювання та адаптації дозволяє розглядати фінансову безпеку ІТ-підприємств не лише як результат оцінювання фінансового стану, а як об'єкт безперервного фінансового впливу в межах механізму забезпечення фінансової безпеки.

Інструменти забезпечення фінансової безпеки ІТ-підприємств являють собою сукупність фінансових інструментів і цифрових засобів, за допомогою яких здійснюється практичне впровадження методів оцінювання, прогнозування та коригування ключових фінансових параметрів діяльності. Саме система інструментів забезпечує практичну реалізацію результатів фінансового аналізу у вигляді конкретних фінансових рішень і заходів у межах механізму забезпечення фінансової безпеки ІТ-підприємств [66].

У межах нашого дослідження інструменти забезпечення фінансової безпеки структуровано за функціональним призначенням на аналітичні, планово-регулятивні, ризик-орієнтовані та цифрові. Така структуризація дозволяє узгодити їх із відповідними групами методів, що забезпечує цілісність і прикладну спрямованість механізму, а також дозволяє врахувати специфіку цифрової діяльності й підвищені кіберризики, притаманні ІТ-сфері [66].

Важелі фінансового впливу в механізмі забезпечення фінансової безпеки ІТ-підприємств виконують функцію безпосереднього впливу на фінансові результати, структуру капіталу, витрати, грошові потоки тощо. На відміну від методів і інструментів, які формують аналітичну та інструментальну основу механізму й забезпечують реалізацію фінансових рішень, фінансові важелі визначають характер і силу впливу на фінансові умови функціонування підприємства через зміну параметрів формування та використання фінансових ресурсів [66].

Застосування фінансово-економічних, стимулюючих, обмежувальних та інституційних важелів дозволяє коригувати рівень фінансових ризиків, стимулювати ефективне використання фінансових та інтелектуальних ресурсів, а також обмежувати негативні фінансові наслідки в умовах нестабільності зовнішнього середовища. У межах механізму фінансової безпеки важелі не мають самостійного характеру, а реалізуються у взаємозв'язку з відповідними методами та інструментами, що забезпечує узгодженість і цілісність фінансового впливу [66; 149].

Для ІТ-підприємств особливе значення має поєднання стимулюючих та обмежувальних фінансових важелів із інституційними механізмами державної підтримки інноваційної діяльності, цифровізації та розвитку людського капіталу. Застосування таких важелів сприяє реалізації превентивного характеру механізму забезпечення фінансової безпеки, підвищенню фінансової стійкості та збереженню конкурентоспроможності ІТ-підприємств у довгостроковій перспективі.

Цифрові технології в межах функціонального блоку механізму забезпечення фінансової безпеки ІТ-підприємств не розглядаються як окремий фінансовий інструмент, а виступають наскрізним елементом, що забезпечує сучасну форму реалізації методів оцінювання, інструментів фінансового регулювання та важелів фінансового впливу в умовах цифровізації (рис. 3.9). Саме цифрові інструменти та технології створюють техніко-аналітичне підґрунтя для автоматизації фінансових розрахунків, безперервного моніторингу ключових фінансових параметрів, підвищити оперативності аналізу та обґрунтованості фінансових рішень, що є особливо важливим в умовах високої динаміки діяльності ІТ-підприємств [66].

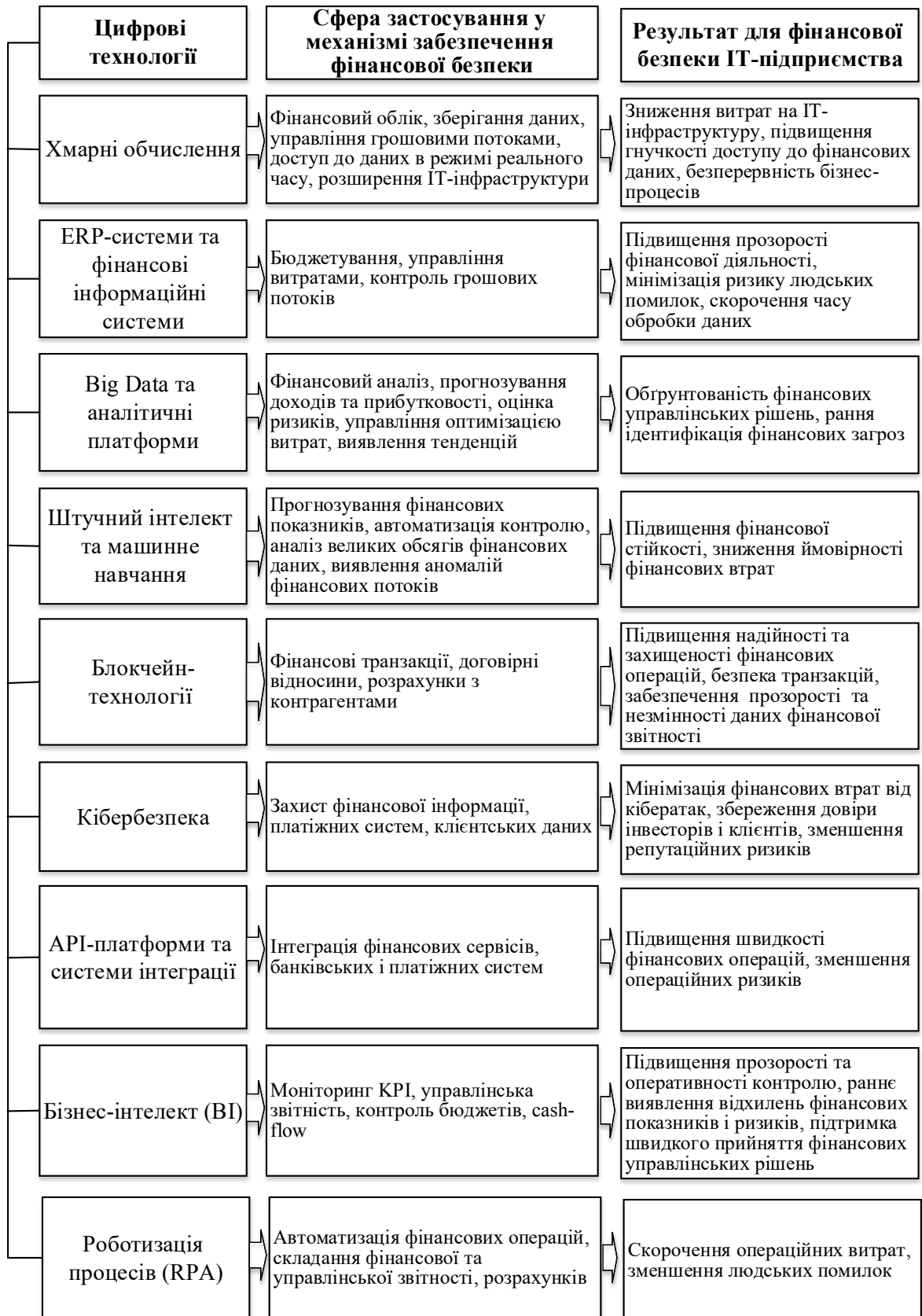


Рис. 3.9. Цифрові технології у механізмі забезпечення фінансової безпеки ІТ-підприємств

Джерело: складено автором на основі [38; 73; 210; 249; 257].

У запропонованому механізмі цифрові технології інтегруються до функціонального блоку, оскільки забезпечують практичну реалізацію методів, інструментів і важелів управління фінансовою безпекою ІТ-підприємств. Такий підхід дозволяє розглядати цифрові технології не як допоміжний елемент, а як органічну складову процесу управління фінансовими ризиками та ресурсами, що відповідає цифровій природі ІТ-бізнесу. На відміну від підприємств традиційних галузей, для яких цифровізація виступає здебільшого засобом підвищення ефективності окремих бізнес-процесів, для ІТ-компаній вона є базовою умовою ведення діяльності та ключовим фактором фінансової стійкості.

Використання цифрових технологій створює передумови для переходу від реактивного реагування на фінансові загрози до превентивного управління фінансовою безпекою, коли управлінські рішення ухвалюються не після виникнення фінансових загроз, а на основі їх ранньої ідентифікації та прогнозування. Автоматизація фінансових процесів, інтеграція фінансових і операційних систем, застосування аналітичних платформ для моніторингу дозволяють підвищити прозорість грошових потоків, зменшити вплив людського фактору, своєчасно виявляти ризики та скоротити часовий лаг між виникненням загрози і прийняттям управлінського рішення [257].

Окремого значення для ІТ-підприємств набуває застосування інструментів фінансової аналітики, прогнозного моделювання та штучного інтелекту. Використання алгоритмів обробки великих масивів фінансових і операційних даних створює можливості для моделювання сценаріїв розвитку, виявлення тенденцій фінансового стану, оцінки ймовірності настання ризиків, прогнозування доходів, виявлення сигналів фінансової нестабільності тощо. Застосування Big Data також допомагає фінансовим аналітикам виявляти тенденції, прогнозувати рентабельність проєктів та оптимізувати управління витратами [73].

У межах механізму забезпечення фінансової безпеки це дозволяє не лише оцінювати поточний рівень фінансової безпеки, а й формувати адаптивні управлінські рішення з урахуванням змін зовнішнього та внутрішнього середовища.

Важливим напрямом цифрового забезпечення фінансової безпеки ІТ-підприємств є інтеграція фінансових, управлінських та операційних систем на основі платформних рішень, ERP-систем, API-інтерфейсів і хмарних технологій. Така інтеграція забезпечує узгодженість фінансових рішень із проєктною діяльністю, кадровою політикою та стратегічними цілями розвитку ІТ-підприємства, що сприяє збереженню фінансової стійкості підприємства в процесі масштабування бізнесу та диверсифікації джерел доходів [66].

Особливе місце в механізмі забезпечення фінансової безпеки ІТ-підприємств посідає кібербезпека фінансових даних та цифрової інфраструктури. Висока залежності ІТ-компаній від цифрових платформ, хмарних сервісів і електронних платіжних систем зумовлює тісний взаємозв'язок фінансової та інформаційної безпеки. Порушення цілісності або конфіденційності фінансових даних, збої в роботі цифрових систем чи кібератаки можуть призвести не лише до прямих фінансових втрат, а й до зниження довіри клієнтів і контрагентів (репутаційних ризиків), що безпосередньо впливає на рівень фінансової безпеки підприємства [66].

Узагальнені на рис. 3.9 цифрові технології охоплюють ключові сфери фінансової діяльності ІТ-підприємств – від управління грошовими потоками та бюджетування до контролю ризиків, автоматизації операцій і захисту фінансової інформації. Їх застосування сприяє оптимізації витрат, підвищенню точності фінансових розрахунків, забезпечує своєчасну ідентифікацію фінансових загроз, зниження рівня транзакційних та операційних ризиків, а також підтримання безперервності бізнес-процесів в умовах нестабільного зовнішнього середовища [66].

Таким чином, цифрові інструменти виступають важливим елементом механізму забезпечення фінансової безпеки ІТ-підприємств, забезпечуючи його адаптивність, превентивний характер та інтеграцію з бізнес-процесами. Їх використання створює підґрунтя для підвищення фінансової стійкості та ефективності функціонування ІТ-підприємств в умовах цифрової економіки.

Окреме місце в механізмі забезпечення фінансової безпеки ІТ-підприємств посідає кіберстійкість, яка в умовах цифрової економіки виходить за межі суто інформаційної безпеки та безпосередньо впливає на фінансову стабільність суб'єктів господарювання ІТ-сфери. Для ІТ-підприємств порушення функціонування цифрової інфраструктури, витік або блокування фінансових даних, кібератаки на платіжні, облікові та інші системи можуть призводити до миттєвих фінансових втрат, збоїв у русі грошових потоків та репутаційних ризиків [147].

У межах запропонованого механізму кіберстійкість розглядається як складова фінансової безпеки, оскільки вона забезпечує безперервність операційної діяльності та фінансових процесів, збереження цілісності інформації та стабільність реалізації фінансових рішень. Високий рівень кіберстійкості створює передумови для підтримання ліквідності, платоспроможності й фінансової стійкості ІТ-підприємств, тоді як її зниження трансформується у фінансові ризики та загрози.

Подальше дослідження в роботі спрямоване на розкриття процесної моделі функціонування механізму забезпечення фінансової безпеки ІТ-підприємств, яка відображає логіку послідовної реалізації його елементів, взаємозв'язок фінансового стану, рівня фінансової безпеки та фінансових управлінських рішень (рис. 3.10).

Процес забезпечення фінансової безпеки починається з формування інформаційно-аналітичної та цифрової бази, яка акумулює дані внутрішнього та зовнішнього середовища діяльності ІТ-підприємства. На цій основі здійснюється ідентифікація фінансових ризиків і загроз, зумовлених як внутрішніми фінансовими дисбалансами, так і зовнішніми економічними, ринковими та цифровими викликами.

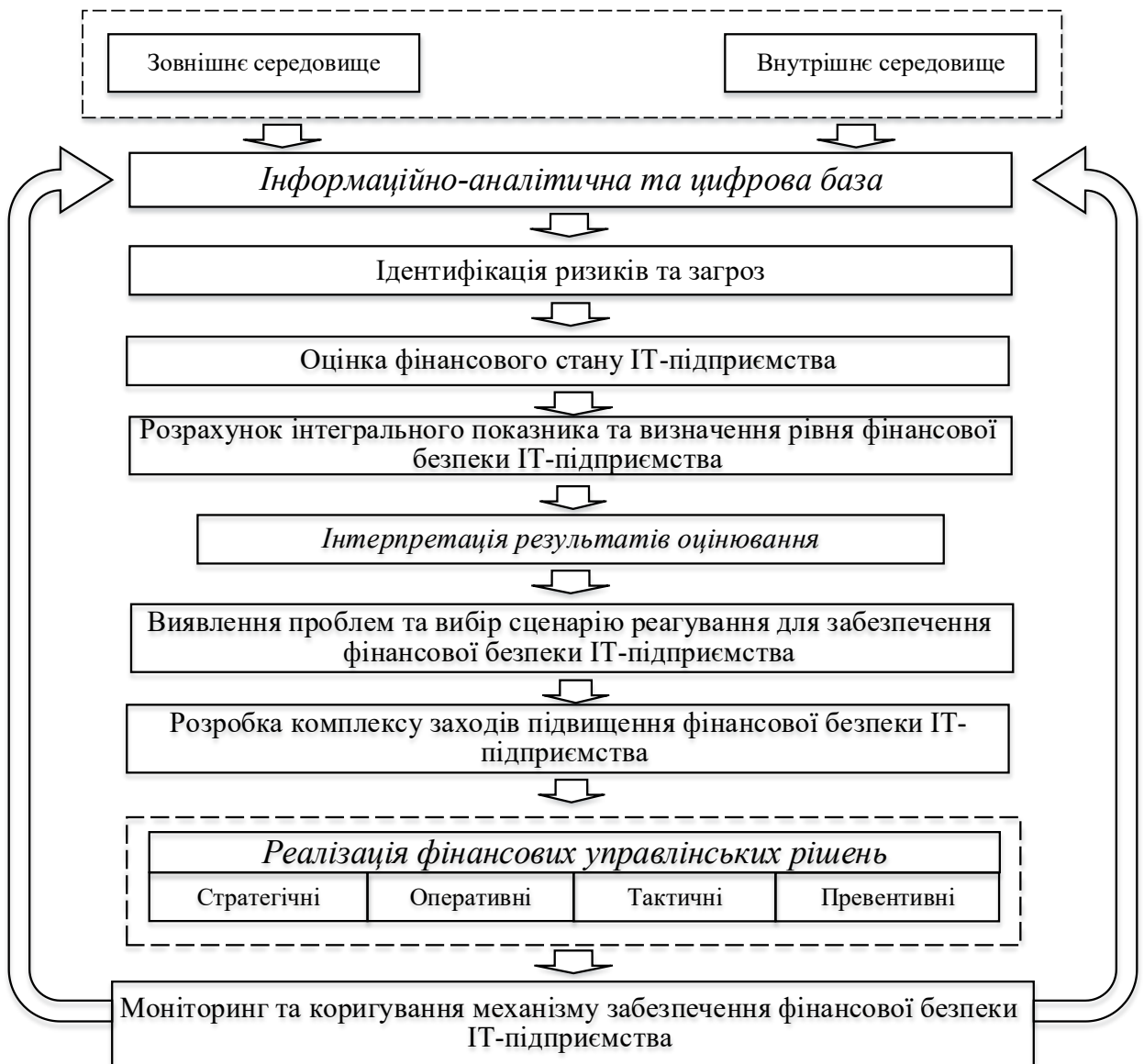


Рис. 3.10. Процес реалізації механізму забезпечення фінансової безпеки ІТ-підприємств

Джерело: складено автором на основі [12; 98; 134].

Наступним етапом є оцінювання фінансового стану ІТ-підприємства, що дозволяє визначити показники ліквідності, платоспроможності, фінансової стійкості, рентабельності та збалансованості грошових потоків. Узагальнення результатів фінансового аналізу та оцінювання ризиків забезпечує визначення рівня фінансової безпеки ІТ-підприємства, який відображає ступінь його захищеності від внутрішніх і зовнішніх загроз.

Важливим елементом процесної моделі є інтерпретація отриманих результатів, у межах якої оцінка рівня фінансової безпеки трансформується у фінансово-аналітичні висновки та управлінські рішення. Саме на цьому етапі формується підґрунтя для розробки заходів підвищення фінансової безпеки ІТ-підприємства з урахуванням виявлених ризиків, фінансових нормативів і стратегічних цілей розвитку.

Реалізація запропонованих заходів здійснюється через систему фінансових управлінських рішень, які в межах моделі диференційовано за стратегічним, оперативним, тактичним та превентивним рівнями. Такий підхід дозволяє поєднати довгострокові орієнтири фінансового розвитку з поточними завданнями забезпечення ліквідності, фінансової стійкості та контролю ризиків.

Завершальним етапом є моніторинг і коригування системи фінансової безпеки ІТ-підприємства, що забезпечує замкнений контур зворотного зв'язку. У межах цього контуру результати реалізації фінансових рішень постійно зіставляються з цільовими параметрами фінансової безпеки, а виявлені відхилення стають підставою для коригування інструментів, методів і заходів механізму.

Реалізація механізму забезпечення фінансової безпеки ІТ-підприємств забезпечує комплексний і цілеспрямований вплив на ключові фінансові параметри діяльності, що проявляється в підвищенні фінансової стійкості, підтриманні ліквідності та платоспроможності, а також у збалансованості та прогнозованості грошових потоків. Узгоджене застосування методів, інструментів і важелів у межах механізму сприяє зниженню рівня фінансових ризиків, своєчасному виявленню загроз та посиленню не тільки кіберстійкості фінансових процесів, а й кіберстійкості ІТ-підприємств загалом.

Важливим результатом дії механізму є підвищення адаптивності фінансової системи підприємства до змін зовнішнього та внутрішнього середовища, що забезпечує можливість оперативного коригування фінансових параметрів і підтримання безперервності діяльності в умовах нестабільності. Формування інтегрованої інформаційно-аналітичної та цифрової бази створює

передумови для системного оцінювання рівня фінансової безпеки та інтерпретації отриманих результатів у динаміці, що дозволяє розглядати фінансову безпеку ІТ-підприємств не як статичний показник, а як об'єкт безперервного фінансового впливу.

Результати функціонування механізму забезпечення фінансової безпеки ІТ-підприємств доцільно систематизувати таким чином. Фінансові результати полягають у:

- досягненні та підтриманні цільового рівня фінансової безпеки ІТ-підприємства;
- підвищенні фінансової стійкості, рентабельності, ліквідності та платоспроможності;
- забезпеченні збалансованості та прогнозованості грошових потоків;
- зниженні ймовірності фінансових втрат унаслідок настання фінансових і кіберризиків.

Аналітичні результати проявляються у підвищенні обґрунтованості фінансових рішень на основі інтегрованої інформаційно-аналітичної та цифрової бази; скороченні часових лагів між виникненням ризиків і реагуванням на них; посиленні превентивного характеру фінансового впливу на ризики і загрози.

До стратегічних результатів варто віднести:

- підвищення здатності ІТ-підприємства адаптуватися до змін цифрового, ринкового та інституційного середовища;
- узгодження короткострокових фінансових рішень із довгостроковими цілями фінансового розвитку;
- зростанні інвестиційної привабливості та довіри з боку стейкхолдерів;
- посиленні кіберстійкості як складової фінансової безпеки та забезпечення безперервності бізнес-процесів.

На рівні підприємства система заходів підвищення фінансової безпеки має бути спрямована не лише на поточну стабілізацію фінансового стану, а й на зниження вразливості до ризиків і загроз, підвищення адаптивності до змін умов функціонування та здатності до раннього реагування на виклики зовнішнього і внутрішнього середовища.

З огляду на специфіку діяльності ІТ-підприємств, заходи підвищення їхньої фінансової безпеки доцільно систематизувати за ключовими напрямками та сферами фінансового управління. Такий підхід дозволяє структурувати дії фінансового менеджменту та підвищити керованість фінансових процесів, тим самим підвищуючи результативність механізму забезпечення фінансової безпеки підприємств ІТ-сфери загалом.

Систематизація заходів має формуватися з урахуванням концептуальних особливостей функціонування ІТ-підприємств, що було розкрито в теоретичному розділі дисертації. Проєктний характер діяльності, домінування нематеріальних активів, висока залежність фінансових результатів від людського капіталу, нестабільність грошових потоків та експортна орієнтація вітчизняного ІТ-бізнесу потребують розробки відповідних завдань та впровадження фінансових рішень у площині фінансового планування, бюджетування, контролінгу, цифровізації фінансових процесів, кіберзахисту та управління ризиками, що виступає прикладним продовженням концептуальної моделі фінансового управління розвитком ІТ-підприємств.

У межах нашого дослідження, з урахуванням зазначених особливостей, виділено п'ять взаємопов'язаних груп заходів підвищення фінансової безпеки ІТ-підприємств мікрорівня: стратегічні, операційні, організаційні, інноваційно-технологічні та ризикорієнтовані (табл. 3.3).

Кожна група заходів має відповідну функціональну спрямованість і очікуваний ефект: від зміцнення фінансової незалежності та підвищення керованості фінансових процесів, до синхронізації грошових потоків та підвищення точності й надійності інформаційно-аналітичного забезпечення для прийняття фінансових рішень. Саме реалізація цих заходів дозволяє трансформувати теоретичні базис, у практичний інструментарій фінансового управління, спрямований на зниження ризиків, запобігання загрозам та зміцнення фінансової стійкості ІТ-підприємств.

Систематизація заходів підвищення фінансової безпеки

ІТ-підприємств на мікрорівні

Група заходів	Зміст заходів	Очікуваний ефект
1	2	3
Стратегічні	<ul style="list-style-type: none"> - формування довгострокової фінансової стратегії ІТ-підприємства; - оптимізація структури капіталу та джерел фінансування (власний капітал, гранти, венчурне фінансування, міжнародні програми); - управління вартістю бізнесу та рентабельністю проєктів; - формування фінансових та страхових резервів; - диверсифікація валютної виручки та ринків збуту; - управління інвестиційним портфелем проєктів та R&D. 	<ul style="list-style-type: none"> - зміцнення довгострокової фінансової стійкості; - підвищення фінансової автономії; - підвищення інвестиційної привабливості; - зменшення залежності від окремих замовників та покупців і валютної виручки.
Операційні	<ul style="list-style-type: none"> - оперативне планування грошових потоків з урахуванням проєктного циклу; - підтримка оптимального рівня ліквідності та платоспроможності; - використання інструментів хеджування валютних ризиків; - впровадження систем бюджетування та проєктно-орієнтованого фінансового планування; - посилення внутрішнього фінансового контролінгу; - оптимізація витрат та управління маржинальністю проєктів; - контроль дебіторської заборгованості та оцінка платоспроможності клієнтів. 	<ul style="list-style-type: none"> - підвищення платоспроможності; - підтримання цільових параметрів ліквідності та фінансової стійкості; - зниження операційних витрат; - стабілізація та збалансованість грошових потоків.
Організаційні	<ul style="list-style-type: none"> - інтеграція функції забезпечення фінансової безпеки в систему фінансового менеджменту; - впровадження внутрішніх положень щодо оцінки та забезпечення фінансової безпеки; - внутрішня регламентація процесів фінансового планування та бюджетування; - чітке розмежування фінансової відповідальності за проєктами; - розробка процедур реагування на фінансові відхилення; - посилення внутрішнього фінансового контролінгу. 	<ul style="list-style-type: none"> - підвищення якості фінансового менеджменту; - підвищення керованості фінансових процесів; - зміцнення фінансової дисципліни.

1	2	3
Ризикорієнтовані	<ul style="list-style-type: none"> - ідентифікація загроз та ризиків, оцінка їх впливу на інтегральний показник фінансової безпеки; - розробка карти ризиків; - розробка сценаріїв реагування на ризики залежно від зони фінансової безпеки; - проведення сценарного моделювання; - розробка альтернативних планів дій залежно від зміни фінансового стану. 	<ul style="list-style-type: none"> - зниження чутливості до зовнішніх загроз; - нейтралізація внутрішніх ризиків; - своєчасне коригування фінансової політики; - мінімізація потенційних фінансових втрат; - забезпечення стабільної траєкторії розвитку.
Інноваційно-технологічні	<ul style="list-style-type: none"> - автоматизація фінансового планування та бюджетування; - використання систем бізнес-аналітики (BI) для моніторингу фінансових показників та фінансової діагностики; - автоматизація фінансового обліку та управлінської звітності; - інтеграція фінансових систем через API; - цифровий захист фінансових даних та кібербезпека фінансової системи підприємства. 	<ul style="list-style-type: none"> - оперативність прийняття фінансових рішень; - зниження кіберризиків, помилок та втрат; - підвищення якості фінансового аналізу, бюджетування та точності прогнозування; - підвищення прозорості фінансових операцій.

Джерело: систематизовано автором на основі [12; 23; 99; 149].

Особливе значення в запропонованій систематизації має попереджувальний характер впроваджуваних заходів. Тобто система фінансової безпеки ІТ-підприємства розглядається не лише як механізм реагування на вже наявні загрози, а передусім як система раннього виявлення ризиків, прогнозування потенційних кризових ситуацій і недопущення переходу підприємства до критичної зони фінансової безпеки. Саме тому ризикоорієнтовані та інноваційно-технологічні заходи повинні бути інтегровані у стратегічний та операційний рівні управління, формуючи цілісну адаптивну модель забезпечення фінансової безпеки ІТ-компаній.

Метою впровадження та реалізації стратегічних заходів є формування стійкої фінансової архітектури ІТ-підприємства. Насамперед йдеться про формування довгострокової фінансової стійкості: диверсифікацію джерел доходів, зниження валютної залежності, залучення інвестиційних ресурсів для розвитку, формування фінансових резервів і забезпечення достатнього рівня

фінансової автономії. Реалізація таких заходів дозволяє підтримувати підприємство у високій зоні фінансової безпеки, зменшує чутливість до макроекономічних коливань і підвищує його інвестиційну привабливість у середньо- та довгостроковій перспективі.

Відповідно операційні заходи впроваджуються в межах поточних фінансових процесів. Управління ліквідністю, платоспроможністю, дебіторською і кредиторською заборгованістю, структурою витрат і рентабельністю проєктів формує основу короткострокової фінансової стійкості IT-підприємства. Саме на цьому рівні здійснюється мінімізація поточних фінансових втрат і оперативне реагування на відхилення у фінансових процесах та показниках, що дозволяє не допустити їх трансформацію в більш серйозні фінансові проблеми у майбутньому.

Організаційні заходи спрямовані на забезпечення внутрішньої узгодженості системи фінансової безпеки підприємства. Чіткий розподіл відповідальності, інтеграція функції забезпечення фінансової безпеки в систему фінансового менеджменту, координація роботи структурних підрозділів, регламентація процедур контролю та реагування на фінансові ризики й загрози сприяють підвищенню прозорості фінансових процесів і зміцненню фінансової дисципліни. У результаті забезпечення фінансової безпеки перестає бути окремою функцією та перетворюється на невід'ємний елемент системи фінансового менеджменту підприємства.

Ризикоорієнтований блок передбачає ідентифікацію, оцінювання, мінімізацію та моделювання фінансових ризиків і загроз з урахуванням специфіки IT-сектора [147]. Сценарний аналіз, стрес-тестування, оцінка чутливості фінансових показників до дестабілізаційних факторів дозволяють своєчасно коригувати фінансову політику залежно від зміни внутрішнього чи зовнішнього середовища, та запобігати різкому погіршенню фінансового стану, що забезпечує впровадження проактивного підходу до управління фінансовими ризиками IT-компаній.

Інноваційно-технологічні заходи спрямовані на підвищення якості інформаційно-аналітичного забезпечення фінансового менеджменту ІТ-підприємства. Використання систем бізнес-аналітики, інтеграція фінансових платформ через API, автоматизація бюджетування та облікових процесів, впровадження цифрових інструментів контролю і кіберзахисту фінансових даних підвищують точність прогнозування, оперативність прийняття рішень, а також знижують інформаційні ризики та кіберзагрози у фінансовій сфері. Застосування таких цифрових інструментів підсилює реалізацію стратегічних, операційних і ризикоорієнтованих заходів фінансового менеджменту, підвищуючи ефективність забезпечення фінансової безпеки ІТ-підприємств.

На нашу думку, при формуванні рекомендацій щодо підвищення фінансової стійкості підприємств заходи також необхідно диференціювати залежно від фінансового стану суб'єкта господарювання та рівня наявних загроз, що забезпечить більшу результативність системи фінансового управління.

З огляду на це застосування запропонованих заходів доцільно здійснювати з урахуванням фактичного значення інтегрального показника фінансової безпеки ІТ-підприємства, який виступає узагальнюючим індикатором рівня його фінансової стійкості та вразливості до ризиків. Перехід підприємства між відповідними зонами фінансової безпеки зумовлює зміну пріоритетів, інтенсивності та глибини управлінського впливу. Таким чином, підхід до забезпечення фінансової безпеки має бути диференційованим, коли рішення фінансового менеджменту ґрунтуються не на універсальних рекомендаціях, а на реальному фінансовому стані ІТ-підприємства.

Водночас інтегральний показник фінансової безпеки набуває не лише діагностичного, а й прогностичного значення. Його використання дозволяє не просто оцінити поточну позицію підприємства в межах відповідної зони, а й прогнозувати можливу зміну рівня фінансової безпеки під впливом макроекономічних, регуляторних, ринкових чи інших чинників.

За таких умов адаптивний механізм забезпечення фінансової безпеки доцільно доповнити сценарним моделюванням, яке дає змогу пов'язати результати оцінювання з практичними заходами підвищення фінансової безпеки. При цьому сценарний підхід дає змогу передбачити можливий перехід підприємства між зонами фінансової безпеки - від стабільної до критичної, розробити відповідні заходи підвищення фінансової безпеки та завчасно скоригувати фінансову політику з урахуванням очікуваних ризиків.

З огляду на це, у межах дослідження вважаємо доцільним виокремлення трьох базових сценаріїв забезпечення фінансової безпеки ІТ-підприємств, сформованих відповідно до значень інтегрального показника та позиції підприємства у відповідній зоні фінансової безпеки: сценарій раннього реагування, стабілізаційний та антикризовий (рис. 3.11). Кожен із них передбачає впровадження та реалізацію певного набору стратегічних, операційних, організаційних, ризикоорієнтованих і інноваційно-технологічних заходів.

Сценарій раннього реагування реалізується, коли ІТ-підприємство має високий інтегральний показник фінансової безпеки, що свідчить про достатній рівень фінансової стійкості, збалансованість грошових потоків та наявність фінансового потенціалу для подальшого розвитку. Для українських ІТ-підприємств така ситуація характерна за умов високого попиту на ІТ-продукцію, стабільної динаміки експортної виручки, зростання рентабельності проєктів та ефективного управління витратами.

Пріоритетом цих заходів є своєчасне попередження проблем та зміцнення досягнутого рівня фінансової безпеки. У межах сценарію раннього реагування заходи орієнтовані на підвищення якості фінансового менеджменту, розширення фінансових можливостей підприємства та формування довгострокової фінансової стійкості шляхом:

- залучення інвестиційних ресурсів для розвитку та розширення діяльності;

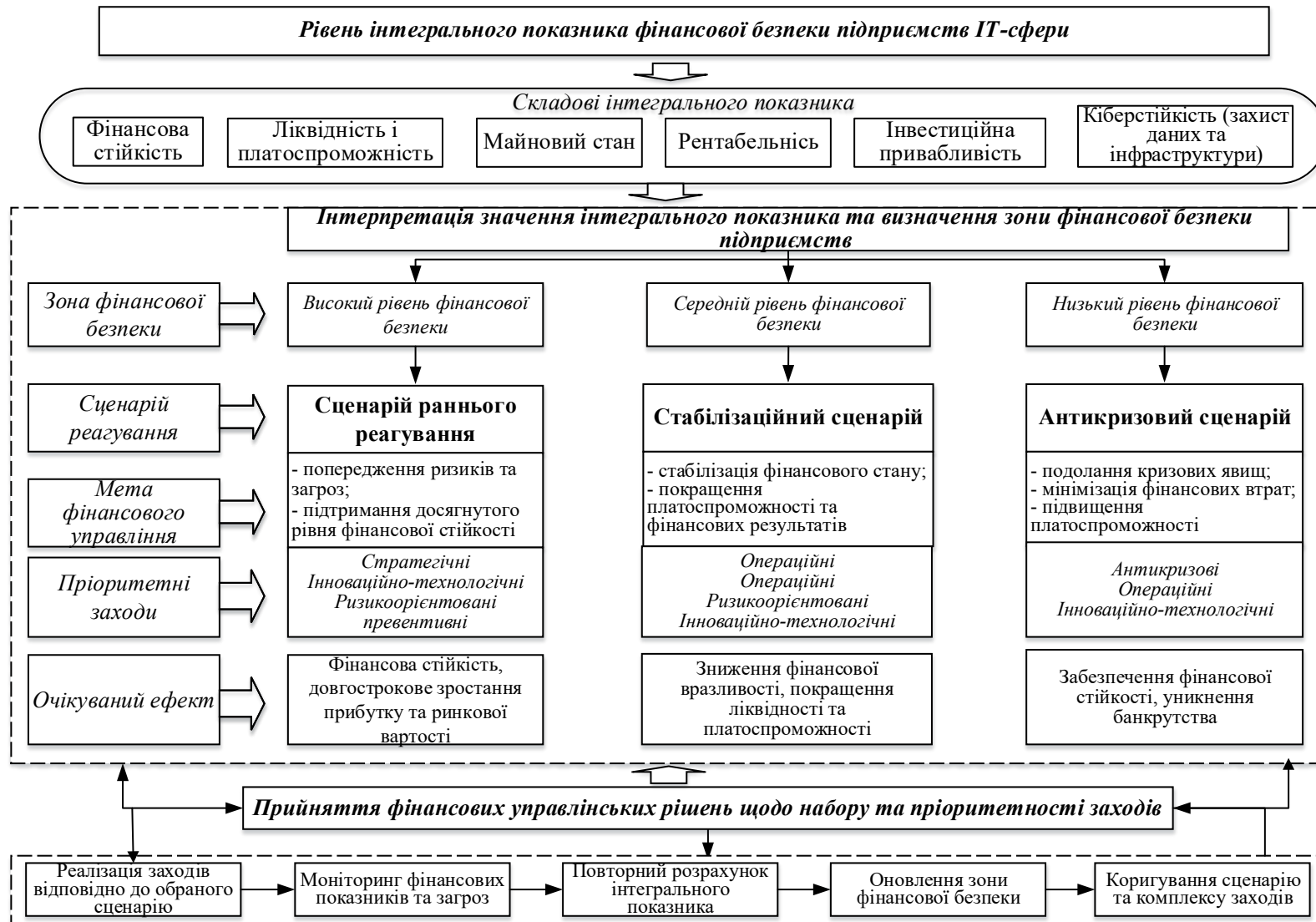


Рис. 3.11. Сценарний підхід до вибору заходів підвищення фінансової безпеки ІТ-підприємств

Джерело: складено автором.

- впровадження сучасних фінансово-аналітичних інструментів та автоматизації бюджетування та фінансового контролінгу;
- використання систем бізнес-аналітики для моніторингу фінансових показників і оперативного прийняття управлінських рішень;
- розвитку системи превентивного ризик-менеджменту, що дозволяє ідентифікувати потенційні фінансові загрози ще до їх настання;
- активного реінвестування прибутку у розвиток та інновації (R&D, нові IT-продукти та технології);
- збільшення інвестицій у людський капітал через навчання, мотиваційні заходи та утримання ключових спеціалістів;
- постійного контролю прибутковості та рентабельності бізнесу на основі моніторингу ключових фінансових показників (ROA, ROE, EBITDA тощо);
- розвитку та удосконалення системи фінансової кібербезпеки;
- оптимізації структури джерел фінансування шляхом залучення венчурного капіталу, грантів, краудфандингу тощо.

Одночасно підприємство може формувати стратегічні фінансові резерви, диверсифікувати ринки збуту та інвестувати у розвиток нових цифрових продуктів або напрямів діяльності.

Якщо IT-підприємство перебуває в задовільній зоні інтегрального показника фінансової безпеки, коли фінансовий стан залишається керованим, проте вже простежуються окремі негативні тенденції, впроваджується *стабілізаційний сценарій*. Для вітчизняних IT-підприємств така ситуація є доволі типовою через значні коливання обсягів виручки, у тому числі й експортної, нерівномірність надходження грошових потоків, зумовлену проєктною моделлю діяльності, нестабільність валютного ринку та загальну макроекономічну турбулентність.

За таких умов першочерговим завданням стає стабілізація фінансових процесів з метою недопущення подальшого погіршення фінансового стану. Тому в межах стабілізаційного сценарію доцільною є реалізація комплексу

управлінських заходів, спрямованих на зміцнення фінансової стійкості та покращення фінансових результатів шляхом:

- формування та підтримання достатнього рівня фінансових резервів;
- коригування бюджетів з урахуванням нерівномірності надходження грошових потоків за проєктами;
- посилення внутрішнього фінансового контролю за витратами, рухом грошових коштів та дебіторською заборгованістю;
- застосування сценарного фінансового планування з моделюванням можливих змін валютного курсу або обсягів замовлень з метою завчасного коригування фінансової політики підприємства;
- оптимізація управління оборотними активами та підтримання належного рівня ліквідності (оптимальний рівень грошових коштів, робота з дебіторською заборгованістю, моніторинг платежів);
- контроль операційних витрат і регулярний аналіз прибутковості проєктів для виявлення низькорентабельних проєктів чи напрямів діяльності;
- використання інструментів управління валютними ризиками (хеджування, страхування валютних коливань);
- автоматизація фінансового менеджменту та використання сучасних цифрових інструментів для контролю грошових потоків, здійснення фінансового аналізу та планування;
- залучення грантових програм, державної підтримки та інших фінансових ресурсів як додаткового джерела підсилення фінансової стійкості.

У підсумку реалізація зазначених заходів сприятиме згладжуванню фінансових коливань, підвищенню прогнозованості грошових потоків та поступовому переходу підприємства до більш стійкої зони фінансової безпеки.

Антикризовий сценарій реалізується в разі переходу ІТ-підприємства до критичної зони інтегрального показника фінансової безпеки, що свідчить про суттєве погіршення його фінансового стану та підвищення ризику втрати фінансової незалежності, ліквідності та платоспроможності. Для підприємств ІТ-

сектору України така ситуація може бути наслідком різкого скорочення експортних замовлень, затримок розрахунків із контрагентами, суттєвих валютних коливань або зростання витрат внаслідок зовнішніх економічних загроз.

Відповідно, основними ознаками цього стану є дефіцит грошових коштів, зменшення обсягів прибутку, зниження показників ліквідності, дисбаланс між надходженнями та витратами, зростання боргового навантаження та погіршення структури капіталу ІТ-підприємства. За таких умов першочерговим завданням для фінансового менеджменту стає оперативна стабілізація фінансового стану шляхом реалізації комплексу заходів, серед яких доцільно виділити такі:

- посилений контроль витрат і тимчасове обмеження неосновних видатків;
- мобілізація внутрішніх фінансових резервів;
- реструктуризація фінансових зобов'язань і перегляд умов співпраці з контрагентами;
- короткострокове фінансове планування з орієнтацією на забезпечення поточної платоспроможності;
- проведення фінансових стрес-тестів для оцінки чутливості підприємства до подальших негативних змін зовнішнього середовища;
- оптимізація управління оборотними активами, зокрема посилення контролю за дебіторською заборгованістю, прискорення інкасації платежів, контроль кредиторської заборгованості та раціональне використання фінансових ресурсів;
- оптимізація структури фінансування для мінімізації боргового навантаження та стабілізації структури капіталу;
- аналіз прибутковості проєктів і перегляд їхнього портфеля з концентрацією ресурсів на найбільш рентабельних напрямках;
- використання грантових програм і державної підтримки як додаткового джерела фінансових ресурсів;
- управління валютними ризиками для зменшення втрат у разі різких курсових коливань;

- посилення фінансової кібербезпеки з метою запобігання шахрайству, витоку фінансових даних, зриву платежів.

Реалізація зазначених заходів спрямована на зниження фінансової вразливості підприємства, відновлення ліквідності та створення передумов для повернення до стабільної роботи.

Також варто зазначити, що в сценарії раннього реагування переважають стратегічні та інноваційно-технологічні заходи, у стабілізаційному – операційні та ризикоорієнтовані, а для антикризового найбільш характерними є операційні, організаційні та антикризові інструменти та заходи короткострокової дії.

Таким чином, у межах цього підрозділу обґрунтовано теоретико-методичні підходи до побудови та функціонування механізму забезпечення фінансової безпеки ІТ-підприємств, визначено його сутність, мету, завдання та структурні складові. Розкрито зміст забезпечувального і функціонального блоків механізму, окреслено його принципи, функції, об'єкти та суб'єкти, а також обґрунтовано роль цифрових технологій як невід'ємного елементу його реалізації в умовах цифрової економіки.

Крім того, у межах підрозділу систематизовано заходи забезпечення фінансової безпеки ІТ-підприємств на мікрорівні, які охоплюють превентивні, стабілізаційні та антикризові напрями фінансового управління й інтегруються в механізм як інструмент реалізації фінансових рішень залежно від рівня фінансової безпеки ІТ-компанії.

Водночас забезпечення належного рівня фінансової безпеки ІТ-підприємств потребує не лише ефективного функціонування внутрішнього механізму, а й формування сприятливого зовнішнього середовища, що зумовлює необхідність дослідження напрямів державної підтримки та інституційного забезпечення розвитку ІТ-сфери, що буде розглянуто в підрозділі 3.3.

3.3. Державна та інституційна підтримка підвищення фінансової безпеки ІТ-підприємств в умовах цифрової економіки

Фінансова безпека ІТ-підприємств у сучасних умовах не може розглядатися виключно як результат внутрішніх фінансових управлінських рішень. Її рівень формується у складній системі взаємодії мікро- та макrorівнів, де внутрішні елементи системи фінансової безпеки ІТ-підприємства поєднуються з державними інституційними, регуляторними та економічними умовами функціонування ІТ-сектору.

Для українських ІТ-підприємств, діяльність яких здійснюється в умовах воєнних ризиків, макроекономічної нестабільності, валютних коливань і обмежень, а також високої залежності від зовнішніх ринків, напрями підвищення фінансової безпеки доцільно обґрунтовувати з урахуванням поєднання внутрішніх управлінських рішень і зовнішніх умов функціонування ІТ-сектору.

Саме тому при їх обґрунтуванні доцільно виходити з двостороннього характеру взаємодії між ІТ-бізнесом і державою. З одного боку, йдеться про заходи, які реалізуються безпосередньо на рівні підприємства, а з іншого – про державну політику та інституційні умови, що формують зовнішнє середовище функціонування ІТ-сектору. В умовах цифрової економіки такий вплив виявляється через якість інституційно-правового середовища, доступність фінансових ресурсів, розвиток кадрового потенціалу, інноваційної інфраструктури та цифрової безпеки ІТ-сектору.

Отже, після систематизації заходів підвищення фінансової безпеки на мікрорівні, що було здійснено у підрозділі 3.2, наступним етапом дослідження є обґрунтування напрямів підвищення фінансової безпеки ІТ-підприємств у системі державної та інституційної підтримки. З цією метою спочатку доцільним є кількісне підтвердження впливу ключових макроекономічних і галузевих чинників, які були розглянуті в підрозділі 2.1 та 3.1, на рівень

фінансової безпеки підприємств ІТ-галузі України. Для цього у роботі використано кореляційно-регресійний аналіз, результати якого дозволяють ідентифікувати найбільш чутливі параметри зовнішнього середовища, на які можуть бути спрямовані відповідні управлінські та регуляторні заходи.

За допомогою кореляційно-регресійного аналізу визначено напрям та силу статистичного зв'язку між інтегральним показником фінансової безпеки підприємств ІТ-сфери України та відповідними макроекономічними чинниками зовнішнього середовища та галузевими факторами.

Для вимірювання тісноти зв'язку між показниками використано коефіцієнт лінійної кореляції Пірсона, який визначається за формулою:

$$r_{xy} = \frac{\sum (x_i - \bar{x}) (y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \cdot \sum (y_i - \bar{y})^2}},$$

де x_i – значення факторного показника;

y_i – значення інтегрального показника фінансової безпеки;

\bar{x}, \bar{y} – середні значення відповідних показників.

З метою забезпечення коректності кореляційно-регресійного аналізу та підвищення надійності отриманих результатів у дослідженні використано обмежений перелік макроекономічних і галузевих факторів, які відображують найбільший вплив зовнішньоекономічного середовища та фінансово-економічного розвитку ІТ-сектору на рівень фінансової безпеки підприємств галузі. До таких факторів віднесено: обсяг експорту ІТ-послуг (x_1); відсоткову ставку за кредитами для юридичних осіб (x_2); чистий дохід від реалізації продукції (x_3); реінвестований прибуток ІТ-підприємств (x_4); обсяг сплачених податків ІТ-сектором України (x_5); індекс споживчих цін (x_6) (табл. 3.4).

Тобто обрані показники дозволяють комплексно охарактеризувати зовнішні та внутрішньогалузеві умови формування фінансової безпеки підприємств ІТ-сфери. Обсяг експорту ІТ-послуг відображає роль валютних надходжень у забезпеченні фінансової стійкості галузі; відсоткова ставка за кредитами характеризує умови залучення позикового капіталу; чистий дохід від реалізації продукції показує масштаби господарської діяльності ІТ-

сектору; реінвестований прибуток свідчить про можливості самофінансування розвитку; обсяг сплачених податків відображає рівень офіційної економічної активності та внесок галузі у фінансову систему держави; індекс споживчих цін характеризує загальне макроекономічне середовище та рівень інфляційного тиску.

Таблиця 3.4

Вихідні дані для проведення кореляційно-регресійного аналізу

Рік	Інтегральний показник рівня фінансової безпеки (ІФБ)	Обсяг експорту ІТ-послуг, млрд дол.	Відсоткова ставка за кредитами для юридичних осіб, %	Чистий дохід від реалізації продукції ІТ-сектору, млн грн.	Реінвестований прибуток ІТ-підприємств, млн грн.	Обсяг сплачених податків ІТ-сектором, млрд грн.	Індекс споживчих цін, %
2019	0,487	4,2	32,0	97663,3	3183,2	16,8	107,9
2020	0,570	5,0	31,7	113817,6	5613,2	19,7	102,7
2021	0,689	6,9	29,4	153488,7	4673,9	27,8	109,4
2022	0,776	7,2	29,4	183929,7	10453,9	32,2	120,2
2023	0,789	6,7	28,7	215364,1	17133,2	35,9	112,9
2024	0,822	6,4	28,5	253186,8	16217,0	41,6	106,5

Джерело: складено автором за даними [137; 141].

Водночас з огляду на обмежений часовий період дослідження та наявність взаємозалежності між окремими показниками, зокрема між чистим доходом, обсягом сплачених податків і реінвестованим прибутком, у роботі використано парні лінійні регресійні моделі. Це дозволяє уникнути надмірного ускладнення моделі та ризику мультиколінеарності, а також провести оцінювання напряму й сили зв'язку між кожним окремим фактором та інтегральним показником фінансової безпеки.

Результати кореляційного аналізу свідчать про наявність достатньо суттєвого зв'язку між рівнем фінансової безпеки підприємств ІТ-сфери та обраними макроекономічними й галузевими факторами (табл. 3.5).

Вплив макроекономічних та галузевих факторів на інтегральний показник фінансової безпеки підприємств ІТ-сфери України

	Y	X ₁	X ₂	X ₃	X ₄	X ₅	X ₆
Y	1,000	0,887	-0,956	0,950	0,857	0,972	0,494
X ₁	0,887	1,000	-0,889	0,712	0,557	0,773	0,650
X ₂	-0,956	-0,889	1,000	-0,932	-0,804	-0,958	-0,455
X ₃	0,950	0,712	-0,932	1,000	0,927	0,995	0,307
X ₄	0,857	0,557	-0,804	0,927	1,000	0,901	0,290
X ₅	0,972	0,773	-0,958	0,995	0,901	1,000	0,357
X ₆	0,494	0,650	-0,455	0,307	0,290	0,357	1,000

Джерело: складено автором.

Так, найтісніший прямий зв'язок виявлено між інтегральним показником фінансової безпеки та обсягом сплачених податків ІТ-сектором України ($r = 0,972$). Це свідчить про те, що збільшення податкових надходжень пов'язане не стільки з самим податковим навантаженням, скільки з розширенням діяльності ІТ-компаній, зростанням їх фінансових результатів та посиленням ролі галузі у фінансовій системі держави.

Високий позитивний зв'язок зафіксовано також між інтегральним показником фінансової безпеки та чистим доходом від реалізації продукції ІТ-сектору ($r=0,950$). Це підтверджує, що розширення дохідної бази підприємств ІТ-сфери є важливою передумовою зміцнення їх фінансової стійкості, ліквідності, платоспроможності та здатності до подальшого розвитку.

Достатньо високий позитивний коефіцієнт кореляції встановлено між інтегральним показником фінансової безпеки та обсягом експорту ІТ-послуг ($r = 0,887$), що підтверджує важливу роль експортної діяльності у формуванні фінансової стійкості ІТ-сфери України.

Позитивний зв'язок встановлено також між інтегральним показником фінансової безпеки та реінвестованим прибутком ІТ-підприємств ($r = 0,857$), що свідчить про важливість внутрішніх джерел фінансування для підтримання розвитку ІТ-компаній, оновлення технологічної бази, реалізації інноваційних проєктів і зменшення залежності від зовнішнього капіталу.

Найбільш тісний обернений зв'язок зафіксовано між інтегральним показником фінансової безпеки та відсотковою ставкою за кредитами ($r = -0,956$), адже зростання вартості кредитних ресурсів істотно обмежує фінансові можливості ІТ-підприємств, знижує їхню інвестиційну активність і негативно позначається на загальному рівні фінансової безпеки.

Також у межах кореляційного аналізу оцінено взаємозв'язок між інтегральним показником фінансової безпеки та індексом споживчих цін, який визначено як помірний. Отримане значення коефіцієнта кореляції ($r = 0,494$) свідчить про неоднозначність впливу інфляційних процесів на підприємства ІТ-сфери. З одного боку, інфляція підвищує операційні витрати та посилює макроекономічну нестабільність. З іншого боку, експортна орієнтація ІТ-сектору частково пом'якшують негативний вплив інфляційних процесів. Тому індекс споживчих цін доцільно розглядати як фактор із потенційно опосередкованим впливом, що потребує додаткової перевірки в межах регресійного моделювання, яке буде здійснено далі.

З метою проведення поглибленої кількісної оцінки впливу виділених макроекономічних і галузевих факторів на рівень фінансової безпеки підприємств ІТ-сфери побудуємо парні лінійні регресійні моделі. У цих моделях залежною змінною виступає інтегральний показник фінансової безпеки ($I_{\text{ФБ}}$), а незалежною - відповідний фактор:

$$Y_{I_{\text{ФБ}}} = \alpha + \beta X_t + \varepsilon_t,$$

де $Y_{I_{\text{ФБ}}}$ – інтегральний показник фінансової безпеки підприємств ІТ-сфери у період t ;

X_t – факторна змінна;

β – коефіцієнт регресії, що відображає силу та напрямок впливу фактору;

α – вільний член;

ε_t – випадкова похибка.

Для оцінки якості побудованих моделей використано коефіцієнт детермінації R^2 , який характеризує частку варіації результативного показника, що пояснюється зміною відповідного фактору. Статистичну значущість регресійних моделей перевірено за критерієм Фішера. За рівня значущості $\alpha=0,05$ табличне значення критерію Фішера становить $F_{\text{табл.}}=7,71$.

Узагальнення результатів регресійного аналізу впливу макроекономічних і галузевих факторів на інтегральний показник фінансової безпеки підприємств ІТ-сфери України представлено на рис. 3.12.

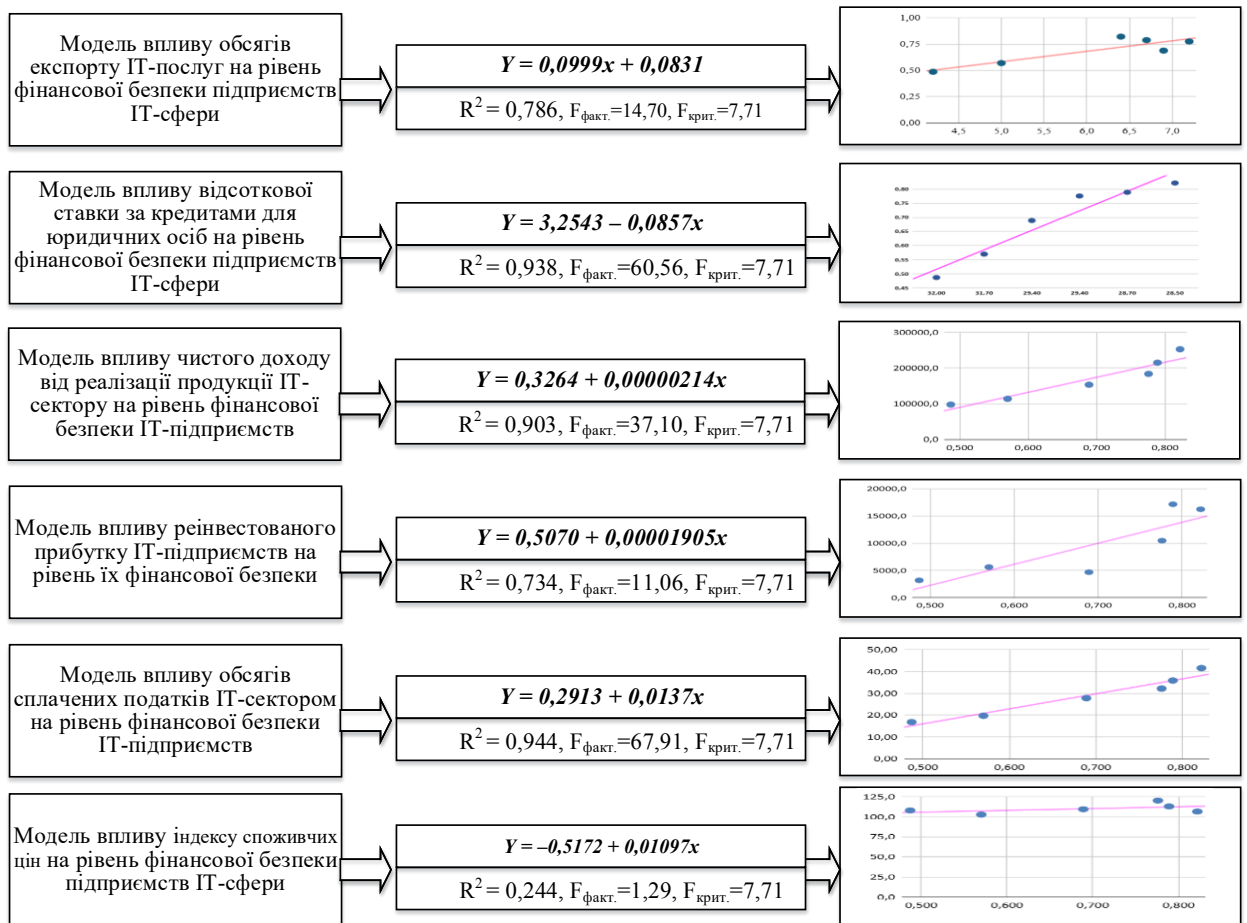


Рис. 3.12. Економетрична оцінка впливу факторів на рівень фінансової безпеки підприємств ІТ-сфери

Джерело: розраховано автором.

Таким чином, результати економетричного моделювання свідчать, що найбільш вагомий вплив на рівень фінансової безпеки підприємств ІТ-сфери мають обсяги сплачених податків ІТ-сектором, середня відсоткова ставка за кредитами, чистий дохід від реалізації продукції та обсяги експорту ІТ-послуг. Значення коефіцієнтів детермінації за відповідними моделями становлять 0,944; 0,938; 0,903 та 0,786, що свідчить про суттєву роль зазначених факторів у зміні інтегрального показника фінансової безпеки.

Позитивний вплив на фінансову безпеку ІТ-підприємств мають фактори, пов'язані зі зростанням масштабів діяльності галузі: експорт ІТ-послуг, чистий дохід від реалізації продукції, реінвестований прибуток та обсяги сплачених податків. Натомість підвищення середньої відсоткової ставки за кредитами має обернений вплив, оскільки зростання вартості кредитних ресурсів обмежує фінансові та інвестиційні можливості підприємств ІТ-сфери.

Щодо індексу споживчих цін, то його вплив на рівень фінансової безпеки є менш вираженим, про що свідчить найнижче серед побудованих моделей значення коефіцієнта детермінації ($R^2 = 0,244$). Це дає підстави розглядати інфляційний чинник не як визначальний, а як опосередкований фактор впливу на фінансову безпеку ІТ-підприємств.

Результати перевірки моделей за F-критерієм Фішера підтвердили статистичну значущість більшості побудованих моделей. Винятком є модель впливу індексу споживчих цін, для якої фактичне значення F-критерію є нижчим за критичне.

Водночас отримані результати слід розглядати з урахуванням обмеженого часового періоду дослідження та високої динамічності зовнішнього середовища, у якому функціонують ІТ-підприємства України. Воєнні ризики, валютні коливання, зміни кон'юнктури зовнішніх ринків, інвестиційна невизначеність та трансформація умов ведення бізнесу можуть посилювати або послаблювати вплив окремих факторів на рівень фінансової безпеки. Тому побудовані моделі доцільно розглядати не як повне відображення всіх чинників формування фінансової безпеки, а як інструмент кількісного підтвердження найбільш значущих напрямів впливу макроекономічних і галузевих факторів.

З метою обґрунтування напрямів державної політики щодо забезпечення фінансової безпеки підприємств ІТ-сектору України пропонуємо систематизувати їх за основними векторами впливу на фінансову безпеку. З цією метою нами виділено напрями прямої та опосередкованої дії та очікувані ефекти від їх реалізації (рис. 3.13).

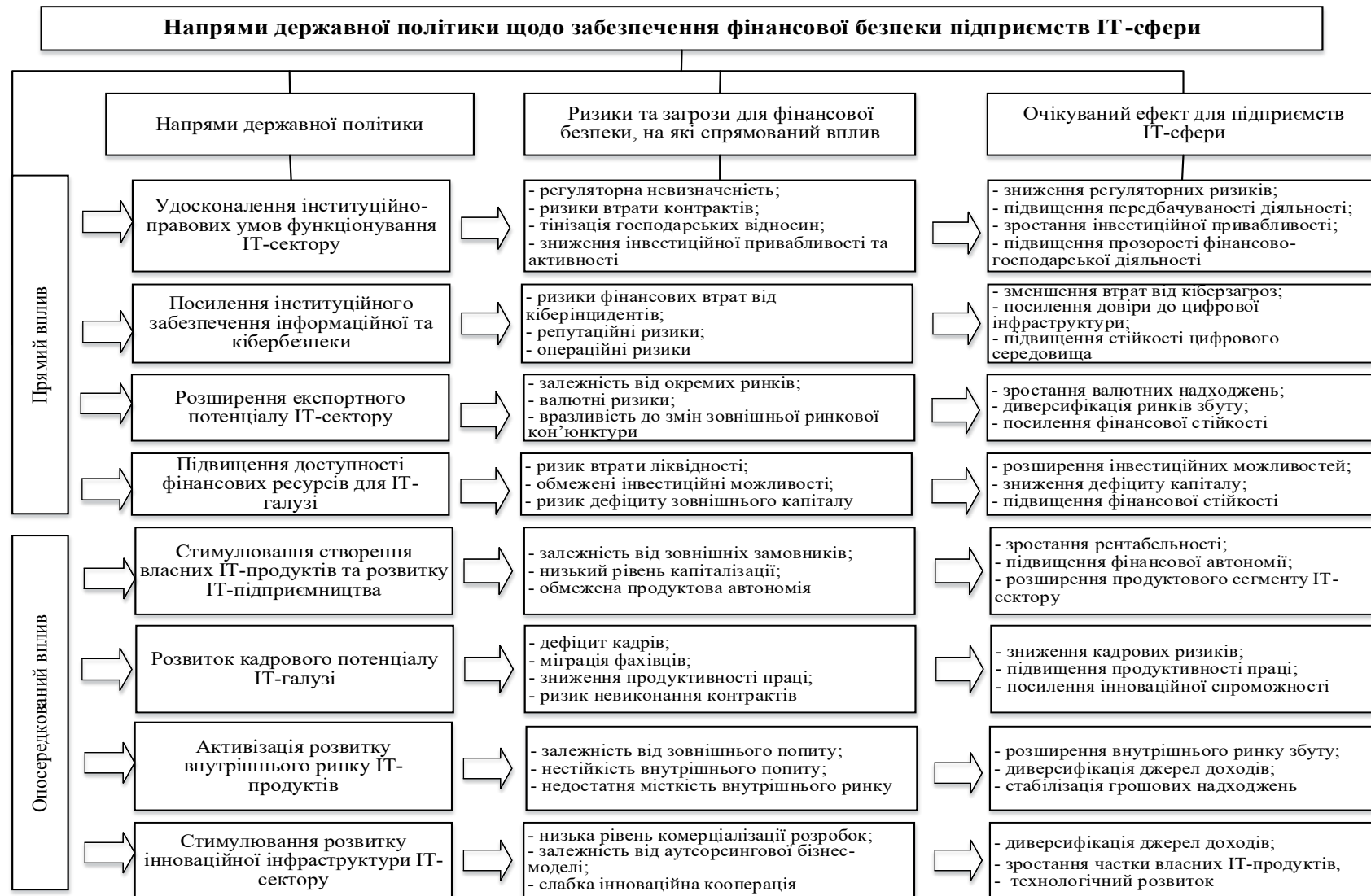


Рис. 3.13. Ризики та очікувані ефекти реалізації державної політики щодо підвищення фінансової безпеки ІТ-підприємств

Джерело: складено автором.

Для подальшої конкретизації запропонованих напрямів державної політики та розкриття практичних інструментів їх реалізації, доцільно провести їх групування за функціональними блоками державної політики, виділивши інституційно-регуляторний блок, спрямований на зниження правових, регуляторних і кіберризиків; інноваційно-інвестиційний блок, орієнтований на посилення інвестиційної спроможності, розвиток інновацій та створення власних ІТ-продуктів; кадровий блок, пов'язаний із формуванням та розвитком людського капіталу ІТ-галузі; а також ринковий блок, спрямований на розширення внутрішнього і зовнішнього ринків збуту та диверсифікацію доходів ІТ-підприємств. У межах кожного з цих блоків виокремлено пріоритетні заходи, спрямовані на нейтралізацію ризиків фінансової безпеки підприємств ІТ-сектору України (табл. Г.1, додаток Г), а також інструменти та методи реалізації (рис. 3.14).

Розглянемо напрями державної політики щодо забезпечення фінансової безпеки підприємств ІТ-галузі України більш детально.

1. Удосконалення інституційно-правових умов функціонування ІТ-сектору.

Формування стабільного інституційно-правового середовища є однією з ключових передумов розвитку ІТ-сектору та зміцнення фінансової безпеки його підприємств, особливо в умовах воєнного стану, коли зростає значення передбачуваності державної політики, захисту прав бізнесу та збереження довіри з боку міжнародних партнерів та інвесторів. Саме державна політика визначає базові правила функціонування ІТ-бізнесу, регулює правові засади його діяльності в цифровій економіці, забезпечує захист інтелектуальної власності, а також формує умови для залучення інвестицій та активізації інноваційної діяльності ІТ-компаній. Для підприємств ІТ-сфери якість інституційного середовища безпосередньо впливає на рівень регуляторних ризиків, доступ до зовнішнього фінансування, інвестиційну привабливість та стабільність умов ведення підприємницької діяльності.

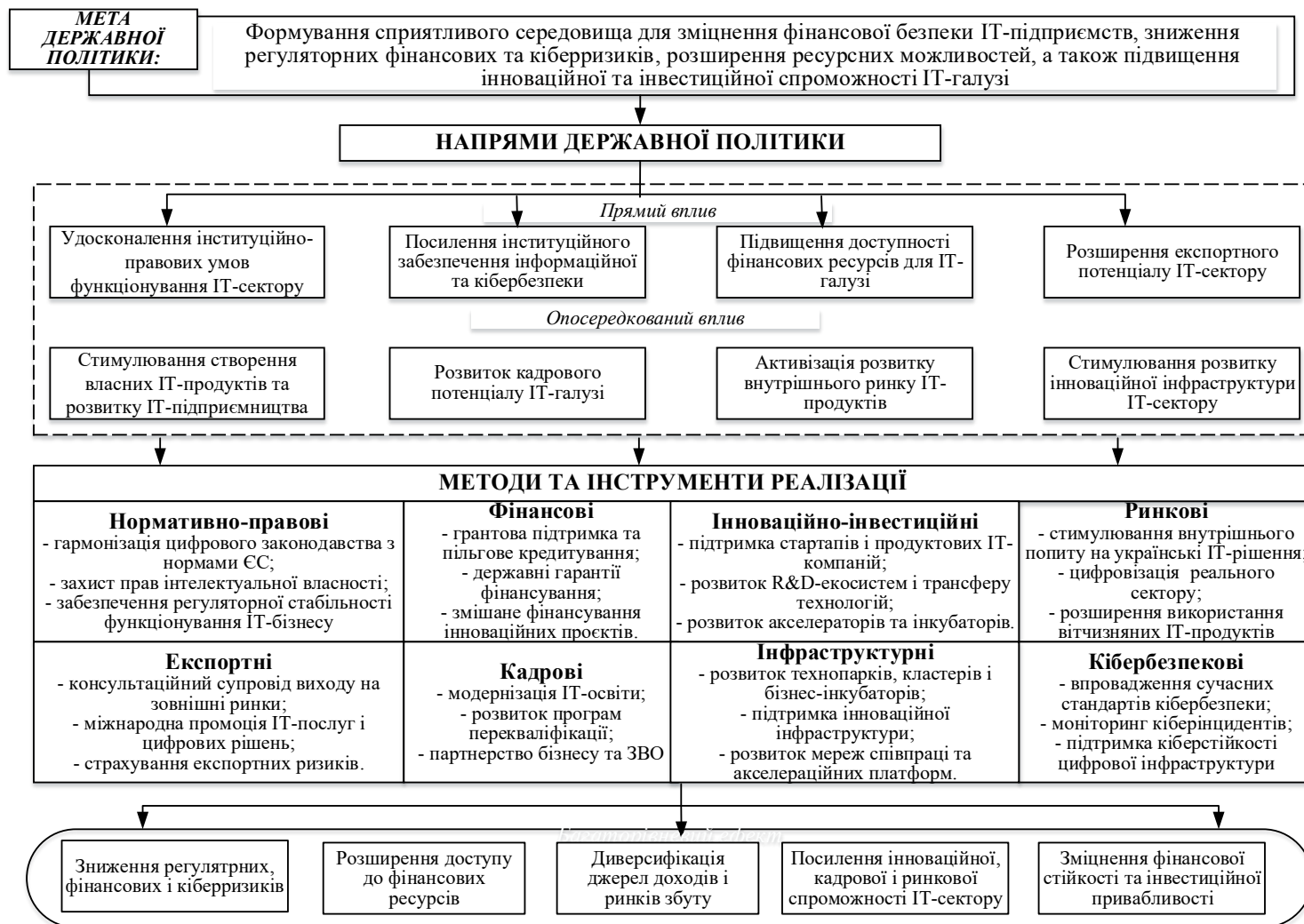


Рис. 3.14. Напрями та інструменти реалізації державної політики щодо підвищення фінансової безпеки ІТ-підприємств

Джерело: узагальнено автором на основі [117; 120; 209].

Як уже зазначалось раніше, з метою створення сприятливого податкового та правового середовища для ІТ-компаній, легалізації нових форм співпраці з фахівцями та формування більш прозорих правил ведення технологічного бізнесу стало запровадження в Україні спеціального правового режиму «Дія.City», що стало одним із прикладів формування спеціального інституційного середовища для підприємств цифрової економіки [44].

Важливою складовою такого середовища є також податковий клімат, оскільки саме він значною мірою визначає можливості ІТ-підприємств щодо інноваційного розвитку та реінвестування ресурсів у створення власних ІТ-продуктів, дослідження і розробки, розвиток цифрової інфраструктури та людського капіталу. Тому податкова політика держави має бути спрямована не лише на фіскальне регулювання, а й на стимулювання інноваційної активності, підтримку прозорості зайнятості та формування стабільних умов для розвитку ІТ-бізнесу шляхом впровадження податкових пільг та стимулів.

Поряд із цим, протягом останніх років в Україні здійснюється поступове удосконалення законодавства у сфері захисту прав інтелектуальної власності. Прийняття у 2022 році Закону України «Про авторське право і суміжні права» [166] стало важливим кроком у напрямку гармонізації національного законодавства з європейськими стандартами. Нові правові механізми сприяють підвищенню рівня захисту цифрових активів, удосконаленню процедур обліку та контролю за використанням інтелектуальної власності, а також посиленню відповідальності за порушення авторських прав.

Позитивні зрушення в державній політиці захисту інтелектуальної власності вплинули, зокрема, на обсяги залучення іноземних інвестицій, які у 2024 р. в технологічну галузь збільшились на 25 %, що свідчить про зростання довіри з боку іноземних інвесторів [253].

Водночас важливою проблемою інституційного забезпечення розвитку ІТ-сектору в Україні тривалий час залишається нестабільність, фрагментарність і недостатня системність нормативно-правової бази. Як зазначає М. І. Мельник, в Україні сформовано значний масив нормативних

актів у сфері інформатизації, легалізації програмного забезпечення, інноваційного розвитку, електронного урядування та цифрового документообігу. Однак наявність численних нормативно-правових актів ще не означає формування якісного регуляторного середовища, що пов'язано з рядом проблем реального застосування чинного законодавства (неефективні процедури його реалізації, розпорошення управлінських функцій і бюджетних ресурсів), а також з кризовими тенденціями соціально-економічного розвитку загалом [117]. За таких умов важливого значення набуває не лише подальше оновлення законодавства у сфері ІТ, а й його систематизація, гармонізація та підвищення ефективності практичного застосування.

Окремою складовою удосконалення інституційно-правового середовища є розвиток електронного урядування, електронного документообігу та правових механізмів легалізації програмного забезпечення. Зазначені інструменти не лише спрощують ведення ІТ-бізнесу, але й сприяють підвищенню прозорості господарських операцій, зниженню адміністративних витрат і формуванню більш передбачуваних умов взаємодії підприємств з державою та контрагентами [117].

Безпосередній вплив на фінансову безпеку ІТ-підприємств має також загальна стабільність інституційного середовища. У періоди політичної або економічної турбулентності зростають ризики скорочення міжнародних контрактів, обмежується доступ до іноземного фінансування, а зарубіжні партнери стають більш обережними у співпраці з українськими компаніями. В умовах повномасштабної війни значення цього чинника ще більше посилюється, тому державна політика має бути спрямована на забезпечення стабільності та передбачуваності інституційного середовища функціонування ІТ-сектору.

Крім того, удосконалення інституційно-правового середовища має бути пов'язане зі зниженням рівня тінізації ІТ-сектору, легалізацією зайнятості та підвищенням прозорості підприємницької діяльності. Зміцнення фінансової безпеки ІТ-сектору потребує не лише стимулювання його розвитку, а й підвищення прозорості господарських відносин, зменшення масштабів

неформальної зайнятості та формування більш контрольованого й передбачуваного ринкового середовища. Це має значення як для розширення податкової бази, так і для посилення довіри з боку інвесторів, кредиторів та міжнародних партнерів [120].

У зв'язку з цим реалізація цього напрямку державної політики має передбачати комплекс пріоритетних заходів, спрямованих на забезпечення стабільності і передбачуваності податкових, валютних, трудових, мобілізаційних та інших регуляторних рішень у сфері ІТ-бізнесу, дерегуляцію ведення ІТ-бізнесу, розвиток електронного документообігу, посилення захисту прав інтелектуальної власності та гармонізацію правового регулювання цифрової економіки з європейськими стандартами.

2. Стимулювання розвитку інноваційної інфраструктури ІТ-сектору

Важливим напрямом державної політики щодо забезпечення фінансової безпеки ІТ-підприємств є розвиток інноваційної інфраструктури ІТ-галузі. Йдеться про формування організаційних, інституційних та координаційних умов для функціонування технологічних парків, бізнес-інкубаторів, акселераторів, центрів трансферу технологій, R&D-центрів, професійних кластерів і платформ взаємодії між бізнесом, наукою, інвесторами та освітнім середовищем.

Як підкреслюється в [120], зростання можливостей інноваційної та технологічної ІТ-інфраструктури є одним із стратегічних пріоритетів розвитку ІТ-сектору України, оскільки саме вона визначає рівень його конкурентоспроможності та здатність генерувати високотехнологічні рішення та формувати власний інноваційний продукт. Водночас проблемою залишається недостатня узгодженість між окремими елементами інноваційної екосистеми: взаємозв'язки між ІТ-підприємствами, науково-дослідним сектором, інвесторами й венчурними структурами досі залишаються недостатньо розвиненими, що стримує темпи комерціалізації розробок і посилює залежність частини галузі від аутсорсингової моделі діяльності.

Сучасні тенденції підтверджують, що в Україні вже сформовано окремі елементи такої екосистеми. За даними Українського фонду стартапів, фонд підтримав понад 380 стартап-команд, а загальний обсяг наданого фінансування перевищив 8,7 млн дол. [207]. Крім того, за підсумками 2025 року Мінцифри повідомило, що Український фонд стартапів надав 2 млн дол. грантів 57 українським стартапам, а в межах програми Seeds of Bravery було профінансовано 274 DeepTech-стартапи на 12 млн євро [29; 218].

Крім грантових програм, фонд реалізує інструменти підтримки участі українських компаній у міжнародних технологічних подіях, а також програми корпоративних інновацій, що сприяють інтеграції стартапів у більші ринкові екосистеми [252].

Позитивною тенденцією є також розвиток акселераційних програм для українських ІІІ-стартапів, а також входження України до четвірки кращих за Startup Nations Standards [29; 126] та функціонування інноваційного парку UNIT.City, що позиціонується як середовище для розвитку стартапів, R&D-центрів та корпоративних інноваційних програм, об'єднуючи понад 100 компаній-резидентів [272]. Також галузеві дослідження IT Ukraine свідчать, що українська стартап-екосистема входить до трійки найшвидше зростаючих у Центральній та Східній Європі, що вказує на наявність реального інноваційного потенціалу навіть попри війну [244].

Водночас інноваційна інфраструктура ІТ-сектору України залишається недостатньо інтегрованою, а взаємозв'язки між ІТ-підприємствами, науково-дослідним сектором і венчурними структурами залишаються недостатньо розвиненими. Така ситуація зумовлює потребу у формуванні більш ефективної моделі взаємодії між її учасниками, здатної забезпечити ефективнішу комерціалізацію розробок і зміцнення інноваційного потенціалу вітчизняного ІТ-сектору.

В умовах повномасштабної війни значення цього напряму державної політики ще більше посилюється через ускладнення довгострокового інвестування, порушення міжнародної кооперації, релокацію частини бізнесу,

перерозподіл бюджетних ресурсів на оборонні потреби та загальне зростання невизначеності [91]. Враховуючи те, що в умовах війни ІТ-сектор зберігає вагоме значення для підтримки економіки України, військово-промислового комплексу та майбутнього повоєнного відновлення, розвиток інноваційної інфраструктури має розглядатися не як допоміжний, а як стратегічний напрям державної політики.

Тому реалізація цього напрямку державної політики має передбачати підтримку кластерних моделей розвитку, стимулювання кооперації між університетами та ІТ-бізнесом, розширення акселераційних програм, розвиток інноваційних парків, центрів трансферу технологій і R&D-екосистем, а також інтеграцію українських технологічних компаній у міжнародні інноваційні мережі. Як зазначає М. І. Мельник, важливими пріоритетами державної політики у цій сфері є комерціалізація ІТ-інновацій, удосконалення інституційного забезпечення інноваційного розвитку ІТ-сектору та формування сприятливих умов для ефективної взаємодії його суб'єктів на вітчизняному і міжнародному ринках [117].

Послідовна реалізація таких заходів сприятиме підвищенню рівня фінансової безпеки ІТ-підприємств через диверсифікацію джерел доходів, зростання частки власних ІТ-продуктів, посилення інноваційного потенціалу, підвищення технологічної конкурентоспроможності та зменшення залежності від зовнішніх замовників.

3. Підвищення доступності фінансових ресурсів для ІТ-галузі.

Для ІТ-компаній доступ до капіталу має стратегічне значення, оскільки визначає можливості фінансування поточної діяльності, інноваційного розвитку, масштабування бізнесу, виходу на нові ринки, розроблення власних ІТ-продуктів, придбання прав на об'єкти інтелектуальної власності та інвестування в дослідження і розробки.

На сьогодні для значної частини вітчизняних ІТ-підприємств, особливо стартапів та невеликих компаній, доступ до зовнішніх джерел фінансування залишається обмеженим. Банківські кредити часто є дорогівартісними або

малодоступними через високі вимоги до застави, короткі строки кредитування, підвищені ризики та загальну обережність фінансових установ щодо інноваційного бізнесу. У результаті багато ІТ-компаній змушені спиратися переважно на власні фінансові ресурси, що обмежує масштаби діяльності та стримує реалізацію інноваційних проєктів.

В умовах війни значення державної політики у сфері фінансування ІТ істотно посилюється. Війна супроводжується зростанням інвестиційних ризиків, підвищенням вартості капіталу, зменшенням доступу до приватного фінансування та перерозподілом значної частини бюджетних ресурсів на оборонні потреби. Тому для багатьох ІТ-компаній саме доступ до грантових, гарантійних і спеціалізованих програм підтримки стає важливою передумовою збереження фінансової стійкості, ліквідності, інноваційної активності та ринкових позицій.

На сьогодні важливим інструментом державної політики у сфері підвищення доступності фінансових ресурсів для ІТ-підприємств є діяльність державного Українського фонду стартапів, започаткованого у 2018 р. [207]. Через механізм конкурсного грантового фінансування фонд підтримує технологічні стартапи на ранніх стадіях розвитку, тим самим розширюючи їх доступ до стартового капіталу. Крім грантової підтримки, фонд реалізує інноваційні ваучери та програми корпоративних інновацій, що розширює можливості інтеграції молодих технологічних компаній у розвинуті бізнес-екосистеми та підвищує їхню інвестиційну спроможність.

Суттєвого значення набувають і механізми змішаного фінансування, у межах яких державна підтримка поєднується з ресурсами міжнародних партнерів та інвестиційних фондів. Так, Український фонд стартапів реалізує грантову програму підтримки українських технологічних компаній спільно з WNISEF, що є прикладом інституційної моделі, за якої держава не лише напряду фінансує інноваційний бізнес, а й створює умови для залучення зовнішніх ресурсів у розвиток технологічного підприємництва [207].

Окремий сегмент державної політики фінансової підтримки ІТ-підприємств формується у сфері defence tech, AI-технологій та кібербезпеки. Тут важливу роль відіграє платформа Brave1, яка об'єднує державу, бізнес, інвесторів і розробників навколо створення високотехнологічних рішень для безпеки й оборони. Через грантові та інші інструменти підтримки Brave1 держава фактично створила спеціалізований фінансовий канал для компаній, які працюють на перетині ІТ, інженерії, кібербезпеки та військових технологій. Для українського ІТ-сектору це створює нові джерела фінансування та стимулює розвиток високотехнологічного продуктового сегмента, здатного генерувати вищі прибутки і зміцнювати фінансову стійкість підприємств [237].

Таким чином, роль держави у цій сфері полягає не лише у загальному стимулюванні розвитку ІТ-сектору, а насамперед у створенні спеціальних механізмів, здатних забезпечити доступ ІТ-підприємств до різних джерел капіталу.

Для удосконалення та подальшого розширення ролі держави у забезпеченні фінансовими ресурсами ІТ-компаній на доцільним є впровадження таких заходів:

- створення спеціального механізму співінвестування технологічних проєктів за участю держави, міжнародних партнерів і приватних венчурних фондів [21];
- розвиток системи державних гарантій і страхування кредитів для ІТ-підприємств [21];
- запровадження програм пільгового банківського кредитування інноваційних і високотехнологічних проєктів [21];
- сприяння розвитку нетрадиційних інструментів фінансової підтримки розвитку ІТ-сфери, таких як: лізинг, франчайзинг, факторинг, краудфандинг та інших [21; 209];
- розширення доступу ІТ-підприємств до міжнародних технічно-фінансових програм [209];

- активніше використання механізмів державного замовлення для підтримки вітчизняних ІТ-компаній і створення стабільного попиту на технологічні рішення [120];
- стимулювання розвитку венчурного інвестування в ІТ-сектор [21];
- розширення інструментів фінансової підтримки інноваційних проєктів на ранніх стадіях їх розробки та апробації;
- розроблення спеціалізованих фінансових механізмів для підприємств із високою часткою нематеріальних активів та об'єктів інтелектуальної власності (наприклад, пільгові кредитні програми для ІТ-компаній без жорсткої вимоги матеріальної застави);
- активізація участі фінансово-кредитних установ у фінансуванні саме ІТ-сфери через спеціальні програми фінансування в партнерстві з державою (гарантійні, компенсаційні тощо) [100];
- масштабування програм фінансування ІТ-проєктів у сферах AI, кібербезпеки, defence tech та цифрової інфраструктури.

Послідовна реалізація таких заходів сприятиме зниженню ризику дефіциту ліквідності, розширенню інвестиційних можливостей ІТ-компаній, підвищенню їх адаптивності до воєнних і макроекономічних ризиків та зміцненню фінансової безпеки підприємств ІТ-сектору України. На макрорівні це позитивно впливатиме на інвестиційну привабливість галузі, зростання податкових надходжень і посилення ролі ІТ-сектору в забезпеченні фінансової стійкості національної економіки.

4. Розширення експортного потенціалу ІТ-сектору

Одним із важливих напрямів державної політики щодо підвищення рівня фінансової безпеки ІТ-підприємств України є розширення експортного потенціалу галузі. Для вітчизняного ІТ-сектору зовнішні ринки традиційно виступають вагомим джерелом доходів, валютних надходжень та інструментом збереження фінансової стійкості в умовах нестабільного внутрішнього економічного середовища.

У [120] підкреслюється, що розвиток ІТ-сектору в Україні має бути пов'язаний не лише зі зростанням обсягів господарювання, а й з більш активною діяльністю щодо дослідження зовнішніх ринків і просування власних ІТ-продуктів на експорт. Для цього необхідною є експертно-консалтингова, маркетингова та фінансово-кредитна підтримка вітчизняних ІТ-виробників – експортерів, а в економічно розвинених країнах у таких цілях ефективно функціонують різного роду експортно-кредитні агентства.

Для фінансової безпеки ІТ-підприємств розширення експортного потенціалу має принципове значення, оскільки дозволяє диверсифікувати джерела доходів, підтримувати стабільність валютних надходжень та знижувати залежність бізнесу від коливань внутрішнього ринку. Вихід на глобальні ринки також стимулює ІТ-компанії до дотримання вищих стандартів якості, захисту даних, належного рівня кібербезпеки та управління ризиками, що позитивно впливає на їхню конкурентоспроможність і фінансову стійкість.

В Україні вже існують окремі інструменти підтримки експортної діяльності, які можуть бути ширше інтегровані у політику розвитку вітчизняного ІТ-сектору. До ключових інституцій державної підтримки експорту в Україні належать Державна установа «Офіс з розвитку підприємництва та експорту» та Експортно-кредитне агентство [51]. Крім того, у межах ініціативи Ukraine-Ready4EU / Business Bridge українські малі та середні підприємства і стартапи могли отримувати фінансову підтримку для участі в ділових зустрічах, виставках, торгових місіях та інших заходах у країнах ЄС [240].

Разом з тим подальше розширення експортного потенціалу ІТ-сектору потребує більш цілеспрямованої державної підтримки саме саме технологічних компаній. У зв'язку з цим державна політика має бути спрямована не лише на загальну промоцію українського бізнесу за кордоном, а й на спеціалізований супровід ІТ-підприємств у пошуку міжнародних партнерів, адаптації до регуляторних вимог іноземних ринків, участі в міжнародних виставках, торговельних місіях і програмах просування цифрових продуктів [108].

Актуальним також є розвиток фінансових інструментів підтримки експорту, включаючи страхування експортних ризиків, часткове компенсаційне фінансування виходу на нові ринки, гарантійна підтримка зовнішньоекономічних контрактів та стимулювання міжнародної експансії українських ІТ-компаній. Такі інструменти дозволяють зменшити фінансове навантаження на підприємства на етапі виходу на нові ринки та підвищити їхню здатність конкурувати у глобальному цифровому середовищі.

В умовах війни окремого значення набуває розвиток механізмів міжнародного просування українських оборонних технологій і технологій подвійного призначення. У цій сфері державна політика має бути спрямована на спрощення процедур експортного контролю, удосконалення митного та валютного супроводу зовнішніх операцій, а також на формування міжнародних платформ презентації українських defense tech.

Показовим прикладом є ініціатива Defence City, у межах якої у 2025 році було задекларовано спрощення митних процедур для оборонних товарів, спрощений експортний контроль для військових технологій та спеціальний валютний режим для зовнішніх операцій резидентів. Водночас кластер Brave1 та організовані ним міжнародні події, зокрема Defense Tech Valley 2025, формують інституційне середовище для залучення іноземних партнерів, інвесторів і потенційних замовників до українських оборонних інновацій [238].

Таким чином, реалізація даного напрямку державної політики має передбачати комплекс пріоритетних заходів, спрямованих на розвиток інституційної підтримки експорту ІТ-послуг і цифрових продуктів, розширення міжнародної промоції українських ІТ-компаній, посилення консультаційного супроводу щодо виходу на нові ринки, а також розвиток фінансових механізмів стимулювання експортної діяльності. Послідовна реалізація таких заходів сприятиме збільшенню валютних надходжень, географічній диверсифікації експорту, зниженню залежності ІТ-підприємств від окремих зовнішніх ринків та зміцненню їх фінансової безпеки.

На макрорівні це означатиме посилення ролі ІТ-сектору у формуванні експортного потенціалу країни, підтримці платіжного балансу та зміцненні фінансової стійкості національної економіки.

5. Розвиток кадрового потенціалу ІТ-галузі.

Одним із ключових напрямів державної політики щодо забезпечення фінансової безпеки ІТ-підприємств є розвиток кадрового потенціалу ІТ-галузі. Для стабільного розвитку ІТ-компаній критично важливими є не лише залучення, а й утримання висококваліфікованих працівників, створення умов для їх професійного зростання, постійного навчання та підвищення мотивації [143].

З огляду на це роль державної політики полягає не лише у загальній підтримці освіти, а у формуванні системи підготовки, перепідготовки та професійного розвитку кадрів, адаптованої до сучасних потреб ІТ-сектору.

У [120] підкреслюється, що одним із стратегічних пріоритетів розвитку ІТ-сфери має бути модернізація системи професійної підготовки кадрів, оновлення освітніх програм відповідно до міжнародних стандартів, а також формування на базі закладів вищої освіти курсів підвищення кваліфікації за спеціальностями, затребуваними ІТ-сектором.

Важливим напрямом державної підтримки є також розвиток цифрових освітніх платформ, інструментів дистанційного навчання та програм швидкого формування актуальних ІТ-компетентностей, що особливо важливо в умовах швидких технологічних змін.

Як зазначають Голобородько А. Ю. та Андрєєва О. С., цифровізація управління персоналом, розвиток e-learning, використання аналітики, HRM-платформ та електронних систем навчання мають розглядатися як важливі інструменти підвищення ефективності роботи персоналу і розвитку трудового потенціалу ІТ-підприємств [34].

На сучасному етапі держава вже реалізує низку програм у цьому напрямі. Важливим прикладом цільової державної політики у сфері кадрового забезпечення ІТ-сектору став проєкт IT Generation, реалізований у 2022 році Міністерством цифрової трансформації. Цей проєкт надавав громадянам

можливість безкоштовно опанувати нову професію в ІТ та був спрямований, зокрема, на часткове розв'язання проблеми дефіциту кадрів у галузі [59].

Продовженням цього напрямку став подальший розвиток платформи Дія.Освіта та нових цифрових освітніх ініціатив, орієнтованих на розвиток цифрових і ШІ-компетентностей, зокрема через інтеграцію інструментів персоналізованого навчання на основі штучного інтелекту [29; 218].

Водночас наявні заходи потребують удосконалення системи розвитку, збереження та професійного оновлення людського капіталу ІТ-галузі, особливо в умовах війни та повоєнного відновлення, коли загострюються ризики міграції кадрів, посилюється конкуренція за кваліфікованих фахівців і зростає потреба у швидкому оновленні їхніх компетентностей.

У зв'язку з цим доцільним є подальше посилення державної політики у даному напрямі, зокрема шляхом:

- модернізації освітніх програм з ІТ-спеціальностей відповідно до потреб цифрової економіки та сучасних технологічних напрямів;
- розширення практикоорієнтованої та дуальної підготовки фахівців у співпраці між закладами освіти та ІТ-бізнесом;
- підтримки навчально-практичних центрів, лабораторій і освітньо-інноваційних хабів при закладах вищої освіти;
- розвитку програм перекваліфікації дорослого населення для входу в ІТ-сферу та адаптації до нових вимог ринку праці;
- масштабування короткострокових програм швидкого формування актуальних ІТ-компетентностей;
- розвитку цифрових освітніх платформ та інструментів персоналізованого навчання;
- посилення співпраці між державою, закладами освіти, ІТ-компаніями та професійними спільнотами у сфері підготовки кадрів;
- упровадження заходів, спрямованих на утримання, професійне оновлення та повернення кваліфікованих ІТ-фахівців в українське економічне середовище.

6. Посилення інституційного забезпечення інформаційної та кібербезпеки.

Важливим напрямом державної політики щодо забезпечення фінансової безпеки ІТ-підприємств України є розвиток інституційної інфраструктури кібербезпеки та інформаційної безпеки. В умовах цифрової трансформації економіки та зростання залежності бізнесу від цифрових сервісів саме держава має забезпечувати формування цілісної системи захисту інформаційних ресурсів, критичної цифрової інфраструктури та механізмів реагування на кіберзагрози.

Нормативно-правову основу забезпечення кібербезпеки в Україні становлять Закон України «Про основні засади забезпечення кібербезпеки України» [169], Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [168], Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [167], а також Стратегія кібербезпеки України (від 26.08.2021) [170] та Стратегія інформаційної безпеки [172] та ін. Саме через ці документи держава визначає інституційні засади організації кіберзахисту, розмежування повноважень між відповідальними органами, пріоритети розвитку системи моніторингу кіберінцидентів та напрями зміцнення стійкості цифрової інфраструктури.

У межах цього напрямку державна політика має реалізовуватися через низку заходів. Передусім йдеться про посилення інституційної спроможності органів, відповідальних за кібербезпеку, зокрема шляхом удосконалення координації між державними структурами, розвитку систем державного нагляду у сфері кібербезпеки та підвищення ефективності реагування на кіберінциденти. Важливим кроком у цьому напрямі стало відновлення у 2025 році повноважень Держспецзв'язку щодо державного нагляду у сфері кібербезпеки, що має на меті посилення координації та результативності захисних заходів [182].

Не менш актуальним на сьогодні є також розвиток системи моніторингу та реагування на кіберінциденти. Підключення до неї відповідних державних організацій дасть змогу підвищити швидкість виявлення загроз, забезпечити оперативне реагування на кібератаки та підтримувати безперервність функціонування цифрових сервісів. Для ІТ-підприємств це означає зниження системних ризиків, пов'язаних із масштабними атаками на державні цифрові сервіси, телекомунікаційні мережі чи об'єкти критичної інфраструктури.

Окремим пріоритетом державної політики має бути державна підтримка кіберстійкості критичної цифрової інфраструктури, зокрема телекомунікаційних мереж, дата-центрів, державних платформ і цифрових сервісів. У період повномасштабної війни саме цей напрям набув особливого значення, оскільки кіберзахист став невід'ємною складовою безперервності функціонування держави, економіки та цифрового бізнес-середовища.

Ще одним вагомим напрямом державної політики є стимулювання впровадження сучасних стандартів кібер- та інформаційної безпеки. Для ІТ-підприємств розвиток державної системи кіберзахисту має подвійний фінансовий ефект. З одного боку, підвищення рівня захисту інформаційних систем сприяє зниженню ризиків фінансових втрат, пов'язаних із витоком даних, кібератаками чи порушенням роботи цифрових сервісів. З іншого боку, дотримання сучасних стандартів кібербезпеки потребує додаткових інвестицій у модернізацію ІТ-інфраструктури, впровадження систем кіберзахисту та підвищення кваліфікації персоналу. Саме тому держава має не лише встановлювати вимоги до кіберзахисту, а й створювати умови для організаційної, методичної та інституційної підтримки підприємств у процесі адаптації до цих вимог.

Окремої уваги потребує розвиток людського капіталу у сфері інформаційної безпеки. Важливим є впровадження державних ініціатив, спрямованих на підвищення цифрової грамотності, розвиток навичок кібергігієни, підготовку фахівців із кібербезпеки та формування культури безпечного використання цифрових технологій як у державному секторі, так і в бізнес-середовищі [217].

Водночас наявні заходи державної політики у сфері кібер- та інформаційної безпеки здебільшого орієнтовані на загальне зміцнення стійкості цифрового середовища та критичної інфраструктури, тоді як потреби ІТ-підприємств як окремої групи суб'єктів господарювання потребують більш адресного підходу. У зв'язку з цим доцільним є розвиток державних механізмів попередження кіберризиків у діяльності ІТ-підприємств, удосконалення інструментів їх адаптації до сучасних стандартів кібербезпеки, розширення державно-приватної координації у сфері моніторингу та реагування на кіберзагрози, а також диференціація заходів підтримки залежно від типу, масштабу та рівня ризиковості ІТ-бізнесу.

7. Стимулювання створення власних ІТ-продуктів та розвитку ІТ-підприємництва.

Важливим напрямом державної політики щодо підвищення рівня фінансової безпеки ІТ-підприємств України є стимулювання з боку держави створення власних ІТ-продуктів та розвиток технологічного підприємництва. Актуальність цього напрямку зумовлена тим, що вітчизняний ІТ-сектор історично розвивався переважно за аутсорсинговою моделлю, яка забезпечує стабільні валютні надходження, проте обмежує розвиток власного продуктового сегменту та технологічної бази всередині країни.

Авторами [120] слушно підкреслюється, що однією зі стратегічних проблем розвитку ІТ-сектору України є недостатня підприємницька активність та незначна частка проєктів, які ініціюються, фінансуються і комерціалізуються безпосередньо вітчизняними суб'єктами господарювання. Хоча, як показав проведений аналіз у другому розділі, в останні роки спостерігається тенденція до зростання частки вітчизняних продуктових ІТ-компаній.

У сучасних умовах такий перехід від аутсорсингової моделі до продуктової набуває не лише економічного, а й безпекового значення. Продуктові ІТ-компанії, як правило, мають вищий потенціал капіталізації, кращі можливості диверсифікації доходів, сильніші конкурентні позиції на глобальному ринку та більшу стійкість до коливань зовнішнього попиту. Для фінансової безпеки ІТ-підприємств це означає зниження залежності від

обмеженого кола замовників, посилення фінансової автономії і створення передумов для розвитку у довгостроковій перспективі.

Сучасні тенденції свідчать, що в Україні вже формується середовище, у якому розвиток власних технологічних продуктів поступово стає окремим вектором політики держави. Підтримка стартапів, наукоємних проєктів, а також розвиток ініціатив у сферах defense tech, штучного інтелекту, кібербезпеки, GovTech та інше свідчать про поступове зміщення акцентів державної політики до підтримки продуктового та технологічно орієнтованого підприємництва [207]. У цьому контексті особливого значення набуває не лише фінансова підтримка стартапів, серед яких найбільше саме в сфері інформаційно-комунікаційних технологій, а і створення умов для їх масштабування, тестування, ринкової апробації та подальшої комерціалізації.

Так і IT Ukraine наголошує, що до 2030 року українське IT має трансформуватися з сервісного експортера на технологічного гравця, що розвиває власні продукти, R&D та стартапи. Ключовими напрямками зростання залишаться кібербезпека, DefenseTech, GovTech, AI та аналітика даних, а також GameDev і EdTech [110].

Водночас наявні заходи державної підтримки у цій сфері поки що переважно орієнтовані на розвиток окремих стартап-ініціатив та інноваційних проєктів, тоді як потребує посилення саме системний підхід до формування продуктового сегмента IT-сектору. У зв'язку з цим державна політика має бути спрямована не лише на підтримку створення нових IT-продуктів, а й на поєднання фінансових, інституційних та ринкових інструментів, здатних забезпечити подальше закріплення їх позицій на ринку.

З огляду на це вважаємо, що реалізація даного напрямку державної політики має передбачати комплекс пріоритетних заходів, спрямованих на підтримку стартапів і продуктових компаній на ранніх стадіях розвитку, стимулювання високотехнологічних інноваційних сегментів, розширення партнерських програм, підтримку державно-приватних проєктів зі створення цифрових рішень, а також забезпечення сприятливих умов для масштабування українських продуктових компаній на внутрішньому та зовнішньому ринках.

Автори [120] також наголошують на важливості співпраці ІТ-підприємств зі сферою торгівлі, послуг та іншими секторами економіки, а також на доцільності державно-приватних проєктів із частковим фінансуванням створення ІТ-продукту. Саме тому створення власного ІТ-продукту має розглядатись як стратегічний вектор розвитку вітчизняного ІТ-бізнесу, що сприятиме зростанню внутрішнього попиту на вітчизняні цифрові рішення та поступовому зменшенню залежності ІТ-сектору від аутсорсингової моделі.

Для фінансової безпеки вітчизняних ІТ-підприємств розвиток власних продуктів має важливе значення, оскільки створює передумови для підвищення рентабельності бізнесу та зміцнення його фінансової стійкості. На відміну від класичної аутсорсингової моделі, продуктові ІТ-компанії потенційно здатні забезпечувати вищу прибутковість, більш стабільні грошові потоки, кращі можливості для нарощення власного капіталу та інвестиційну привабливість. На макрорівні такі зміни створюють передумови для структурної модернізації ІТ-сектору та зміцнення позицій України як розробника і виробника власних цифрових продуктів, а не лише постачальника ІТ-послуг.

8. Активізація розвитку внутрішнього ринку ІТ-продуктів.

Важливим напрямом державної політики щодо забезпечення фінансової безпеки ІТ-підприємств України є створення сприятливих умов для розвитку внутрішнього ринку ІТ-продуктів. У цьому контексті роль держави полягає у формуванні платоспроможного внутрішнього попиту на цифрові рішення, стимулюванні використання вітчизняних ІТ-продуктів у державному та корпоративному секторах, а також у створенні умов для більш широкої інтеграції ІТ-розробок у різні сфери національної економіки.

Для фінансової безпеки ІТ-підприємств розвиток внутрішнього ринку має принципове значення, оскільки дає змогу диверсифікувати джерела доходів, зменшити залежність від зовнішніх замовників, розширити можливості реалізації власних продуктів і підтримати стабільність грошових надходжень. В умовах війни та макроекономічної нестабільності внутрішній ринок може виступати додатковим каналом збуту для компаній, які працюють

у продуктовому сегменті або створюють прикладні цифрові рішення для українського бізнесу й держави.

У площині державної політики розвиток внутрішнього ринку ІТ-продуктів має передбачати насамперед стимулювання попиту на українські цифрові рішення у межах національної економіки. Насамперед йдеться про цифровізацію підприємств реального сектору економіки, сфери торгівлі, послуг, логістики, освіти, медицини та публічного управління, де саме ІТ-продукти здатні підвищувати ефективність господарських процесів і якість послуг. Держава в цьому разі виступає не лише регулятором, а й важливим замовником і стимулятором попиту.

Сучасні приклади підтверджують, що такий підхід уже має практичну реалізацію. Так, сервіс «Дія», створений як Єдиний державний веб-портал електронних послуг, розширює можливості використання цифрових рішень у сфері надання державних послуг в Україні. Крім того, у межах Ukraine Facility визначено цифрову трансформацію однією з наскрізних складових вітчизняних реформ, а в урядових програмах підкреслюється, що цифровізація процесів державного управління, відкритість даних і розвиток державних сервісів для бізнесу мають стати основою для покращення бізнес-середовища та розвитку приватного сектору [266].

Водночас наявні заходи поки що не формують цілісної системи підтримки внутрішнього збуту вітчизняних ІТ-продуктів. Тому державна політика має бути спрямована не лише на загальну цифровізацію економіки, а й на системне розширення практики використання українських цифрових рішень у державному секторі, бізнес-середовищі та ключових галузях національної економіки. Йдеться про стимулювання державного, муніципального та корпоративного замовлення на вітчизняні ІТ-продукти, підтримку їх пілотного впровадження, а також створення умов для подальшого поширення українських цифрових рішень у внутрішньому економічному середовищі.

У цьому напрямку важливим інструментом є створення інформаційної платформи для забезпечення комунікації між представниками ІТ-сфери, суб'єктами підприємницької діяльності, інвесторами та державним сектором з метою сприяння залученню інвестицій та реалізації креативних ідей щодо створення вітчизняних ІТ-брендів з подальшими їх впровадженням у національній економіці [21].

Окремого значення набуває розвиток державно-приватних проєктів, у межах яких частина витрат на створення або впровадження ІТ-продукту може фінансуватися державою або іншими партнерами. Крім того, перспективним напрямом є ширше використання державного замовлення на створення суспільно значущих ІТ-продуктів, що може виступати не лише інструментом цифрової модернізації державного сектору, а й засобом підтримки вітчизняних ІТ-підприємств та формування стабільного внутрішнього ринку збуту.

Отже, реалізація даного напрямку державної політики має передбачати комплекс пріоритетних заходів, спрямованих на стимулювання внутрішнього попиту на українські ІТ-рішення, розвиток цифрових державних сервісів, підтримку державно-приватних проєктів із впровадження цифрових продуктів, цифровізацію реального сектору економіки, розширення державного і корпоративного замовлення на вітчизняні ІТ-продукти, а також створення сприятливих умов для ринкової апробації та масштабування українських цифрових рішень у ключових сферах суспільного життя. Послідовне впровадження таких заходів сприятиме розширенню внутрішнього ринку збуту, диверсифікації джерел доходів ІТ-підприємств, стабілізації їх грошових надходжень і зміцненню фінансової безпеки підприємств ІТ-сектору України.

Таким чином, у підрозділі 3.3. обґрунтовано, що підвищення фінансової безпеки ІТ-підприємств потребує не лише внутрішніх управлінських рішень на рівні окремого суб'єкта господарювання, а й формування сприятливого державного та інституційного середовища функціонування ІТ-сектору. На основі проведеного кореляційно-регресійного аналізу встановлено, що найбільш значущими зовнішніми чинниками впливу на інтегральний рівень

фінансової безпеки вітчизняних ІТ-підприємств є доступність фінансових ресурсів та експортна спроможність галузі. Це підтверджує необхідність поєднання фінансово-економічних, правових, інноваційно-інвестиційних, ринкових, інфраструктурних та інших інструментів державної політики.

Запропонована систематизація напрямів державної та інституційної підтримки дозволила виокремити напрями прямого й опосередкованого впливу на фінансову безпеку ІТ-підприємств та пов'язати їх із конкретними методами й інструментами реалізації.

Висновки до третього розділу

1. Визначено та систематизовано основні зовнішні загрози фінансовій безпеці підприємств ІТ-сфери. Встановлено, що вони формуються під впливом політичних, економічних, соціальних та технологічних чинників, що було узагальнено за компонентами PEST-аналізу. Доведено, що найбільш деструктивний вплив у сучасних умовах мають воєнно-політична нестабільність, валютні та регуляторні обмеження, нестабільність інституційного середовища, кадрові втрати, технологічні й кіберзагрози, які безпосередньо впливають на доходи, витрати, ліквідність і загальну фінансову стійкість ІТ-підприємств.

2. Обґрунтовано, що внутрішні ризики доцільно групувати за напрямами їх впливу на фінансову безпеку, з виокремленням фінансових, інвестиційних, кадрових, управлінських, операційних та інформаційно-технологічних ризиків. Проведений SWOT-аналіз підтвердив, що фінансова безпека підприємств ІТ-сфери України формується на перетині достатньо сильного внутрішнього фінансового потенціалу та високої чутливості до зовнішніх загроз, що зумовлює необхідність поєднання внутрішніх управлінських заходів з адаптації до нестабільного зовнішнього середовища.

3. Обґрунтовано концептуальні засади розробки та впровадження механізму забезпечення фінансової безпеки ІТ-підприємств, визначено його основні елементи та розкрито взаємозв'язок між ними. Побудовано структурну схему механізму, яка охоплює мету, завдання, об'єкт, суб'єктів, принципи, функції, інструменти, важелі та інформаційно-аналітичне забезпечення, що дозволило цілісно представити архітектуру управління фінансовою безпекою ІТ-підприємств з урахуванням галузевої специфіки та високої динамічності зовнішнього середовища.

4. Розкрито структурно-логічну модель забезпечення фінансової безпеки ІТ-підприємств як послідовного управлінського процесу, що поєднує стратегічний і оперативний рівні фінансового впливу. Доведено, що ефективність реалізації такого процесу залежить від його адаптивності, своєчасного реагування на ризики і загрози, інтеграції у систему фінансового менеджменту та використання цифрових технологій для підвищення обґрунтованості управлінських рішень. Окремо встановлено, що невід'ємною складовою цього процесу має бути кіберстійкість, оскільки порушення цифрової інфраструктури безпосередньо впливає на безперервність операційної діяльності, стабільність грошових потоків і фінансові результати ІТ-компаній.

5. Систематизовано заходи підвищення фінансової безпеки ІТ-підприємств на мікрорівні шляхом їх групування за п'ятьма взаємопов'язаними блоками: стратегічними, операційними, організаційними, ризикорієнтованими та інноваційно-технологічними. Обґрунтовано, що така систематизація дозволяє поєднати довгострокові завдання зміцнення фінансової стійкості з поточним управлінням ліквідністю, витратами, грошовими потоками, ризиками та інформаційно-аналітичним забезпеченням фінансових рішень. Для практичної реалізації цих заходів запропоновано сценарний підхід, який передбачає виокремлення сценарію раннього реагування, стабілізаційного та антикризового сценарію залежно від фактичного рівня фінансової безпеки підприємства.

6. Обґрунтовано, що підвищення фінансової безпеки ІТ-підприємств потребує поєднання заходів мікро- та макрорівня. Визначено, що на макрорівні вагоме значення мають державна та інституційна підтримка ІТ-сектору, розвиток сприятливого правового, економічного й організаційного середовища його функціонування, а також посилення кіберзахисту та інфраструктурної стійкості цифрового середовища. Це створює необхідні зовнішні умови для ефективної реалізації внутрішніх управлінських заходів підприємств і зміцнення їх фінансової стійкості в умовах цифрової економіки.

Основні результати дослідження опубліковані в таких наукових роботах [66; 100; 103; 146; 147; 149].

ВИСНОВКИ

1. Поглиблено теоретичні положення щодо розуміння сутності фінансової безпеки підприємства в умовах становлення цифрової економіки. Це здійснено шляхом узагальнення наукових підходів до трактування понять «фінансова безпека підприємства» та «цифрова економіка», а також обґрунтування зміни змісту фінансової безпеки під впливом цифровізації. Виокремлено інноваційний підхід до її розуміння, відповідно до якого фінансова безпека підприємства розглядається також як здатність підприємства забезпечувати захист інформаційних ресурсів і цифрових активів, протидіяти кіберризикам та адаптуватися до змін цифрового середовища. Це дало змогу визначити, що в умовах цифрової економіки фінансова безпека підприємства набуває нового змістового наповнення та має формуватися на основі поєднання традиційних фінансових механізмів із цифровими інструментами аналізу, контролю, прогнозування, управління ризиками та кіберзахисту.

2. Досліджено концептуально-змістовні характеристики функціонування підприємств ІТ-сфери в умовах цифрової економіки. Це реалізовано через уточнення змісту поняття «ІТ-сфера», конкретизацію меж функціонування вітчизняних ІТ-підприємств за видами економічної діяльності та класифікацію ІТ-компаній за ознаками, що визначають особливості їх фінансової безпеки. Встановлено, що ІТ-підприємства виступають не лише окремим сектором економіки, а й інфраструктурною основою цифрової трансформації, оскільки створюють технологічні рішення, які забезпечують модернізацію інших галузей і формують мультиплікативний ефект розвитку цифрової економіки. Обґрунтовано, що фінансова безпека ІТ-підприємств формується під впливом специфічних галузевих детермінант, пов'язаних із домінуванням нематеріальних активів, високою роллю людського капіталу, проєктним характером діяльності, залежністю від цифрової інфраструктури, інноваційністю та кіберризиками. Це дозволило визначити, що забезпечення фінансової безпеки ІТ-підприємств потребує адаптивних підходів до

фінансового управління, здатних враховувати специфічний ризик-профіль ІТ-бізнесу та високу динамічність цифрового середовища.

3. Обґрунтовано теоретичні засади формування системи фінансової безпеки підприємств ІТ-сфери. Це реалізовано через застосування системного підходу до розуміння фінансової безпеки ІТ-підприємств як складної, відкритої, адаптивної та динамічної системи, що функціонує в умовах цифрової економіки. Розроблено концептуальну модель такої системи, у межах якої визначено її мету, ресурси, суб'єкти, об'єкти захисту, структурні підсистеми, функції та принципи функціонування. Це дозволило показати, що система фінансової безпеки ІТ-підприємств має не лише внутрішньогосподарське значення, а й формує багаторівневий ефект - від зміцнення фінансової стійкості окремого підприємства до підвищення стійкості ІТ-сектору та фінансової безпеки держави.

4. Проведено аналіз сучасного стану ІТ-сфери України та фінансового стану її підприємств, який підтвердив, що вітчизняний ІТ-сектор, попри погіршення окремих показників у період повномасштабної війни, зберігає важливе значення для національної економіки, формування експортного потенціалу, валютних надходжень та податкової бази держави. Встановлено, що фінансовий стан ІТ-підприємств, на відміну від суб'єктів господарювання традиційних галузей економіки, характеризується переважанням оборотних активів, високою мобільністю ресурсів, відносно низькою капіталомісткістю, достатнім рівнем ліквідності та фінансової автономії. Це дозволило визначити, що фінансова стійкість ІТ-підприємств значною мірою забезпечується особливостями структури їх активів і капіталу, що дає змогу підтримувати фінансово-економічну активність і адаптуватися до складних умов макроекономічної нестабільності та воєнних викликів.

5. Удосконалено методичний підхід до комплексної оцінки рівня фінансової безпеки підприємств ІТ-сфери в умовах цифрової економіки. Це здійснено шляхом систематизації наукових підходів до оцінювання фінансової безпеки підприємств та обґрунтування доцільності використання

інтегрального показника, адаптованого до специфіки ІТ-бізнесу. Запропоновано здійснювати оцінювання рівня фінансової безпеки ІТ-підприємств за складовими фінансової стійкості, ліквідності, прибутковості, майнового стану, ділової активності та інвестиційної привабливості. Це дозволило перейти від аналізу окремих фінансових коефіцієнтів до узагальненої оцінки рівня фінансової безпеки і сформувати аналітичну основу для подальшого визначення загроз, обґрунтування механізму та заходів забезпечення їх фінансової безпеки.

6. Систематизовано зовнішні загрози та внутрішні ризики формування системи фінансової безпеки підприємств ІТ-сфери. Це реалізовано шляхом розмежування понять «виклик», «ризик» і «загроза» та уточнення характеру їх впливу на фінансову стійкість ІТ-підприємств. Аргументовано, що зовнішні дестабілізуючі чинники доцільно розглядати як загрози фінансовій безпеці, а внутрішні - як ризики, що можуть бути ідентифіковані та мінімізовані в межах фінансового менеджменту підприємства. Застосування PEST-аналізу дозволило ідентифікувати політичні, економічні, соціальні та технологічні зовнішні загрози, тоді як внутрішні ризики згруповано за фінансовим, кадровим, інформаційно-технологічним, інвестиційним та управлінським блоками. Це дало змогу визначити джерела порушення фінансової стійкості ІТ-підприємств і сформувати аналітичне підґрунтя для розробки механізму забезпечення їх фінансової безпеки.

7. Сформовано концептуальні засади механізму забезпечення фінансової безпеки ІТ-підприємств та визначено напрями його практичної реалізації в умовах цифрової економіки. Це здійснено через обґрунтування необхідності переходу від реактивного реагування на фінансові загрози до превентивного, адаптивного та цифровоорієнтованого управління фінансовою безпекою, а також визначення завдань, принципів, суб'єктів, об'єктів і системи забезпечення такого механізму. Функціональне наповнення механізму розкрито через методи, інструменти та важелі фінансового впливу, інтегровані з цифровими технологіями. Практичну реалізацію механізму конкретизовано

через систему заходів мікрорівня, згрупованих за стратегічним, операційним, організаційним, інноваційно-технологічним та ризикорієнтованим напрямками. Це дозволило сформулювати підхід до вибору заходів забезпечення фінансової безпеки ІТ-підприємств залежно від значення інтегрального показника та сценарію управлінського реагування.

8. Сформовано концептуальні засади механізму забезпечення фінансової безпеки ІТ-підприємств та визначено напрями його практичної реалізації в умовах цифрової економіки. Це здійснено шляхом поєднання превентивного, адаптивного та цифровоорієнтованого підходів до управління фінансовою безпекою, а також визначення мети, завдань, принципів, суб'єктів, об'єктів і системи забезпечення такого механізму. Функціональне наповнення механізму охоплює методи, інструменти та важелі фінансового впливу, інтегровані з цифровими технологіями. Напрями практичної реалізації механізму представлено системою заходів мікрорівня, згрупованих за стратегічним, операційним, організаційним, інноваційно-технологічним та ризикорієнтованим напрямками. Це дозволило обґрунтувати залежність пріоритетів забезпечення фінансової безпеки ІТ-підприємств від значення інтегрального показника та відповідного сценарію управлінського реагування.

9. Обґрунтовано напрями державної та інституційної підтримки підвищення фінансової безпеки ІТ-підприємств в умовах цифрової економіки. Це здійснено з урахуванням кореляційно-регресійного аналізу, який підтвердив залежність рівня фінансової безпеки ІТ-підприємств від макроекономічних і галузевих умов їх функціонування. Державну політику у цій сфері представлено через вектори прямого та опосередкованого впливу з визначенням відповідних методів і інструментів реалізації, спрямованих на посилення інституційно-правової, фінансової, експортної, кібербезпекової, кадрової, інноваційної та ринкової підтримки ІТ-сектору. Це дозволило конкретизувати комплекс заходів державної та інституційної підтримки, спрямованих на зміцнення фінансової стійкості, інвестиційної привабливості, експортного потенціалу та кіберстійкості ІТ-підприємств.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Акулов О. О. Ринок праці ІТ-сектору України в умовах воєнного стану та його вплив на національну економіку. *Інновації та науковий потенціал світу*. Умань, 2024. С. 23-36. URL: <https://archives.mcnd.org.ua/index.php/conference-proceeding/article/view/244/242>.
2. Алексеевська Г., Чайковська М. Трансформація ІКТ-сектору в Україні: аналіз тенденцій та стратегії сталого розвитку. *Економіка та суспільство*. 2024. № 60. DOI: <https://doi.org/10.32782/2524-0072/2024-60-98>.
3. Ананьєва О. О. Економіка підприємств ІТ-сектору: особливості аналізу. *Вчені записки Університету «КРОК»*. 2025. № 2(78). С. 51–56. DOI: <https://doi.org/10.31732/2663-2209-2025-78-51-56>.
4. Андріїв Н. М. Економічна безпека підприємства в умовах цифровізації ринку праці: теоретичні та практичні аспекти : монографія. Львів : Растр-7, 2023. 320 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/7359/1/%D0%90%D0%9D%D0%94%D0%A0%D0%86%D0%87%D0%92_%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F.pdf.
5. Ареф'єва О. В., Кузенко Т. Б. Планування економічної безпеки підприємств. Київ : Вид-во Європ. ун-ту, 2005. 170 с.
6. Ареф'єва О., Кузенко Т. Економічні основи формування фінансової складової економічної безпеки. *Актуальні проблеми економіки*. 2009. № 1. С. 98–103.
7. Ареф'єва О., Титикало В., Коваленко Н. Економічний механізм забезпечення фінансової безпеки підприємств при нестабільності зовнішнього середовища. *Адаптивне управління: теорія і практика. Серія: Економіка*. 2023. Вип. 16 (32). URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=admthp_2023_16_4.

8. Базилінська О. Я., Панченко О. І Фінансова стійкість у системі стратегічного управління підприємством. *Проблеми економіки*. 2019. №1. С. 89-94.
9. Барановський О. І. Філософія безпеки : монографія : у 2 т. Київ : УБС НБУ, 2014. / Фінансова безпека підприємств і банківських установ : монографія / за заг. ред. А. О. Єпіфанова. Суми : ДВНЗ «УАБС НБУ», 2009. 295 с.
10. Берталанфі Л. фон. Загальна теорія систем. Відень, 1968.
11. Біломістна І. І., Ковальчук А. В. Оцінка стану фінансової безпеки на основі економіко-математичного моделювання. *Науковий вісник Херсонського державного університету*. 2014. № 4. С. 28-32.
12. Біляк Ю. В. Основні загрози фінансовій безпеці корпоративних підприємств. *Агросвіт*. 2017. № 12. С. 20–30. URL: http://www.agrosvit.info/pdf/12_2017/5.pdf.
13. Блинков В. Г. Кібербезпека як ключовий елемент економічної безпеки в ІТ-секторі. *Проблеми сучасних трансформацій*. Серія: економіка та управління. 2025. № 20. DOI: <https://doi.org/10.54929/2786-5738-2025-20-03-01>.
14. Бойко І. В. Дефініції «ризик», «загроза», «небезпека» як об'єкти наукових досліджень у напрямі економічної безпеки підприємства. *Приазовський економічний вісник*. 2017. Вип. 5 (05). С. 94–98. URL: https://pev.kpu.zp.ua/journals/2017/5_05_uk/20.pdf.
15. Бондарчук Н., Гуменчук М. Сутність фінансово-економічної безпеки підприємства та необхідність її забезпечення. *Ефективна економіка*. 2016. № 11. URL: <http://www.economy.nayka.com.ua/?op=1&z=5409>.
16. Будник Л., Ронська О., Лісецька Л. Фінансова безпека держави в умовах воєнного стану. *Галицький економічний вісник*. 2022. № 4 (77). С. 138–147. URL: <https://galicianvisnyk.tntu.edu.ua/pdf/77/1100.pdf>.
17. Бутенко В. В., Музика С. Є. Фінансова безпека підприємств у контексті глобальних трансформацій і воєнного стану. *Ринкова економіка: сучасна теорія і практика управління*. 2024. Т. 23. Вип. 1 (56). С. 9-21. URL: <https://dspace.onu.edu.ua/server/api/core/bitstreams/d57cb55e-e3d8-4f46-91d7-dcfbbe96fe92/content>.

18. Вараксіна О. В., Кругова А. О. Сутність підприємницького ризику в господарській діяльності підприємства. *Економіка та суспільство*. 2021. № 4. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/217/208>.

19. Варналій З. С., Мехед А. М. Теоретико-методичні підходи до оцінки фінансової безпеки суб'єктів підприємництва. *Наукові записки Львівського університету бізнесу та права*. 2022. № 32. С. 203-211.

20. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення : монографія. Львів : Арал. 2008. 386 с.

21. Васильців Т., Шехлович А., Васильців В. Фінансово-економічні інструменти стимулювання розвитку ІТ-сфери України. *Економічний дискурс*. 2017. № 4. С. 128–136. URL: <http://ed.pdatu.edu.ua/article/view/127638>.

22. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. Київ ; Ірпінь : ВТФ «Перун», 2003. 1020 с.

23. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. Київ Ірпінь: Перун, 2005. 1728 с.

24. 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.

25. Виговська Н. Г., Полчанов А. Ю., Литвинчук І. В., Городиський М. П., Полчанов О. Ю. ІТ-бізнес як об'єкт фінансового управління. *Економіка, управління та адміністрування*. 2023. № 3(105). С. 159–165. DOI: [https://doi.org/10.26642/jen-2023-3\(105\)-159-165](https://doi.org/10.26642/jen-2023-3(105)-159-165).

26. Вівчар О. І. Практичний базис системи фінансової безпеки підприємницьких структур: нові виклики та можливості. *Сталий розвиток економіки*. 2016. № 4 (33). С. 136–142.

27. Вівчар О. Практичний базис системи фінансової безпеки підприємницьких структур: нові виклики та можливості. *Modeling the Development of the Economic Systems*. 2023. № 1. С. 8–13. DOI: <https://doi.org/10.31891/mdes/2023-7-1>.

28. Від Frontend до AI: як змінювались тренди IT-освіти в Україні за 20 років. *IT Ukraine*. 18.08.2025. URL: <https://itukraine.org.ua/vid-frontend-do-ai-yak-zminyuvalis-trendi-it-osviti-v-ukrayini-za-20-rokiv/>.

29. Від супутникового зв'язку до ШІ-асистента в Дії та оборонних технологій: підсумки Мінцифри у 2025 році. 24 грудня 2025. URL: <https://thedigital.gov.ua/news/progress/vid-shi-asystenta-v-diyi-do-suputnykovoho-zviazku-ta-oboronnykh-tekhnologiy-pidsumky-mintsyfyry-u-2025-rotsi>.

30. Вінтоняк А. А., Чубай В. М. Методики аналізу загрози банкрутства підприємств та чинники впливу на зміну її рівня. *Економіка та суспільство*. 2024. № 61. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/3761/3682>.

31. Волошина-Сідей В. В. Аналіз оцінки ризиків як інструмент сталого розвитку підприємництва в умовах глобальних викликів та коронакризи. *Приазовський економічний вісник*. 2021. № 2(25). С. 72–76. http://pev.kpu.zp.ua/journals/2021/2_25_ukr/15.pdf.

32. Газанфаров Е. М. Сутність фінансової безпеки банків та її роль у системі забезпечення фінансової безпеки держави. *Економіка та держава*. 2010. № 6. С. 62–64.

33. Геєць В. М., Кизим М. О., Клебанова Т. С. Моделювання економічної безпеки: держава, регіон, підприємство. Харків : ВД «ІНЖЕК», 2006. 240 с.

34. Голобородько А. Ю., Андрєєва О. С. Діагностика трудового потенціалу на IT-підприємствах в умовах цифровізації. *Економіка. Менеджмент. Бізнес*. 2023. № 3 (45). С. 60–70. DOI: <https://doi.org/10.31673/2415-8089.2023.036071>.

35. Горячева К. С. Оцінка рівня фінансової безпеки підприємства. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/55127/5/Horiacheva_Finansova_bezpeka.pdf;jsessionid=C01D52ED7D309F1E1D3220D2DD00C73D.

36. Губарєва І. О., Середіна Г. В. Прогнозування індикаторів фінансової безпеки України. *Економіка розвитку*. 2017. № 4. С. 38–48.

37. Данилюк І. Управління ризиками в ІТ-бізнесі. *Світ фінансів*. 2023. Вип. 3(76). С. 105–114. DOI: <https://doi.org/10.35774/sf2023.03.105>.

38. Демчишак Н., Шевчук Р., Гоменюк К. Цифрові технології та інструменти забезпечення фінансової безпеки підприємств у контексті вартісно-орієнтованого управління. *Економіка та суспільство*. 2025. № 73. DOI: <https://doi.org/10.32782/2524-0072/2025-73-53>.

39. Демчишак Н.Б., Шевчук Р.С., Онофрійчук А.О. Фінансовий потенціал розвитку підприємств інформаційно-комунікаційної сфери в умовах воєнного стану та вартісно-орієнтованого управління. *Інвестиції : практика та досвід*. 2025. № 11. DOI: <https://doi.org/10.32702/2306-6814.2025.11.67>.

40. Державна служба статистики України : офіційний вебсайт. URL: <https://www.ukrstat.gov.ua>.

41. Десятнюк О. М., Птащенко О. В. Вплив цифрових трансформацій на забезпечення фінансової безпеки підприємств в умовах глобалізації. *Світ фінансів*. 2024. Вип. 4 (81). С. 157–166. URL: <http://sf.wunu.edu.ua/index.php/sf/article/view/1754/1765>.

42. Деєва Н. Е., Делейчук В. В. Механізми залучення інвестицій емітентами в умовах розвитку цифрової економіки. *Молодий вчений*. 2018. № 1. С. 670–674. URL: <https://molodyivchenyi.ua/index.php/journal/article/view/5027>.

43. Довгань Л. Є., Козинець А. В. Розвиток ІТ-сфери: проблеми та шляхи вирішення в забезпеченні конкурентоспроможності вітчизняних підприємств. *Актуальні проблеми економіки та управління : збірник наукових праць молодих учених*. 2018. Вип. 12. URL: <https://ela.kpi.ua/handle/123456789/24607>.

44. Дранус В. В., Купчишина О. А. Особливості податкового менеджменту резидентів ДІЯ.CITY. *Ефективна економіка*. 2025. № 10. DOI: <http://doi.org/10.32702/2307-2105.2025.10.64>.

45. Дропа Я. Б. Фінансовий аналіз : навч. посіб. Львів : ЛНУ ім. Івана Франка, 2023. 238 с.

46. Дубина М. В. Механізм розвитку ринку фінансових послуг на основі інституту довіри: теорія, методологія, практика : монографія. Чернігів : ЧНТУ, 2018. 668 с.

47. Дубина М. В., Кальченко О. М., Лесун С. М. Фінансове забезпечення розвитку ІТ-компаній в Україні. *Проблеми системного підходу в економіці*. 2025. Вип. 5(102). С. 72–86.

48. Дубинська О. Визначення рівня фінансово-економічної безпеки на підставі аналізу фінансової звітності підприємства. *Таврійський науковий вісник. Серія: Економіка*. 2021. № 5. С. 112-122. DOI: <https://doi.org/10.32851/2708-0366/2021.5.14>.

49. Д'яконова І. І. Фінансова безпека як складова системи стратегічного управління підприємством. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2013. Вип. 1. С. 102–109. URL: <https://fkd.net.ua/index.php/fkd/article/view/242/242>.

50. Економіка підприємства : підручник / за заг. ред. Л. Г. Мельника. Суми : Університетська книга, 2019. 864 с. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/80106/1/Melnik_econom.pdf.

51. Експортно-кредитне агентство (ЕКА). URL: <https://me.gov.ua/Documents/MoreDetails?id=6ae94da1-5155-4ee7-a3d2-f75ac0ad1345&lang=uk-UA&title=EksportnokreditneAgentstvo-eka-&utm>.

52. Єрмошенко М. М. Безпека фінансова: Енциклопедія банківської справи України / гол. редкол. В. С. Стельмахтаїн. Київ : Молодь; ІнЮре, 2001. 680 с.

53. Єрмошенко М. М., Горячева К. С. Фінансова складова економічної безпеки: держава і підприємство : монографія. Київ : НАУ, 2010. 232 с.

54. Жахалов Я. Втрати ІТ-сектора через війну склали \$19,3 млрд. Вийшов звіт KSE про економічні збитки в Україні. *DOU*. 2024. URL: <https://dou.ua/lenta/news/IT-sector-losses-in-war/>.

55. Живко З. Б., Родченко С. С., Лелюк Н. Є. Цифрова економіка: сутність, ознаки та завдання управління. *Науковий погляд: економіка та управління*. 2022. № 2 (78). С. 31–37.

56. Загородній А. Г., Вознюк Г. Л. Фінансово-економічний словник. Київ : Знання, 2007. 1079 с.

57. Захаркіна О. О., Бойко А. В., Сокол Л. В. Цифрові технології та інструменти забезпечення фінансової безпеки бізнесу. *Проблеми сучасних трансформацій. Серія: економіка та управління*. 2023. № 10. DOI: <https://doi.org/10.54929/2786-5738-2023-10-08-02>.

58. Збитки України від війни зросли до \$170 млрд – KSE. *Фінансовий клуб*. 17 лютого 2025. URL: <https://finclub.net/news/zbytky-ukrainy-vid-viiny-zrosly-do-usd170-mlrd-kse.html>.

59. Звіт про стан інформатизації та виконання галузевих, регіональних програм, проектів, робіт з інформатизації, програм, проектів, робіт з інформатизації органів місцевого самоврядування, завдань, проектів, робіт з інформатизації Національної програми інформатизації за 2022 рік. Червень 2023. URL: <https://storage.thedigital.gov.ua/files/6/f6/9f712dc44d0bf4506ddc1e162d6f5f64.pdf>.

60. Індекси споживчих цін, 2024. *Державна служба статистики України*. 07.09.2025. URL: <https://stat.gov.ua/uk/publications/indeksy-spozhyvchykh-tsin-2024>.

61. ІТ-бізнес продовжує ухилятися від податків: деталі від Гетманцева. *Дебет-Кредит*. 2025. URL: <https://news.dtki.ua/taxation/profits-tax/102213-it-biznes-prodovzuje-uxiliatisia-vid-podatviv-detali-vid-getmanceva>.

62. ІТ-компанія: що це і чим вона займається. URL: <https://it-rating.ua/it-kompaniya-scho-tse-i-chim-vona-zaumaetsya>.

63. Кальченко О. М., Андросенко Я. С. Методичні підходи до оцінювання фінансової безпеки підприємства. *Проблеми і перспективи економіки та управління*. 2015. № 2 (2). С. 244-250. URL: <http://ppeu.stu.cn.ua/article/view/68609/63714>.

64. Кальченко О. М., Зеленська О. О., Лесун С. М. Фінансова поведінка домогосподарств у контексті розвитку поведінкових фінансів. *Проблеми і перспективи економіки та управління*. 2023. № 4(36). С. 280-290. URL: <http://ppeu.stu.cn.ua/article/view/299261>.

65. Кальченко О. М., Лесун С. М. Економіко-статистичне дослідження ефективності використання фінансових ресурсів підприємств ІТ-сфери. *Проблеми і перспективи економіки та управління*. 2025. № 1(41). С. 422-436. URL: <http://ppeu.stu.cn.ua/issue/view/19295/12492>.

66. Кальченко О. М., Лесун С. М., Кальченко М. В. Фінансовий інструментарій забезпечення фінансової безпеки ІТ-підприємств в умовах цифрової економіки. *Успіхи і досягнення у науці*. 2026. №4(26). С. 1356-1372.

67. Кальченко О. М., Шишкіна О. В. Фінансовий аналіз : навч. посіб. Чернівці : Видавець Брагинець О.В., 2018. 524 с.

68. Карбівський В. Л. Фінансова безпека аграрних підприємств в умовах цифровізації економіки. *Сталий розвиток економіки*. 2025. № 2 (53). С. 318–323. DOI: <https://doi.org/10.32782/2308-1988/2025-53-44>.

69. Карпінський Р. Ідентифікація ризиків господарської діяльності аграрних підприємств: можливості та загрози у процесі управління. *Економіка та суспільство*. 2024. № 70. DOI: <https://doi.org/10.32782/2524-0072/2024-70-189>.

70. Карчева Г. Т., Огородня Д. В., Опенько В. А. Цифрова економіка та її вплив на розвиток національної та міжнародної економіки. *Фінансовий простір*. 2017. № 3 (27). С. 13–21.

71. Качинський А. Б. Екологічна безпека України: системний аналіз перспектив покращення. К.: НІСД. 2001. 312 с.

72. КВЕДи для ІТ. URL: <https://itaccounting.com.ua/kvedi>.

73. Кладницька Т., Катаєва С. Інноваційні методи оптимізації фінансової роботи на підприємстві. *Сталий розвиток економіки*. 2025. № 4 (51). С. 355–360. DOI: <https://doi.org/10.32782/2308-1988/2024-51-50>.

74. Класифікація видів економічної діяльності : наказ Держспоживстандарту України від 11.10.2010 № 457. URL: <https://zakon.rada.gov.ua/rada/show/vb457609-10#Text>.

75. Кліпкова О. І. Фінансовий розвиток: конвергенція чи дивергенція. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2021. № 2(37). URL: <https://fkd.net.ua/index.php/fkd/article/view/3813>.

76. Князєв М. В. Системний аналіз: методологія та застосування. Київ : Наукова думка, 2005. 240 с.

77. Ковтуненко Ю. В., Дукіна Д. М. Проблеми та перспективи розвитку вітчизняних підприємств ІТ-сфери на міжнародних ринках в умовах глобальних ризиків. *Економічний журнал Одеського політехнічного університету*. 2024. № 3(29). С. 20–26. DOI: <https://doi.org/10.15276/EJ.03.2024.3>.

78. Ковтуненко Ю. В., Дукіна Д. М. Проблеми та перспективи розвитку підприємств ІТ-сфери на міжнародних ринках. *Економічний журнал Одеського політехнічного університету*. 2024. № 3(29). С. 20–26. DOI: <https://doi.org/10.15276/EJ.03.2024.3>.

79. Козаченко Г. В., Пономарьов В. П., Ляшенко О. М. Економічна безпека підприємства: сутність та механізм забезпечення : монографія. Київ : Лібра, 2003. 280 с.

80. Коленда Н. В. Поняття соціально-економічної безпеки підприємства. *Економіка і суспільство*. 2016. № 7. С. 672–678. URL: <https://evnuir.vnu.edu.ua/bitstream/123456789/12361/3/113.pdf>.

81. Коляда О., Рожик Р., Бокочей Б. Основи системного аналізу об'єктів і процесів комп'ютерного моделювання : навч. посіб. Вінниця : ВНТУ, 2013. 135 с.

82. Кононова І. В. Підходи до трактування фінансової безпеки підприємства. *Бізнес-навігатор*. 2021. № 6(67). С. 7–10.

83. Копитко М. І. Комплексне забезпечення економічної безпеки підприємств : дис. ... д-ра екон. наук : 21.04.02 / Університет економіки і права «КРОК». Київ, 2015. 478 с. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/421/1/%d0%9a%d0%be%d0%bf%d0%b8%d1%82%d0%ba%d0%beDis.pdf>.

84. Кораблінова І. А., Кульбацька Н. М. Актуальні проблеми дослідження ІТ-ринку України. *Ефективна економіка*. 2017. № 12. URL: <http://www.economy.nayka.com.ua/?op=1&z=5997>.

85. Коссе І., Бетлій О., Кравчук В. Дія.City: оцінка впливу на показники економічного і соціального розвитку та його ефективності / Міністерство економіки України. 2024. URL: <https://me.gov.ua/download/ef2cc7be-d44e-47cf-ac14-f1d8490a5f92/file.pdf>.

86. Костюнік О. В., Дергалюк М. О., Щепіна Т. Г. Погребняк А. Ю. Формування системи фінансової безпеки Іт-підприємств в умовах становлення цифрової економіки. Інвестиції: практика та досвід. 2025. № 21. С 52-59. DOI: <https://doi.org/10.32702/2306-6814.2025.21.52>.

87. Кракос Ю. Б., Разгон Р. О. Управління фінансовою безпекою підприємств. *Економіка та управління підприємствами машинобудівної галузі: проблеми теорії та практики*. 2008. № 1. С. 86–97.

88. Краус Н. М., Голобородько О. П., Краус К. М. Цифрова економіка: тренди та перспективи авангардного характеру розвитку. *Ефективна економіка*. 2018. № 1. URL: http://www.economy.nauka.com.ua/pdf/1_2018/8.pdf.

89. Криниця С., Тригуб Ю. Методичні підходи до діагностики фінансової безпеки підприємства з урахуванням фактору конкурентоспроможності. *Socio-Economic Relations in the Digital Society*. 2020. № 3(39). С. 79–84. DOI: [https://doi.org/10.18371/2221-755X3\(39\)2020225583](https://doi.org/10.18371/2221-755X3(39)2020225583).

90. Крутова А. С., Ставерська Т. О., Шевчук І. Л. The problems of the enterprises' financial security. *Економічна стратегія і перспективи розвитку сфери торгівлі та послуг*. 2015. Вип. 1. С. 93–105. URL: <https://repo.btu.kharkiv.ua/server/api/core/bitstreams/22672876-1eb6-437d-a97b-73e429e63b9b/content>.

91. Кужелєв М. О. Особливості діяльності ІТ-підприємств України. *Сталий розвиток економіки*. 2025. № 5(56). С. 101–106. DOI: <https://doi.org/10.32782/2308-1988/2025-56-14>.

92. Кузенко Т. Б., Мартюшева Л. С., Грачов О. В., Литовченко О. Ю. Фінансова безпека підприємства : навчальний посібник. Харків : Вид. ХНЕУ, 2010. 304 с.

93. Кузенко Т. Б., Сабліна Н. В. Фінансова безпека підприємства : навч. посіб. Харків : ХНЕУ ім. С. Кузнеця, 2020. 123 с. URL: <https://files.znu.edu.ua/files/Bibliobooks/Inshi78/0058646.pdf>.

94. Кульпінський С. Роль фінансової безпеки України в поглибленні інтеграційних стосунків з європейськими країнами. *Фінансова консультація*. 2015. № 5. С. 34–35.

95. Кульчицький І. І. Цифрова економіка та економічна безпека підприємства: стратегії управління. *Актуальні питання економічних наук*. 2024. № 6. DOI: <https://doi.org/10.5281/zenodo.14575016>.

96. Куцик В. І., Бартиш А. І. Фінансова безпека підприємства як самостійний об'єкт управління: проблеми забезпечення. *Науковий вісник НЛТУ України*. 2011. Вип. 21.4. С. 250–255.

97. Лаговська О. А., Лоскоріх Г. Л. Класифікація ІТ-підприємств: обліковий аспект. URL: http://www.psae-jrnl.nau.in.ua/journal/1_69_2_2019_ukr/18.pdf.

98. Лазарева А. П. Стратегія фінансової безпеки підприємства. *Економічний аналіз*. 2014. Т. 18, № 2. С. 166–172. URL: <https://library.wunu.edu.ua/images/stories/naukovi%20zhurnaly/economichnyy%20analiz/2014/document18-2.pdf>.

99. Лазебник Л. Л. Аналіз дефініцій поняття фінансових механізмів. *Наукові праці НДФІ*. 2005. Вип. 4 (33). С. 96–103. URL: https://npndfi.org.ua/docs/NP_05_04_096_uk.pdf.

100. Лесун С. М. Соціально-філософський контекст управління фінансовими ризиками. *Юність науки – 2024: соціально-економічні та гуманітарні аспекти розвитку суспільства* : збірник тез доповідей XIV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 24-26 квітня 2024 р.). Чернігів : НУ «Чернігівська політехніка», 2024. С. 635–638. URL: <https://ir.stu.cn.ua/handle/123456789/30262>.

101. Лесун С. М. Фінансова безпека підприємств в умовах становлення цифрової економіки. *Сучасні критерії оцінки ефективності господарських процесів в нестабільних економічних умовах* : матеріали Всеукр. наук.-практ. конф. (Чернігів, 12 листопада 2024 р.). Чернігів : Коледж транспорту та комп'ютерних технологій НУ «Чернігівська політехніка», 2024. С. 220-222.

102. Лесун С. М. Фінансова безпека підприємств та її особливості в умовах цифрової економіки. *Проблеми і перспективи економіки та управління*. 2024. № 3(39). С. 341–352. URL: <http://ppeu.stu.cn.ua/article/view/319324>.

103. Лесун С.М. Цифрова економіка та фінансова безпека: роль інформаційних технологій. *Фінансово-управлінські інновації як драйвер сталого розвитку в умовах сучасних викликів* : матеріали Міжнародної науково-практичної конференції. (м. Хмельницький, 7 листопада 2025 року). Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2025. Ч. 1. С. 360-363.

104. Лінгур Л. Прогнозування розвитку продуктового ІТ-ринку в Україні. *Економіка та суспільство*. 2025. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/5606>. 99

105. Лоскоріх Г. Л. Обліково-аналітичне забезпечення діяльності підприємств сфери ІТ : дис. ... д-ра філософії : 071. Житомир, 2021. 231 с.

106. Лоскоріх Г. Л. Характерні риси діяльності ІТ-підприємств: обліковий аспект. *Проблеми системного підходу в економіці*. 2021. № 3(83). С. 72-77. URL: http://www.psae-jrnl.nau.in.ua/journal/3_83_2021_ukr/12.pdf.

107. Луговець Б. Облікове забезпечення розвитку підприємств ІТ-сфери у військовий час. *Економіка та суспільство*. 2025. № 76. DOI: <https://doi.org/10.32782/2524-0072/2025-76-54>.

108. Лункіна Т., Дранус Л., Дранус В., Сметана А. (2023) Управління експортоорієнтованою стратегією сучасної ІТ-сфери. *Аграрна економіка*. 2024 Т. 17, № 1. С. 103-112. URL: <https://agrarianeconomy.lnup.edu.ua/index.php/en/archive/68-arkhiv-nomeriv/2024-t-17-1/557-10> 11.

109. Лютик Т. В. Функція бажаності Харрінгтона як інструмент інтегральної оцінки інноваційної та науково-технологічної складових економічного потенціалу. *Історія науки і біографістика*. 2016. № 4. URL: http://nbuv.gov.ua/UJRN/INB_Title_2016_4_11.

110. Майбутнє українського ІТ: між збереженням талантів і європейськими законами : офіційний вебсайт Асоціації «IT Ukraine». 21.10.2025. URL: <https://itukraine.org.ua/majbutnye-ukrayinskogo-it-mizh-zberezhennyam-talantiv-i-yevropejskimi-zakonami/>.

111. Макаrchук І. М., Малишко В. В., Яременко Л. М. Фінансова безпека підприємств: характерні ознаки, складові, основні загрози й небезпеки. *Економічний вісник університету*. 2023. Вип. 56. С. 183-193.

112. Марова С. Ф. Управління безпекою життєдіяльності : монографія. Донецьк: Вебер, 2009. 344 с.

113. Марусяк Н. Л., Бак Н. А. Фінансова безпека підприємства та загрози її втрати в сучасному економічному середовищі. *Економіка та держава*. 2022. № 2. С. 109–113. URL: http://www.economy.in.ua/pdf/2_2022/20.pdf.

114. Марченко О. М. Концептуальні засади управління фінансовою безпекою підприємства. *Вісник Львівського університету*. Серія економічна. 2003. Вип. 32. С. 104–110.

115. Марченко О. Цифрова економіка в Україні: основні тенденції та перспективи розвитку. *Galician Economic Journal*. 2020. № 4 (65). С. 34–39.

116. Медведєва І. Б., Погосова М. Ю. Діагностування безпеки промислового підприємства у трирівневій системі фінансових відносин: монографія. Харків : Видавництво ХНЕУ, 2011. 264 с. URL: https://repository.hneu.edu.ua/jspui/bitstream/123456789/3459/1/%D0%9C%D0%B5%D0%B4%D0%B2%D0%B5%D0%B4%D0%B5%D0%B2%D0%B0_%D0%9F%D0%BE%D0%B3%D0%BE%D1%81%D0%BE%D0%B2%D0%B0.pdf.

117. Мельник М. І. Інституційне забезпечення розвитку ІТ-сектору в Україні. *Регіональна економіка*. 2018. № 1. С. 102–110. URL: https://re.gov.ua/re201801/re201801_102_MelnykMI.pdf.

118. Мельник Н. В. Управління фінансовою безпекою підприємства на засадах бенчмаркінгу. *Національний університет харчових технологій* : [сайт]. URL: <https://dspace.nuft.edu.ua/server/api/core/bitstreams/eb3d3dc5-fc50-4a0e-8eb4-3a084a0d71fd/content>.

119. Мельник С. І. Дослідження викликів, ризиків, загроз та небезпеки в системі забезпечення фінансової безпеки підприємства. *Проблеми системного підходу в економіці*. 2019. Вип. 4 (72). С. 172–177. DOI: <https://doi.org/10.32782/2520-2200/2019-4-25>.

120. Механізми та функціонально-структурні інструменти забезпечення конкурентоспроможності національної економіки в умовах сучасних загроз економічної безпеки : монографія / за ред. Т. Г. Васильціва, Р. Л. Лупака. Львів : АТБ, 2019. 552 с. URL: https://www.lute.lviv.ua/fileadmin/www.lac.lviv.ua/data/kafedry/Ekonomiky/Docs/2019_MonogLupakVas_1.pdf.

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

122. Мисник Т. Г. Теоретико-методичні основи фінансової безпеки підприємств. *Вісник ХНАУ*. Серія: Економічні науки. 2017. № 2. С. 91–98.

123. Михалків А., Булезюк В. Фінансова стійкість підприємства з позиції системного підходу. *Grail of Science*. 2023. № 33. С. 66–71. DOI: <https://doi.org/10.36074/grail-of-science.10.11.2023.09>.

124. Мініна О., Поцелуйко І., Олійник С. Формування системи фінансової безпеки ІТ-підприємств: ідентифікація ключових компонентів в умовах цифрової економіки. *Економіка та суспільство*. 2026. № 83. DOI: <https://doi.org/10.32782/2524-0072/2026-83-50>.

125. Мініна О., Шадура-Никипорець Н., Мойсеєнко К. Цифрова економіка як основа інноваційної моделі повоєнної відбудови підприємств України. *Проблеми і перспективи економіки та управління*. 2025. № 4 (44). С. 39–47. DOI: [https://doi.org/10.25140/2411-5215-2025-4\(44\)-39-47](https://doi.org/10.25140/2411-5215-2025-4(44)-39-47).

126. Мінцифри: Україна — четверта країна в Європі за рівнем підтримки стартапів / Міністерство цифрової трансформації України. 21 лютого 2025 року. URL: <https://www.kmu.gov.ua/news/mintsyfry-ukraina-chetverta-kraina-v-ievropi-za-rivnem-pidtrymky-startapiv>.

127. Міщенко В. І. Перспективи розвитку ІТ-сектору та цифрової інфраструктури України. *Науковий вісник УжНУ*. 2022. № 43. С. 105–111. DOI: <https://doi.org/10.32782/2413-9971/2022-43-18>.

128. Могиліна Л. А. Управління фінансовою безпекою підприємств в умовах економічної нестабільності : автореф. дис. ... канд. екон. наук : 08.00.08. Суми, 2015. 24 с.

129. Мосорко А. Атаки не стихають, донори зникають: як еволюціонує ринок кібербезпеки в Україні. Дані свіжого дослідження. *Mind.ua*. 21 квітня 2025. URL: <https://mind.ua/publications/20288157-ataki-ne-stihayut-donori-znikayut-yak-evolyucionue-rinok-kiberbezpeki-v-ukrayini-dani-svizhog>.

130. Мунтіян В. І. Економічна безпека України : підручник. Київ : КВІЦ, 1999. 464 с.

131. Мунько А. Ю. Кібербезпека як складник політики фінансової безпеки держави. *Фінанси України*. 2023. № 5. URL: <https://reicst.com.ua/pmtl/article/view/2023-7-02-09>.

132. На 0,1% більше, ніж торік: яким був експорт ІТ-послуг у першому півріччі 2025 року. *Lviv IT Cluster*. 2025. URL: <https://itcluster.lviv.ua/na-01-bilshe-nizh-torik-yakym-buv-eksport-it-poslug-u-pershomu-pivrichchi-2025-roku/>.

133. Назаренко Я. Я., Теслюк Н. П. Концепція забезпечення фінансової безпеки підприємств пасажирського транспорту в умовах воєнного стану. *Актуальні питання економічних наук*. 2025. DOI: <https://doi.org/10.5281/zenodo.14978001>.

134. Наконечна О., Михайлик О. Фінансова безпека підприємства в цифровому середовищі. *Економіка та право: глобальна трансформація* : міжнар. колект. монографія. Київ : Наукова столиця, 2021. С. 59–90. URL: <https://dspace.nuft.edu.ua/handle/123456789/39688>.

135. Національний банк і далі пом'якшує валютні обмеження. *Національний банк України*. 18 вер. 2025. URL: <https://bank.gov.ua/ua/news/all/natsionalniy-bank-i-dali-pomyakshuye-valyutni-obmejennya>.

136. Національний банк переглянув граничні строки розрахунків для деяких експортно-імпортних операцій. *Національний банк України*. 10 лип. 2024. URL: <https://bank.gov.ua/ua/news/all/natsionalniy-bank-pereglyanuv-granichni-stroki-rozrahunkiv-dlya-deyakh-eksportno-importnih-operatsiy>.

137. Національний банк України : офіційний вебсайт. URL: <https://bank.gov.ua/>.

138. Несенюк А. Найнижчий показник за останнє десятиріччя: у 2024-му частка новачків в ІТ опустилася до 24%. *Forbes Ukraine*. 2024. URL: https://forbes.ua/news/naynizhchiy-pokaznik-za-ostanne-desyatirichchya-u-2024-mu-chastka-novachkiv-v-it-opustilasya-do-24-dou-09092024-23495?utm_source=chatgpt.com.

139. Орехова К. В. Забезпечення фінансової безпеки підприємства: теорія, методологія, практика : дис. ... д-ра екон. наук : 08.00.08 / Сумський державний університет. Суми, 2025. 627 с. URL: <https://essuir.sumdu.edu.ua/handle/123456789/100721>.

140. Остафієва О. Внутрішній фронт: як ІТ-ринок України бореться за виживання та чому не варто очікувати зростання зарплат найближчими роками. *ProIT: media для профі в ІТ*. URL: <https://proit.ua/vnutrishnii-front-iaak-it-rinok-ukrayini-borietsia-za-vizhivannia-ta-chomu-nie-varto-ochikuvati-zrostannia-zarplat-naiblizhchimi-rokami/>.

141. Офіційний сайт Державної служби статистики України. URL: <https://www.ukrstat.gov.ua>.

142. Павлова О. М., Павлов К. В., Демчук Н. В., Дмитрук І. Я. Роль сучасних інформаційно-комунікаційних технологій в управлінні підприємством. *Міжнародний науковий журнал «Інтернаука»*. 2021. № 18. DOI: <https://doi.org/10.25313/2520-2057-2021-18>.

143. Павлова О., Новосад О., Мурзіна А. Розвиток підприємництва у сфері ІТ-бізнесу за умов змін та комунікацій. *Актуальні проблеми інноваційної економіки та права*. 2024. № 2. С. 124-130. DOI: <https://doi.org/10.36887/2524-0455-2024-2-23>.

144. Пантелєєва Н. М. Фінансова безпека в умовах цифрової економіки: очікування і реальність. *Економіка та держава*. 2020. № 8. DOI: [https://doi.org/10.18371/fp.2\(38\).2020.209289](https://doi.org/10.18371/fp.2(38).2020.209289).

145. Панченко В. А. Управління фінансово-економічними результатами підприємств ІТ-сектора. *Проблеми економіки*. 2023. № 1. С. 105–110. URL: <http://jnas.nbu.gov.ua/article/UJRN-0001417950>.

146. Панченко О. І., Кальченко О. М., Лесун С. М. Банкостраховання як основа стабільності фінансового ринку. *Юність науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства* : збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 26-27 квітня 2023 р.). Чернігів : НУ «Чернігівська політехніка», 2023. С. 117-118.

147. Панченко О. І., Кальченко О. М., Лесун С. М. Проблеми розвитку сучасної системи ризик-менеджменту в банківських установах. *Юність науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства* : збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 26-27 квітня 2023 р.). Чернігів : НУ «Чернігівська політехніка», 2023. С. 118-120. URL: <https://stu.cn.ua/wp-content/uploads/2023/11/zbirnyk-tez-yunist-nauky-2023.pdf>.

148. Панченко О. І., Лесун С. М. Методичні підходи до оцінки рівня фінансової безпеки підприємств ІТ-сфери. *Проблеми і перспективи економіки та управління*. 2025. № 3(43). С. 347-358.

149. Панченко О. І., Лесун С. М. Особливості страхування фінансових ризиків банківських установ. *Фінансове та інформаційно-аналітичне забезпечення безпеки бізнесу в умовах воєнної економіки та повоєнного відновлення* : матеріали XII Міжнар. наук.-практ. конф., Харків, 22–23

листопада 2023 р. Харків : ХНУМГ ім. О. М. Бекетова, 2023. С. 220-222. URL: https://eprints.kname.edu.ua/64334/1/%D0%9A%D0%9E%D0%9D%D0%A4%D0%95%D0%A0%D0%95%D0%9D%D0%A6%D0%98%D0%AF%20%D0%A2%D0%B5%D0%B7%D0%B8%D1%81%D0%B8_2023_2.pdf.

150. Панченко О.І., Лесун С. М. Специфіка підприємств ІТ-сфери як об'єкта фінансового управління. *Юність науки – 2025* : збірник тез доповідей XV Міжнародної науковопрактичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 23-25 квітня 2025 р.). Чернігів : НУ «Чернігівська політехніка», 2025. С. 78-80. URL: <https://ir.stu.cn.ua/items/7024c8b0-86f3-4ff4-baa0-3548f8c61574>.

151. Папінко А. І. Економічна безпека та управління бізнес-процесами в ІТ-підприємствах. *Економічний аналіз*. 2023. Т. 33, № 4. С. 271–279. DOI: <https://doi.org/10.35774/econa2023.04.271>.

152. Пащенко О. В., Базик О. В. Сучасні тренди та перспективи розвитку ІТ-сектору України. *Ефективна економіка*. 2024. № 9. DOI: <https://doi.org/10.32702/2307-2105.2024.9.45>.

153. Підтримати Збройні Сили України та постраждалих від російської агресії. *НБУ*. URL: <https://bank.gov.ua>.

154. Пластун О. Л. Система фінансової безпеки суб'єктів підприємництва. *Вісник Сумського національного аграрного університету*. 2007. № 1. С. 100–107. URL: <http://essuir.sumdu.edu.ua/handle/123456789/54680>.

155. Податкові зміни для резидентів Дія Сіті з 1 січня 2025 року. *7eminar*. 29.01.2025. URL: <https://7eminar.ua/news/3460-podatkovyi-zmini-dlya-rezidentiv-diya-siti-z-1-sicnya-2025>.

156. Подольчак Н. Ю., Білик О. І., Левицька Я. В. Сучасний стан цифровізації в Україні. *Ефективна економіка*. 2019. № 10. URL: http://www.economy.nayka.com.ua/pdf/10_2019/6.pdf.

157. Пойда-Носик Н. Н. Науково-методичні підходи до оцінки рівня фінансової безпеки підприємства. *Теоретичні і практичні аспекти економіки та інтелектуальної власності* : збірник наукових праць : у 3 т. 2013. Вип. 1, т. 1. С. 88–292. URL: <https://journals.uran.ua/index.php/2225-6407/article/view/16019>.

158. Пойда-Носик Н. Н. Сутність фінансової безпеки суб'єктів підприємництва та її роль в забезпеченні національної економічної безпеки. *Вісник ЖДТУ. Серія: Економічні науки*. 2011. № 1 (55). С. 340–342.

159. Пойда-Носик Н. Н. Фінансова безпека акціонерних товариств: теоретико-методологічний та практичний аспекти системного підходу : монографія. Чернігів: ЧНТУ, 2020. 304 с. URL: https://nubip.edu.ua/sites/default/files/u295/poyda-nosik_monografiya_2020.pdf.

160. Політологічний енциклопедичний словник / упоряд. В. П. Горбатенко ; за ред. Ю. С. Шемшученка, В. Д. Бабкіна, В. П. Горбатенка. 2-ге вид., допов. і переробл. Київ : Генеза, 2004. 736 с.

161. Полтініна О. П. Забезпечення фінансової безпеки суб'єктів підприємництва на засадах контролінгу : автореф. дис. ... канд. екон. наук : спец. 08.00.08 «Гроші, фінанси і кредит». Харків, 2013. 21 с.

162. Попко О. В. Стратегічний маркетинговий аналіз ринку ІТ-послуг в Україні. *Економіка та суспільство*. 2024. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/5520/5458>.

163. Портрет айтивця 2024. Як змінилося українське ІТ за 10 років. *DOU*. 2024. URL: https://dou.ua/lenta/articles/portrait-2024/?from=recent_pinned#companies.

164. Портрет ІТ-спеціаліста 2025. *DOU*. 2025. URL: <https://dou.ua/lenta/articles/portrait-2025/>.

165. Правдюк Н. Л., Мулик Т. О., Мулик Я. І. Управління фінансовою безпекою підприємств: обліково-аналітичний аспект : монографія. Київ : Центр учбової літератури, 2019. 224 с.

166. Про авторське право і суміжні права : Закон України від 01.12.2022 № 2811-IX. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#Text>.

167. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 18.06.2024 № 3788-IX (законопроект 4336-20). URL: <https://zakon.rada.gov.ua/laws/show/4336-20#Text>.

168. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.

169. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

170. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.

171. Про стимулювання розвитку цифрової економіки в Україні : Закон України від 15.07.2021 № 1667-IX. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/1667-20#Text>.

172. Про Стратегію інформаційної безпеки : Указ Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n5>.

173. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки : Розпорядження Кабінету Міністрів України від 17 січ. 2018 р. № 67-р. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text>.

174. Прокопишин О. С., Дранус Л. С., Дранус В. В. Стратегічна стійкість підприємств електронної комерції в умовах глобальної цифрової трансформації. *Ефективна економіка*. 2024. № 9. DOI: <http://doi.org/10.32702/2307-2105.2024.9.32>.

175. Процикевич К. І. Організаційно-економічний механізм реалізації потенціалу високотехнологічних стартапів у сфері інформаційно-комунікаційних технологій : дис. ... д-ра філософії : 051. Львів, 2025. 269 с. URL: https://www.lute.lviv.ua/fileadmin/www.lac.lviv.ua/data/pidrozdily/Aspirantura/Rady/Spec_vchena_rada/Robota_razovikh_specializovanikh_vchenikh_rad/2025/PROCIKEVICH_Kseniji_Igorivni/Disertacija_Procikevich_K_Do_zakhistu.pdf.

176. Пшик Б. І. Формування системи фінансової безпеки суб'єктів підприємництва як основи стабільного їх функціонування. *Ефективна економіка*. 2021. № 9. URL: <http://www.economy.nayka.com.ua/?op=1&z=9270>.

177. Радєв Д. В. Сутність та змістоутворювальні ознаки цифрової економіки у контексті інституціоналізму. *Підприємництво та торгівля*. 2021. № 31. С. 27–34. URL: <http://journals-lute.lviv.ua/index.php/pidpr-torgi/article/view/1492>.

178. Рахман М. С., Корабельський С. О. ІТ-галузь в очах світової спільноти. *Економіка. Інформаційні технології в економіці*. 2020. № 7. С. 181–188.

179. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур : монографія. Львів : ЛБІ НБУ, 2004. 195 с.

180. Рубаха М., Ткачик Л., Приймак І., Демчишак Н., Юрків Р. Факторний аналіз фінансової результативності та формування стратегічної стійкості українських ІТ-компаній в умовах викликів війни. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2024. Т. 1. № 54. С. 260–281. DOI: <https://doi.org/10.55643/fcaptp.1.54.2024.4229>.

181. Руденко В. В., Погріщук Г. Б. Ідентифікація змісту та класифікаційних ознак загроз і ризиків фінансовій безпеці підприємства. *Modern Economics*. 2023. № 41. С. 105–112. DOI: [https://doi.org/10.31521/modecon.V41\(2023\)-15](https://doi.org/10.31521/modecon.V41(2023)-15).

182. Рудзінська В. Які державні програми спрямовані на захист критичної цифрової інфраструктури в 2025 році. *Speka*. 1 квітня 2025. URL: <https://speka.ua/business/yaki-derzavni-programi-spryamovani-na-zaxist-kriticnoyi-cifrovoyi-infrastrukturi-v-2025-roci-v45m7o>.

183. Рудзінська В. Які державні програми зміцнюють кіберзахист України у 2025 році? *SPEKA – інтернет-видання про підприємництво та технології, бізнес-тренди, інновації та розвиток ІТ*. 1 квітня 2025. URL: <https://speka.ua/business/yaki-derzavni-programi-spryamovani-na-zaxist-kriticnoyi-cifrovoyi-infrastrukturi-v-2025-roci-v45m7o>.

184. Сабадишина Ю. «Кожен місяць першого кварталу є гіршим, аніж цей період торік». Що відбувається з українським ІТ-експортом. *DOU.ua*. 6 травня 2024. URL: <https://dou.ua/lenta/articles/it-export-1-quarter-2024/>.

185. Ситник Н. С., Джиговська Л. І. Методика оцінювання рівня фінансової безпеки підприємства: зміст та функціональні складники. *Причорноморські економічні студії*. 2019. № 46/2. С. 65-70. URL: <https://financial.lnu.edu.ua/wp-content/uploads/2015/10/13.pdf>.

186. Сімагін Д. У 2024 році іноземці відкрили в Україні 109 ІТ-компаній. *Highload*. 2024. URL: <https://highload.tech/uk/u-2024-rotsi-inozemtsi-vidkryly-v-ukrayini-109-it-kompanij>.

187. Скільки айтівців в Україні: рекордна кількість закритих ІТ-ФОПів за рік. *DOU*. 2025. URL: <https://dou.ua/lenta/articles/how-many-devs-in-ukraine-2025/>.

188. Скільки податків сплачують ІТ-фахівці. Інфографіка. *DOU*. 2025. URL: <https://dou.ua/lenta/articles/how-much-taxes-it-companies-pay/>.

189. Словник української мови : в 11 т. / АН УРСР, Ін-т мовознавства ім. О. О. Потебні ; редкол.: І. К. Білодід (голова) та ін. Київ : Наукова думка, 1978. Т. 9. 203 с.

190. Смагло О. В. Сучасний стан розвитку ринку фінансових технологій. *Цифрова економіка та економічна безпека*. 2023. № 6(06). С. 17–21.

191. Соляник Л. Г., Штефан Н. М., Ніколаєнко А. О. Fintech-інструменти для прогнозування банкрутства: інтеграція традиційних та інноваційних підходів. *Економічний вісник Дніпровської політехніки*. 2023. № 2. С. 128-135. URL: https://ev.nmu.org.ua/docs/2023/2/EV20232_128-135.pdf.

192. Стащук О. В., Шикун В. В. Фінансова безпека суб'єктів господарювання сектора малого підприємництва. *Економічний часопис Волинського національного університету імені Лесі Українки*. 2024. № 1(37). С. 105–110. DOI: <https://doi.org/10.29038/2786-4618-2024-01-105-110>.

193. Степаненко Р. Д., Мануйлов О. В. Сучасні ризики та загрози фінансово-економічної безпеки в умовах глобалізації. *Актуальні проблеми інноваційної економіки та права*. 2024. № 3. С. 75–80. URL: <https://repo.btu.kharkov.ua/handle/123456789/55905>.

194. Стець С. Управлінські зміни в ІТ компаніях України в умовах трансформацій. *Економіка та суспільство*. 2025. № 71. DOI: <https://doi.org/10.32782/2524-0072/2025-71-118>.
195. Судакова О. І. Стратегічне управління фінансовою безпекою підприємства. *Економічний простір*. 2008. № 9. С. 140–148.
196. Сукрушева Г. О., Коляда К. В. Теоретична сутність фінансової безпеки суб'єкта господарювання. *Науковий вісник Миколаївського національного університету імені В. О. Сухомлинського. Економічні науки*. 2018. Вип. 23. С. 560–562. URL: <http://global-national.in.ua/archive/23-2018/108.pdf>.
197. Сутність фінансової безпеки як об'єкта аналізу. *Світ фінансів*. 2023. № 4(73). С. 184–192. URL: <http://sf.wunu.edu.ua/index.php/sf/article/view/1561>.
198. Тимошенко Н. Ю., Ронський Б. Ю. Проблеми та перспективи розвитку ІТ-індустрії. *Економіка і суспільство*. 2018. № 17. С. 384–388. DOI: <https://doi.org/10.32782/2524-0072>.
199. Тимощенко К. С. Фінансовий механізм фінансової безпеки суб'єктів підприємництва : дис. ... канд. екон. наук : 08.00.08 / Дніпропетровський національний університет імені Олеся Гончара. Дніпропетровськ, 2015. 219 с.
200. Тітенко З. Інноваційна складова фінансової безпеки підприємств. *Економіка та суспільство*. 2023. № 48. DOI: <https://doi.org/10.32782/2524-0072/2023-48-14>.
201. Ткачик Л., Рубаха М., Пайтра Н., Демчишак Н., Ознамець В. Дослідження ІТ-бізнесу в Україні: тенденції, прогнози та стратегії розвитку. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2023. Т. 5, № 52. С. 353–368. DOI: <https://doi.org/10.55643/fcaptp.5.52.2023.4128>.
202. Топ-50 ІТ-компаній України, літо 2025: перша стабільність за роки війни і вже дві продуктові компанії у «великій п'ятірці». *DOU*. 11 серпня 2025. URL: <https://dou.ua/lenta/articles/top-50-summer-2025/>.
203. Туліка Н. М. Роль ІТ-індустрії у формуванні цифрової економіки України. *Вісник Львівського торгово-економічного університету. Серія: Економічні науки*. 2025. № 83. DOI: <https://doi.org/10.32782/2522-1205-2025-83-29>.

204. Тульчинський Р., Костюнік О., Красношопка В., Погребняк А. Стратегічний підхід до управління фінансовою безпекою підприємств в умовах формування соціальної економіки. *Вісник Хмельницького національного університету. Серія: Економічні науки*. 2024. Том 330, № 3. С. 190-194.

205. Українська техгалузь на четвертий рік війни: стабілізація, нові стратегії та зміна архітектури ринку – результати IT Research Ukraine 2025. Від адаптації до перебудови. *Lviv IT Cluster*. 11 Грудня, 2025. URL: <https://itcluster.lviv.ua/ukrayinska-tehgaluz-na-chetvertyj-rik-vijny-stabilizacziya-novi-strategiyi-ta-zmina-arhitektury-rynku-rezultaty-it-research-ukraine-2025-vid-adaptacziyi-do-perebudovy/>.

206. Український інвестиційний ландшафт: ретроспектива буремного десятиріччя. *InVenture*. 2024. URL: <https://inventure.com.ua/uk/analytics/investments/ukrayinskij-investicijnij-landshaft:-retrospektiva-buremnogo-desyatirichchya>.

207. Український фонд стартапів : офіційний вебсайт. URL: <https://usf.com.ua/>.

208. Управління фінансово-економічною безпекою : навч. посіб. / О. А. Кириченко, С. М. Лаптев, П. Я. Пригунов, О. І. Захаров та ін. ; за ред. В. С. Сідака. Київ : Дорадо-Друк, 2010. 480 с.

209. Устінов Я., Ільчук В. Ландшафт фінансування розвитку ІТ-індустрії в Україні. *Грааль науки*. 2023. № 33. С. 32–42. DOI: <https://doi.org/10.36074/grail-of-science.10.11.2023.03>.

210. Федорович І. М., Рудич В. С. Інноваційні технології у забезпеченні фінансової безпеки підприємств реального сектора економіки. *Інвестиції: практика та досвід*. 2025. № 2. С. 165–172. URL: <https://www.nayka.com.ua/index.php/investplan/article/view/5489>.

211. Фінансова безпека банку. *Мислене древо*. URL: <https://myslenedrevo.com.ua/uk/Sci/Economics/CorporateRelationsBank/4/1.html>.

212. Фісуненко П., Берестюк М. Систематизація поглядів на сутність поняття «цифрова економіка». *Сталий розвиток економіки*. 2025. № 4 (55). С. 556–563. DOI: <https://doi.org/10.32782/2308-1988/2025-55-75>.
213. Франчук В. І. Економічна безпека суб'єктів господарської діяльності : підруч. Львів : ЛьвДУВС, 2015. 236 с.
214. Фучеджи В. І. Характеристика структурних елементів фінансової безпеки суб'єктів підприємництва. *Ефективна економіка*. 2013. № 12. URL: <http://www.economy.nayka.com.ua>.
215. Хижняк Ю. О. Методичний підхід до оцінки рівня фінансової безпеки підприємства. *Інфраструктура ринку*. 2018. № 23. С. 305-312.
216. Цвігун Т. В. Економічна безпека в системі національної безпеки України. *Економіка і суспільство*. 2017. Вип. 11. С. 150–156. URL: https://economyandsociety.in.ua/journals/11_ukr/24.pdf.
217. Цифрова освіта : проєкт Міністерства цифрової трансформації України : офіційний вебсайт. URL: <https://thedigital.gov.ua/projects/education/osvita>.
218. Цифрова трансформація 2025 : офіційний вебсайт Міністерства цифрової трансформації України. URL: <https://2025.thedigital.gov.ua/>.
219. Чижов В. Діагностування кризового стану ІТ-підприємств. *Фінансовий простір*. 2017. № 4(28). С. 142–148. URL: <https://fp.lnu.edu.ua/index.php/fp/article/view/548>.
220. Чібісова І. В., Івашина Є. М. Механізм забезпечення фінансової безпеки підприємства. *Проблеми підвищення ефективності інфраструктури : зб. наук. праць*. 2011. № 31. URL: <https://jrnl.nau.edu.ua/index.php/PPEI/article/view/347>.
221. Чуй І. Р., Мицак О. В. Особливості управління фінансами суб'єктів бізнесу ІТ-сектора. *Вісник Львівського торгово-економічного університету*. Серія: Економічні науки. 2023. № 74. С. 92–101. DOI: <https://doi.org/10.32782/2522-1205-2023-74-12>.

222. Чупілко О. Інноваційні технології у розвитку людського капіталу як складової систем управління в економіці. *Сталий розвиток економіки*. 2025. № 3(54). С. 227–231. DOI: <https://doi.org/10.32782/2308-1988/2025-54-35>.

223. Шадура-Никипорець Н. Т., Мініна О. В. Теоретичні підходи до змістовного наповнення категорії «фінансова безпека підприємства». *Науковий вісник Полісся*. 2025. № 2 (31). С. 411-420.

224. Шишкіна О. В. Механізм управління фінансовими ризиками промислових підприємств: теорія, методологія, практика : монографія. Чернігів : ЧНТУ, 2020. 318 с.

225. Шишкіна О. В., Суховерський М. Ю., Даньков А. Ю. Оцінка впливу фінансових інструментів на економічну безпеку підприємств. *Науковий вісник Полісся*. 2025. № 1(30). С. 160-179. DOI: [https://doi.org/10.25140/2410-9576-2025-1\(30\)-160-179](https://doi.org/10.25140/2410-9576-2025-1(30)-160-179).

226. Шкарлет С. М. Економічна безпека підприємства: інноваційний аспект : монографія. Київ : НАУ, 2007. 436 с.

227. Шкарлет С. М., Дубина М. В., Тарасенко А. В. Організаційно-інфраструктурне забезпечення розвитку сільського господарства України : монографія. Чернігів : ЧНТУ, 2016. 207 с.

228. Що потрібно знати про валютні обмеження, запроваджених під час воєнного стану. *KPMG*. URL: <https://kpmg.com/ua/uk/home/media/press-releases/2023/09/currency-controls-under-martial-law-when-investing-or-doing-business-in-ukraine.html>.

229. Які є типи ІТ-компаній. *FoxmindEd*. 2024. URL: <https://foxminded.ua/it-kompanii/>.

230. Яструбецька Л. Комплексна методика оцінки рівня фінансової безпеки суб'єктів підприємництва в Україні за умов гібридних загроз. *Підприємництво та інновації*. 2021. № 17. С. 75-82. URL: <http://ejournal.in.ua/index.php/journal/article/view/428>.

231. Яструбецька Л. С. Фінансова безпека суб'єктів підприємництва в Україні в умовах гібридних загроз : монографія. Львів : ЛНУ ім. Івана Франка, 2022. 370 с. URL: https://econom.lnu.edu.ua/wp-content/uploads/2016/09/Financial-SecurityHybrid-Wars_Yastrubetska.pdf.

232. Ad hoc Report: Situation in Ukraine and Displacement to the EU+: Trends, Drivers and Future Prospects. *European Union Agency for Asylum (EUAA)*. 2025. 5 September. URL: https://www.euaa.europa.eu/sites/default/files/publications/2025-09/2025_09_EUAA_Ad_hoc_Report_Ukraine_EN.pdf.

233. Annual Market Overview by UVCA and Mind.ua. 7 June 2023. URL: <https://www.uvca.eu/news/annual-market-overview-by-uvca-and-mind.ua>.

234. Banking Sector Review (February 2025). *National Bank of Ukraine*. 2025. URL: https://bank.gov.ua/admin_uploads/article/Banking_Sector_Review_2025-02_eng.pdf?v=12.

235. Bilyi M., Kravchenko A., Lesun S., Fedoriv Y., Penteleichuk M., Akinchyts O. Formation of competitive advantages of financial institutions in the conditions of digitization and instability of the national economy. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2026. Т. 1. № 66. С. 123–137. DOI: <https://doi.org/10.55643/fcaptp.1.66.2026.5024>.

236. Blakyta G., Ganushchak T. Enterprise financial security as a component of the economic security of the state. *Investment Management and Financial Innovations*. 2018. Vol. 15, Issue 2. P. 248–256. URL: https://www.researchgate.net/publication/325779265_Enterprise_financial_security_as_a_component_of_the_economic_security_of_the_state.

237. Bravel — кластер оборонних технологій в Україні : офіційний вебсайт. URL: <https://bravel.gov.ua>.

238. Bravel Defense Tech Valley 2025 у Львові відвідало 5000 людей з понад 50 країн світу / Міністерство цифрової трансформації України. 9 вер. 2025. URL: <https://thedigital.gov.ua/news/technologies/bravel-defense-tech-valley-2025-u-lvovi-vidvidalo-5000-lyudey-z-ponad-50-krain-svitu>.

239. Brynjolfsson E., McAfee A. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York : W.W. Norton & Company, 2014. 336 p.

240. Call for Applications 2024-2. Financial support combined with additional advice and assistance to up to 1.500 Ukrainian SMEs planning specific activities to integrate into the EU Single Market. URL: https://epo.org.ua/downloads/bb_call_2024-2.pdf.

241. Cebula J. J., Young L. R. A Taxonomy of Operational Cyber Security Risks. Pittsburgh : Carnegie Mellon University / Software Engineering Institute, 2014. (Technical Note CMU/SEI-2014-TN-006).

242. Deal Book: Ukrainian Venture Capital and Private Equity Overview 2022-2023. *Slideshare*. URL: <https://www.slideshare.net/slideshow/deal-book-ukrainian-venture-capital-and-private-equity-overview-20222023/258287825>.

243. Digital Tiger 2024 : [analytics report]. IT Ukraine Association. 2024. URL: <https://itukraine.org.ua/files/DigitalTiger2024.pdf>.

244. Digital Tiger: the Marker Power of Ukrainian IT research for 2024 / IT Ukraine Association ; Ministry of Digital Transformation of Ukraine. 2024. 68 p. URL: <https://itukraine.org.ua/files/DigitalTiger2024.pdf>.

245. Digital Tiger: the Power of Ukrainian IT research for 2023. *IT Ukraine Association*. 2023. URL: https://itukraine.org.ua/files/ITU_GT.pdf.

246. Diia Reaches 23 Million Users: Ukraine's Digital Government Becomes the New Normal. *Міністерство цифрової трансформації*. 2025. URL: <https://digitalstate.gov.ua/news/govtech/ponad-23-milyony-ukrayintsiv-uzekorystuiutsia-diyeyu-tsyfrova-derzava-stala-novoiu-normoiu>.

247. Do IT Like Ukraine 2022: Industry Report. URL: https://itukraine.org.ua/files/reports/2022/DoITLikeUkraine2022_EN.pdf.

248. Dubyna M., Panchenko O., Shpomer T., Shyshkina O., Kosach I., Bazilinska O. The Role of Digitalization of the Payment Infrastructure in Ensuring the Economic Security of the State Under the Conditions of Social and Political Shocks. *International Journal of Sustainable Development and Planning*. 2024. Vol. 19, No. 3. P. 893–908.

249. Dubyna M., Shchur R., Shyshkina O., Sadchykova I., Panchenko O., Bazilinska O. The Role of Artificial Intelligence in the Cybersecurity System of Banking Institutions in the Conditions of Instability. *Journal of Theoretical and Applied Information Technology*. 2024. Vol. 102, No. 19. P. 6950–6965.

250. Dubyna M., Verbivska L., Shyshkina O., Los A., Fediai Y. Innovative Development and Investment Advancement of Industrial Enterprises in Deriving Conditions of Digital Economy. *Pacific Business Review International*. 2024. Vol. 17. Iss. 4. P. 40–49. URL: http://www.pbr.co.in/2024/2024_month/October/4.pdf.

251. Financing options for Ukrainian startups. *Prikhodko & Partners*. 2025. URL: <https://prikhodko.com.ua/en/media/media/article/financing-options-for-ukrainian-startups/>.

252. Grant Support : Ukrainian Startup Fund official website. URL: <https://usf.com.ua/en/programs/grant-support>.

253. Impact of Economic Fluctuation on IT Salaries in Ukraine – Insights and Trends. *MoldStud*. 2025. 30 March. URL: <https://moldstud.com/articles/p-impact-of-economic-fluctuation-on-it-salaries-in-ukraine-insights-and-trends>.

254. Kostyunik O., Andriienko M., Voinalovych I., Bosa I., Bilychenko M. Organizational support for the formation of the economic security system of enterprises in the conditions of intellectual and innovative development of society. *Management Theory and Studies for Rural Business and Infrastructure Development*. 2023. № 45(4). P. 399-405. DOI: <https://doi.org/10.15544/mts.2023.39>.

255. Mesarovic M. D., Takahara Y. General Systems Theory: Mathematical Foundations. New York : Academic Press, 1975. 268 p.

256. Optimization of the financial security of industrial enterprises in the era of digitalization using information-analytic tools / V. Saienko et al. *Proceedings of the 6th International Conference on Modern Management*. 2024. URL: https://www.researchgate.net/publication/378991316_OPTIMIZATION_OF_THE_FINANCIAL_SECURITY_OF_INDUSTRIAL_ENTERPRISES_IN_THE_ERA_OF_DIGITALIZATION_USING_INFORMATION-ANALYTIC_TOOLS.

257. Oriekhova K., Golovko O., Khrystoforova O., Efymenko M. Features on providing enterprise financial security in the Covid-19 pandemic. *Bulletin of V. N. Karazin Kharkiv National University Economic Series*. 2022. № 102. С. 14–22. DOI: <https://doi.org/10.26565/2311-2379-2022-102-02>.
258. Reutov I., Khomenko V. Fundamentals of Legal Regulation in the Sector. *IT Law*. URL: <https://ukrainianlawfirms.com/reviews/it-law/>.
259. Rushchyshyn N., Nikonenko U., Kostak Z. Formation of financial security of the enterprise based on strategic planning. *Baltic Journal of Economic Studies*. 2017. Vol. 3, No. 4. P. 231–237.
260. Scaling Up: Accelerating Ukraine’s Tech Sector. *Civitta*. 2024. URL: <https://civitta.com/wp-content/uploads/2024/09/Scaling-Up-accelerating-Ukraines-Tech-Sector.pdf>.
261. Schwab K. *The Fourth Industrial Revolution*. Geneva : World Economic Forum, 2016. 171 p.
262. Tapscott D. *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*. New York : McGraw-Hill, 1996. 342 p.
263. The Startup Ecosystem of Ukraine. *StartupBlink*. 2025. URL: <https://www.startupblink.com/startup-ecosystem/ukraine>.
264. Top Companies, Export Volumes, Startups, and the Most In-Demand Tech Stacks. *AIN*. 2024. URL: https://18dccfa619686586.cdn.express/AIN_Research_10_Years_of_Ukrainian_IT_2014_2024.pdf.
265. Ukraine - Corporate - Significant developments. *Worldwide Tax Summaries Online*. 31 December 2025. URL: <https://taxsummaries.pwc.com/ukraine/corporate/significant-developments>.
266. Ukraine Facility : офіційний вебсайт Міністерства економіки України. URL: <https://www.ukrainefacility.me.gov.ua>.
267. Ukraine IT Exports Rise to 43% of Total Trade. 2025. *Digitalstate*. URL: <https://digitalstate.gov.ua/news/it-outsourcing/it-posluhy-staly-holovnym-drayverom-eksportu-ukrayiny-u-2025-rotsi>.

268. Ukraine: Firms through the War 2.0. *The World Bank Group*. November 13, 2024. URL: <https://documents1.worldbank.org/curated/en/099061924125589588/pdf/P177312124626806b1aa081021aad774db2.pdf>.

269. Ukraine: Firms through the War. *The World Bank Group*. November 28, 2023. URL: <https://kse.ua/wp-content/uploads/2024/03/Ukraine.-Firms-through-the-War-Paper-Nov-2023.pdf>.

270. Ukraine's IT shift: from outsourcing to innovation. *Ministry of Digital Transformation*. 2025. URL: <https://digitalstate.gov.ua/news/it-outsourcing/ukraines-it-shift-from-outsourcing-to-innovation>.

271. Ukrainian Tech Industry in the Fourth Year of the War: Stabilization, New Strategies, and a Shift in Market Architecture — Results of IT Research Ukraine 2025. From Adaptation to Transformation. *CodeUA*. December 16, 2025. URL: <https://codeua.com/ukrainian-tech-industry-in-the-fourth-year-of-the-war-stabilization-new-strategies-and-a-shift-in-market-architecture-results-of-it-research-ukraine-2025-from-adaptation-to-transformatio/>.

272. UNIT.City — перший інноваційний парк в Україні : офіційний вебсайт. URL: <https://unit.city/>.

273. Updated Ukraine Recovery and Reconstruction Needs Assessment. *The World Bank Group*. 2026. URL: <https://www.worldbank.org/en/country/ukraine/overview>.

274. World Bank Group. Home. Worldwide Governance Indicators. *World Bank*. URL: <https://www.worldbank.org/en/publication/worldwide-governance-indicators>.

275. Yevtushenko Y., Bilyi M., Lesun S., Fedoriv Y., Kravchenko A., Akinchyts O. Customization of Financial Services: Digitalization, Transformation, Trust, Emphasizing the Role of Education in Processes. *Cadernos De Educação Tecnologia E Sociedade*. 2025. Vol. 18(se3). Pp. 239–249. DOI: <https://doi.org/10.14571/brajets.v18.nse3.239-249>.

276. Zavhorodnya E. Modeling the system of factors influencing the international competitiveness of Ukraine's ICT sector. *Economy and Society*. 2024. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/6127/6069>.

ДОДАТКИ

**Система показників-індикаторів для оцінки рівня фінансової безпеки
підприємств ІТ-сфери**

Складові компоненти фінансової безпеки	Індикатори для підприємств ІТ-сфери	Економічне обґрунтування
1	2	3
Майновий стан	Вартість активів підприємств ІТ-сфери, млн грн	Відображає масштаби діяльності та ресурсний потенціал ІТ-підприємств.
	Частка основних засобів та нематеріальних активів в загальній сумі активів	Характеризує структуру майна і показує орієнтацію на інновації та технологічний розвиток.
	Забезпеченість підприємства оборотними активами	Важливий для оцінки ліквідності майна та мобільності ресурсів; вказує на гнучкість підприємства в управлінні активами.
	Коефіцієнт зміни вартості активів на одного працівника	Характеризує рівень забезпеченості персоналу активами; важливий для ІТ, де працівники виступають ключовим ресурсом
	Рівень фондовіддачі	Дозволяє оцінити ефективність управління ресурсами та показує як основні засоби та нематеріальні активи генерують прибуток
Інвестиційна привабливість	Обсяги капітальних інвестицій у матеріальні активи підприємств ІТ сфери, млн грн	Дозволяє оцінити здатність підприємства модернізувати свою матеріально-технічну базу та важливий для аналізу забезпечення робочої інфраструктури, обладнання, серверів тощо.
	Обсяги капітальних інвестицій у нематеріальні активи підприємств ІТ-сфери, млн грн	Відображає рівень інвестиції у інноваційний розвиток, науково-технічні розробки та дослідження
	Коефіцієнт самофінансування	Відображає здатність ІТ- підприємств фінансувати свою діяльність за рахунок власних ресурсів, що важливо для їх фінансової стійкості та незалежності
	Обсяги залучених венчурних/прямих інвестицій в ІТ-сферу, млн дол.	Важливий для оцінки потенціалу зростання та фінансового ресурсного забезпечення, а також характеризує привабливість ІТ-сектору для інвесторів.
Фінансова стійкість	Коефіцієнт фінансової автономії	Для ІТ-підприємств важлива фінансова автономія, адже це знижує залежність від зовнішніх кредиторів
	Коефіцієнт фінансової стійкості	В ІТ-компаніях надмірна залежність від позикових коштів підвищує фінансові ризики, особливо в умовах макроекономічної нестабільності
	Коефіцієнт маневреності власного оборотного капіталу	Характеризує мобільність власного капіталу, яка у контексті високодинамічного ІТ-бізнесу є надзвичайно важливою для забезпечення гнучкості та безперервності операційних процесів

Закінчення таблиці 2.11

1	2	3
	Коефіцієнт забезпеченості оборотних активів	Для ІТ-підприємств виступає критичним індикатором внутрішньої фінансової гнучкості, стабільності операційної діяльності та його здатності витримувати короткострокові фінансові навантаження без зовнішньої підтримки
	Коефіцієнт довгострокової фінансової стійкості	Оцінює платоспроможність у довгостроковій перспективі, а в ІТ-секторі ще є показником здатності компанії розвиватися стратегічно, витримувати високі інноваційні навантаження та залишатися фінансово автономною.
Прибутковість	Рентабельність власного капіталу, %	Відображає ефективність використання власного капіталу підприємства та важливий для оцінки прибутковості з погляду венчурних та приватних інвесторів.
	Рентабельність основних засобів та нематеріальних активів, %	В ІТ-секторі основні засоби мають відносно менший вплив, а нематеріальні активи відіграють ключову роль, але в статистичних даних ці активи відображаються разом. Тому, за наявності потрібної інформації, можна акцентувати увагу саме на рентабельності нематеріальних активів.
	Рентабельність активів, %	Відображає ефективність використання усіх активів для отримання прибутку; у ІТ-галузі високі значення свідчать про комерційний успіх ІТ-продуктів та послуг.
	Чиста рентабельність продажів, %	Характеризує ефективність основної діяльності, конкурентоспроможність та стійкість ІТ-бізнесу
Ліквідність	Коефіцієнт загальної ліквідності	Оцінює здатність підприємства покривати короткострокові зобов'язання поточними активами та є особливо важливим для ІТ-підприємств з проєктною формою діяльності.
	Коефіцієнт проміжної ліквідності	Враховує лише найбільш ліквідні активи; релевантний для ІТ, де основними оборотними активами є грошові кошти та дебіторська заборгованість.
	Коефіцієнт абсолютної ліквідності	Показує частку поточних зобов'язань, яку можна погасити негайно; важливий в умовах нестабільності та криз.
Ділова активність	Обсяги реалізованої продукції підприємств ІТ-сфери, млрд грн	Відображає масштаб операційної діяльності, розвиток ІТ-бізнесу і його здатність генерувати дохід.
	Коефіцієнт оборотності активів	Відображає швидкість використання активів у господарському обороті; у ІТ галузі високі значення свідчать про ефективне управління ресурсами.
	Рівень доходу на одного працівника	Відображає продуктивність праці.
	Коефіцієнт оборотності дебіторської заборгованості	Оцінює швидкість повернення коштів від клієнтів; важливо в умовах проєктної діяльності.
	Коефіцієнт оборотності кредиторської заборгованості	Показує швидкість розрахунків з постачальниками та підрядниками; в ІТ-сфері це впливає на репутацію і стійкість підприємств.
	Коефіцієнт оборотності власного капіталу	Оцінює ефективність використання власного капіталу для отримання доходів.

Джерело: складено автором на основі [67; 45; 20].

Додаток Б

Таблиця Б.1

Нормовані значення показників-індикаторів компонентів фінансової безпеки підприємств ІТ-сфери

Компоненти фінансової безпеки	Індикатори для підприємств ІТ-сфери	2019	2020	2021	2022	2023	2024	Вага показника-індикатора у складовій компоненті ФБ
1	2	3	4	5	6	7	8	9
Майновий стан	Вартість активів підприємств ІТ-сфери, млн грн	0,000	0,045	0,108	0,322	0,668	1,000	0,333
	Забезпеченість підприємства оборотними активами	0,000	0,362	0,427	0,899	0,996	1,000	0,267
	Частка основних засобів та нематеріальних активів у загальній сумі активів	0,947	1,000	0,803	0,303	0,013	0,000	0,133
	Коефіцієнт зміни вартості активів на одного працівника	0,791	0,000	0,172	0,410	0,844	1,000	0,200
	Рівень фондовіддачі	0,266	0,442	1,000	0,667	0,190	0,000	0,067
Інвестиційна привабливість	Обсяги капітальних інвестицій у матеріальні активи підприємств ІТ сфери, млн грн	0,305	0,031	0,448	0,000	0,281	1,000	0,100
	Обсяги капітальних інвестицій у нематеріальні активи підприємств ІТ-сфери, млн грн	0,123	0,000	0,356	0,109	0,688	1,000	0,200
	Коефіцієнт самофінансування	0,212	0,983	0,000	0,774	1,000	0,334	0,300
	Обсяги залучених венчурних/прямих інвестицій в ІТ-сферу, млн дол.	0,745	0,510	0,922	1,000	0,000	0,390	0,400

Закінчення таблиці 2.16

1	2	3	4	5	6	7	8	9
Фінансова стійкість	Коефіцієнт фінансової автономії	0,668	0,795	0,842	0,830	0,860	0,860	0,333
	Коефіцієнт фінансової стійкості	0,558	0,759	0,852	0,828	0,889	0,907	0,267
	Коефіцієнт маневреності власного оборотного капіталу	0,492	1,000	1,000	1,000	1,000	1,000	0,133
	Коефіцієнт забезпеченості оборотних активів	0,252	0,628	0,688	0,782	0,980	0,996	0,200
	Коефіцієнт довгострокової фінансової стійкості	0,750	0,882	0,905	0,883	0,988	1,000	0,067
Прибутковість	Рентабельність власного капіталу, %	0,148	0,000	0,448	0,905	1,000	0,790	0,300
	Рентабельність ОЗ та нематеріальних активів, %	0,000	0,000	0,189	0,566	0,958	1,000	0,100
	Рентабельність активів, %	0,000	0,207	0,596	0,850	1,000	0,886	0,400
	Чиста рентабельність продажів, %	0,000	0,066	0,073	0,389	0,827	1,000	0,200
Ліквідність	Коефіцієнт загальної ліквідності	1,000	1,000	1,000	0,974	0,816	0,804	0,500
	Коефіцієнт проміжної ліквідності	1,000	1,000	0,972	0,897	0,761	0,753	0,333
	Коефіцієнт абсолютної ліквідності	1,000	1,000	1,000	1,000	1,000	1,000	0,167
Ділова активність	Обсяги реалізованої продукції підприємств ІТ-сфери, млрд грн	0,166	0,255	0,509	0,641	0,000	1,000	0,238
	Коефіцієнт оборотності активів	0,328	0,316	1,000	0,903	0,360	0,000	0,19
	Рівень доходу на одного працівника	0,000	0,051	0,183	0,323	0,559	1,000	0,286
	Коефіцієнт оборотності дебіторської заборгованості	0,703	0,636	1,000	0,672	0,206	0,000	0,143
	Коефіцієнт оборотності кредиторської заборгованості	0,071	0,167	1,000	0,882	0,187	0,000	0,095
	Коефіцієнт оборотності власного капіталу	0,937	0,708	1,000	0,855	0,305	0,000	0,048

Джерело: розраховано автором.

PEST-аналіз зовнішніх загроз фінансовій безпеці підприємств ІТ-сфери

Компонент PEST	Зовнішні загрози	Характеристика	Вплив на фінансову безпеку
1	2	3	4
Р – Політичні загрози	Військові дії та політична нестабільність	<ul style="list-style-type: none"> - військові дії та фізичне знищення чи пошкодження інфраструктури; - непередбачуваність політичних рішень; - мобілізація ключових ІТ-фахівців; - вимушена релокація персоналу. 	<ul style="list-style-type: none"> - збільшення витрат на заходи безпеки; - втрата контрактів та зниження прибутковості; - скорочення доходів через простої; - погіршення ліквідності та ризику касових розривів; - зниження інвестиційної привабливості ІТ-галузі.
	Валютні та фінансові обмеження НБУ	<ul style="list-style-type: none"> - ліміти на міжнародні платежі; - складність репатріації дивідендів; - контроль руху капіталу; - валютні обмеження. 	<ul style="list-style-type: none"> - ускладнення виконання міжнародних контрактів; - скорочення валютних надходжень; - заморожування частини оборотного капіталу; - зростання витрат на управління валютними ризиками; - зростання ризиків неплатоспроможності та зниження ліквідності ІТ-компаній; - зниження інвестиційної активності іноземних інвесторів.
	Регуляторна нестабільність в ІТ-сфері	<ul style="list-style-type: none"> - часті зміни законодавства (податкового, трудового); - систематичні зміни у законодавстві щодо мобілізації та бронювання; - нестабільність умов ведення бізнесу для ІТ-компаній. 	<ul style="list-style-type: none"> - ускладнення довгострокового фінансового планування; - зростання адміністративних витрат та податкового навантаження; - зниження рентабельності ІТ-послуг та продуктів; - скорочення інвестицій через регуляторну невизначеність; - ризики втрати персоналу через політику бронювання/мобілізації.
	Нестійкість інституційного середовища	<ul style="list-style-type: none"> - корупційні ризики та бюрократичні бар'єри; - недосконалість інституційних механізмів захисту прав інтелектуальної власності; - недостатня узгодженість та координація цифрових реформ. 	<ul style="list-style-type: none"> - затримки реалізації проєктів, що призводять до додаткових фінансових витрат; - підвищення витрат на юридичний супровід та комплаєнс; - ускладнення стратегічного фінансового планування; - зниження довіри міжнародних партнерів та інвесторів до українських ІТ-компаній.

Продовження таблиці 3.1

1	2	3	4
Е – Економічні загрози	Інфляційний тиск	- високі темпи зростання цін; - зростання витрат на оплату праці; - подорожчання матеріальних, енергетичних та ін. ресурсів.	- зростання операційних витрат; - зниження реальної рентабельності; - знецінення купівельної спроможності клієнтів; - підвищення ризиків касових розривів.
	Валютна нестабільність та девальвація	- коливання курсу гривні; - зростання вартості імпортного обладнання, програмного забезпечення тощо; - переоцінка валютних активів та зобов'язань	- підвищення витрат у валютному еквіваленті; - коливання доходів у гривневому еквіваленті; - недоотримання прибутку внаслідок курсових змін; - підвищення ризиків касових розривів та зниження ліквідності; - ускладнення фінансового планування.
	Сповільнення темпів економічного зростання	- зменшення внутрішнього попиту на ІТ-послуги; - загальне уповільнення економічної активності в країні; - скорочення інвестицій в ІТ-бізнес.	- зниження ділової активності ІТ-компаній; - зменшення доходів ІТ-компаній; - зростання термінів окупності інвестиційних проєктів.
	Обмежений доступ до кредитів та капіталу	- високі ставки за кредитами; - жорсткі умови банківського кредитування; - недостатній розвиток венчурного фінансування, - обмежена доступність сучасних інструментів інвестування	- дефіцит інвестицій у розвиток ІТ-сектору та інновації; - уповільнення темпів зростання ІТ-бізнесу; - зростання витрат на обслуговування залученого капіталу; - зниження платоспроможності та фінансової стійкості ІТ-компаній.
	Зниження зовнішнього попиту на ІТ-послуги	- скорочення замовлень з боку іноземних клієнтів; - перегляд бюджетів іноземними замовниками; - зростання частки короткострокових контрактів	- зменшення доходів та валютної виручки; - нестабільність іноземних контрактів; - скорочення чисельності працівників ІТ-компаній; - зниження рентабельності та інвестиційних можливостей.

Продовження таблиці 3.1

1	2	3	4
S – Соціальні загрози	Дефіцит та міграція IT-кадрів	<ul style="list-style-type: none"> - виїзд IT-фахівців за кордон; - дисбаланс між попитом і пропозицією на ринку праці; - загострення конкуренції за кваліфіковані кадри 	<ul style="list-style-type: none"> - зростання витрат на персонал та рекрутинг; - зниження продуктивності IT-команд; - зниження конкурентоспроможності IT-компаній; - зниження виробничих можливостей компаній, зриви виконання проєктів.
	Трансформація форм зайнятості	<ul style="list-style-type: none"> - поширення дистанційної та гібридної моделі роботи; - ускладнення координації, контролю та комунікації в командах; - зростання частки проєктної зайнятості 	<ul style="list-style-type: none"> - збільшення витрат на цифрову інфраструктуру (VPN, хмарні сервіси, офісні резерви); - зростання витрат на управління персоналом; - підвищення ризиків порушення термінів виконання контрактів; - втрати доходів IT-компаній через зниження керованості бізнес-процесів.
	Демографічні та освітні дисбаланси на ринку праці	<ul style="list-style-type: none"> - невідповідність компетентностей випускників потребам IT-ринку; - зменшення кількості студентів, виїзд молоді на навчання за кордон; - зростання середнього віку IT-кадрів. 	<ul style="list-style-type: none"> - зростання витрат на навчання та перекваліфікацію персоналу; - ризики зниження якості IT-продуктів та ефективності діяльності; - зниження відтворення людського капіталу; - підвищення собівартості IT-проєктів.
	Соціальна напруга, що пов'язана з війною, мобілізацією та адаптацією персоналу	<ul style="list-style-type: none"> - мобілізаційні ризики: - потреба в адаптації ветеранів до трудових колективів; - психологічне та емоційне вигорання персоналу. 	<ul style="list-style-type: none"> - зниження продуктивності праці; - підвищення витрат на адаптацію та підтримку персоналу; - підвищення ризиків плинності кадрів; - зниження якості IT-продуктів та послуг,

1	2	3	4
Т – Технологічні загрози	Зростання кіберзагроз	- кібератаки на ІТ-бізнес і критичну інфраструктуру; - зростання кількості інцидентів викрадення даних; - посилення ризиків кібершпигунства та несанкціонованого доступу.	- прямі збитки від простоїв та збоїв у роботі; - додаткові фінансові втрати на відновлення інфраструктури; - збільшення витрат на кіберзахист; - ризики витоку даних і репутаційних втрат; - зниження довіри клієнтів і замовників.
	Руйнування цифрової та телекомунікаційної інфраструктури	- пошкодження мереж, дата-центрів та енергетичної інфраструктури; - перебої з електропостачанням; - збої у роботі інтернету, хмарних сервісів тощо.	- втрати через зрив контрактів і порушення строків виконання проєктів; - зростання витрат на резервне енергозабезпечення та альтернативні канали зв'язку; - зниження доходів через вимушені простої; - збільшення операційних витрат; - підвищення ризиків невиконання контрактних зобов'язань.
	Прискорення технологічних змін в ІТ-секторі та ризик технологічного відставання	- прискорене технологічне старіння ІТ-рішень та продуктів; - зростання потреби у постійній модернізації технологічної бази; - ризик технологічного відставання від глобальних трендів цифровізації.	- зростання витрат на R&D, модернізацію та оновлення програмних рішень; - втрата конкурентоспроможності; - ризики втрати клієнтів; - необхідність великих інвестицій у модернізацію та технологічне оновлення; - зниження рентабельності ІТ-компаній.
	Технологічна залежність від зовнішніх цифрових платформ	- залежність від глобальних цифрових платформ і провайдерів; - ризики обмеження або блокування доступу до сервісів з боку провайдерів; - валютні коливання вартості сервісів і підписок.	- зростання собівартості ІТ-послуг; - ризики перебоїв у роботі та порушення безперервності бізнес-процесів; - зниження маржинальності; - залежність витрат від змін цінової політики зовнішніх провайдерів; - підвищення фінансової вразливості у разі зміни умов доступу до сервісів.

Джерело: складено автором.

Додаток Г

Таблиця Г.1

**Характеристика заходів реалізації державної політики
щодо підвищення рівня фінансової безпеки підприємств ІТ-сектору**

Блоки державної політики	Напрями державної політики щодо забезпечення фінансової безпеки підприємств ІТ-сектору	Пріоритетні заходи реалізації державної політики
1	2	3
Інституційно-регуляторний	Удосконалення інституційно-правових умов функціонування ІТ-сектору	<ul style="list-style-type: none"> - удосконалення правового режиму функціонування ІТ-бізнесу; - забезпечення стабільності й передбачуваності податкових, валютних, трудових, мобілізаційних та інших регуляторних рішень у сфері ІТ-бізнесу; - покращення податкового клімату; - запровадження системи планування, розвитку та реалізації потенціалу ІТ-сектору в системі національної економіки; - гармонізація цифрового законодавства з нормами ЄС; - розвиток електронного документообігу та урядування; - посилення захисту прав інтелектуальної власності; - детінізація зайнятості та підвищення прозорості господарських відносин.
	Посилення інституційного забезпечення інформаційної та кібербезпеки	<ul style="list-style-type: none"> - розвиток систем державного моніторингу та реагування на кіберінциденти; - посилення інституційної спроможності органів кіберзахисту та державно-приватної координації в сфері кібербезпеки; - підтримка кіберстійкості критичної цифрової інфраструктури; - стимулювання впровадження сучасних стандартів кібербезпеки та підтримка адаптації ІТ-підприємств до цих вимог; - посилення превентивної кіберстійкості ІТ-підприємств з урахуванням типу, масштабу та рівня ризиковості ІТ-бізнесу; - розвиток системи підготовки фахівців у сфері кібербезпеки.

Продовження таблиці 3.7

1	2	3
Інноваційно-інвестиційний	Стимулювання розвитку інноваційної інфраструктури ІТ-сектору	<ul style="list-style-type: none"> - підтримка розвитку технопарків, інноваційних парків, бізнес-інкубаторів і акселераторів; - стимулювання кластерної взаємодії між ІТ-бізнесом, інвесторами, ЗВО та науковими установами; - розвиток центрів трансферу технологій і R&D-екосистем і механізмів комерціалізації інновацій; - інтеграція українських стартапів у міжнародні інноваційні мережі.
	Підвищення доступності фінансових ресурсів для ІТ-галузі	<ul style="list-style-type: none"> - розвиток державних грантових програм для ІТ-стартапів, продуктових компаній та інноваційних проєктах на ранніх стадіях розвитку; - підтримка змішаного фінансування за участю держави, міжнародних партнерів та інвестиційних фондів; - стимулювання венчурного інвестування в ІТ-секторі; - розширення спеціалізованих механізмів підтримки defence tech, AI, кібербезпеки; - активізація участі фінансово-кредитних установ у фінансуванні ІТ-сектору за підтримки держави; - розвиток альтернативних джерел фінансування ІТ-підприємств; - застосування гарантійних і страхових механізмів для інноваційних проєктів.
	Стимулювання створення власних ІТ-продуктів та розвитку ІТ-підприємництва	<ul style="list-style-type: none"> - розширення грантової підтримки стартапів та продуктових компаній на початкових стадіях розвитку; - підтримка розвитку високотехнологічних інноваційних сегментів, зокрема у сфері штучного інтелекту, кібербезпеки, оборонних технологій, GovTech тощо; - стимулювання та економічна підтримка державно-приватних проєктів зі створення ІТ-продуктів; - створення умов для масштабування українських продуктових ІТ-компаній; - підтримка комерціалізації вітчизняних цифрових рішень.

Закінчення таблиці 3.7

1	2	3
Кадровий	Розвиток кадрового потенціалу ІТ-галузі	<ul style="list-style-type: none"> - модернізація систем підготовки кадрів для ІТ-сектору відповідно до потреб цифрової економіки; - розвиток програм перекваліфікації та підвищення кваліфікації кадрів; - підтримка навчально-практичних центрів при ЗВО; - розширення співпраці між ІТ-компаніями та освітніми установами; - сприяння збереженню, професійному оновленню та адаптації кадрового потенціалу ІТ-галузі; - підтримка цифрових освітніх платформ і програм швидкої підготовки кадрів.
Ринковий	Активізація розвитку внутрішнього ринку ІТ-продуктів	<ul style="list-style-type: none"> - стимулювання попиту на українські ІТ-рішення; - підтримка цифровізації реального сектору економіки; - розвиток державно-приватних проєктів із впровадження ІТ-продуктів; - збільшення обсягів державного замовлення на ІТ-продукти; - підтримка пілотного впровадження та ринкової апробації українських ІТ-рішень; - розвиток цифрових державних сервісів для бізнесу.
	Розширення експортного потенціалу ІТ-сектору	<ul style="list-style-type: none"> - розвиток інституційної підтримки експорту ІТ-послуг і продуктів; - сприяння участі ІТ-компаній у міжнародних виставках, бізнес-заходах тощо; - консультативний супровід виходу на нові ринки; - розвиток фінансових механізмів стимулювання експорту та страхування експортних ризиків; - удосконалення митного та валютного супроводу зовнішньоекономічних операцій ІТ-компаній; - спрощення процедур експортного контролю та міжнародного просування українських оборонних технологій; - підтримка міжнародної промоції українських ІТ-компаній.

Джерело: систематизовано автором на основі [21; 44; 120; 146; 209; 231].

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

статті в закордонних наукових виданнях,

включених до міжнародних наукометричних баз:

1. Yevtushenko Y., Bilyi M., **Lesun S.**, Fedoriv Y., Kravchenko A., & Akinchyts O. (2025). Customization of Financial Services: Digitalization, Transformation, Trust, Emphasizing the Role of Education in Processes. *Cadernos De Educação Tecnologia E Sociedade*, 18(se3), 239–249. DOI: <https://doi.org/10.14571/brajets.v18.nse3.239-249> (1,3 ум. друк. арк.). Особистий внесок: розглянуто роль цифрових технологій у трансформації фінансових послуг та формуванні довіри між фінансовими установами і споживачами (0,22 ум. друк. арк.).

2. Bilyi M., Kravchenko A., **Lesun S.**, Fedoriv Y., Penteleichuk M., & Akinchyts O. (2026). Formation of competitive advantages of financial institutions in the conditions of digitization and instability of the national economy. *Financial and Credit Activity Problems of Theory and Practice*, 1(66), 123–137. DOI: <https://doi.org/10.55643/fcaptp.1.66.2026.5024> (0,9 ум. друк. арк.). Особистий внесок: визначено роль цифрових технологій у формуванні конкурентних переваг фінансових установ в умовах нестабільності (0,16 ум. друк. арк.).

статті в наукових фахових виданнях України:

3. **Лесун С. М.** Фінансова безпека підприємств та її особливості в умовах цифрової економіки. *Проблеми і перспективи економіки та управління*. 2024. № 3(39). С. 341-352. URL: <http://ppeu.stu.cn.ua/article/view/319324> (0,61 ум. друк. арк.).

4. Кальченко О. М., Зеленська О. О., **Лесун С. М.** Фінансова поведінка домогосподарств у контексті розвитку поведінкових фінансів. *Проблеми і перспективи економіки та управління*. 2023. № 4(36). С. 280-290. URL: <http://ppeu.stu.cn.ua/article/view/299261> (0,69 ум. друк. арк.). Особистий внесок: узагальнено поведінкові чинники прийняття фінансових рішень в умовах ризику та невизначеності, що впливають на фінансову стійкість економічних суб'єктів (0,1 ум. друк. арк.).

5. Кальченко О. М., Лесун С. М. Економіко-статистичне дослідження ефективності використання фінансових ресурсів підприємств ІТ-сфери. *Проблеми і перспективи економіки та управління*. 2025. № 1(41). С. 422-436.

URL: <http://ppeu.stu.cn.ua/issue/view/19295/12492> (0,68 ум. друк. арк.)

Особистий внесок: проведено аналіз структури фінансових ресурсів, активів і фінансових результатів підприємств ІТ-сфери та визначено їх вплив на фінансову стійкість ІТ-компаній (0,4 ум. друк. арк.).

6. Панченко О. І., Лесун С. М. Методичні підходи до оцінки рівня фінансової безпеки підприємств ІТ-сфери. *Проблеми і перспективи економіки та управління*. 2025. № 3(43). С. 347-358. URL:

<http://ppeu.stu.cn.ua/article/view/344079> (0,75 ум. друк. арк.). Особистий внесок:

систематизовано методичні підходи до оцінки фінансової безпеки підприємств ІТ-сфери, обґрунтовано доцільність використання інтегрального підходу та запропоновано етапи комплексного оцінювання її рівня з урахуванням галузових особливостей (0,45 ум. друк. арк.).

7. Дубина М. В., Кальченко О. М., Лесун С. М. Фінансове забезпечення розвитку ІТ-компаній в Україні. *Проблеми системного підходу в економіці*. 2025. Вип. 5 (102). С. 72-86. URL:

http://www.psae-jrnl.nau.in.ua/journal/5_102_2025_ukr/11.pdf (1,06 ум. друк. арк.). Особистий

внесок: визначено сутність, види та особливості функціонування ІТ-компаній, що впливають на формування їх фінансової стійкості та безпеки (0,45 ум. друк. арк.).

8. Кальченко О. М., Лесун С. М., Кальченко М. В. Фінансовий інструментарій забезпечення фінансової безпеки ІТ-підприємств в умовах цифрової економіки. *Успіхи і досягнення у науці*. 2026. № 4(26). С. 1356–1372

(1,07 ум. друк. арк.). Особистий внесок: узагальнено фінансовий

інструментарій забезпечення фінансової безпеки ІТ-підприємств та визначено роль цифрових технологій у його реалізації (0,45 ум. друк. арк.).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

9. Панченко О. І., Лесун С. М. Особливості страхування фінансових ризиків банківських установ. *Фінансове та інформаційно-аналітичне забезпечення безпеки бізнесу в умовах воєнної економіки та повоєнного відновлення* : матеріали XII Міжнар. наук.-практ. конф., Харків, 22–23 листопада 2023 р. Харків : ХНУМГ ім. О. М. Бекетова, 2023. С. 220-222. URL: https://eprints.kname.edu.ua/64334/1/%D0%9A%D0%9E%D0%9D%D0%A4%D0%95%D0%A0%D0%95%D0%9D%D0%A6%D0%98%D0%AF%20%D0%A2%D0%B5%D0%B7%D0%B8%D1%81%D0%B8_2023_2.pdf (0,13 ум. друк. арк.).
Особистий внесок: розглянуто страховий механізм як інструмент мінімізації фінансових ризиків та забезпечення фінансової стійкості суб'єктів господарювання (0,05 ум. друк. арк.).

10. Панченко О. І., Кальченко О. М., Лесун С. М. Банкострахування як основа стабільності фінансового ринку. *Юність науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства* : збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 26-27 квітня 2023 р.). Чернігів : НУ «Чернігівська політехніка», 2023. С. 117-118. URL: <https://stu.cn.ua/wp-content/uploads/2023/11/zbirnyk-tez-yunist-nauky-2023.pdf> (0,15 ум. друк. арк.).
Особистий внесок: розглянуто страхові інструменти як засіб мінімізації фінансових ризиків і підтримання фінансової стійкості економічних суб'єктів (0,05 ум. друк. арк.).

11. Панченко О. І., Кальченко О. М., Лесун С. М. Проблеми розвитку сучасної системи ризик-менеджменту в банківських установах. *Юність науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства* : збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 26-27 квітня 2023 р.). Чернігів: НУ «Чернігівська політехніка», 2023. С. 118-120. URL: <https://stu.cn.ua/wp-content/uploads/2023/11/zbirnyk-tez-yunist-nauky-2023.pdf>

(0,18 ум. друк. арк.). Особистий внесок: узагальнено проблеми розвитку системи ризик-менеджменту та визначено його роль у забезпеченні фінансової стійкості суб'єктів господарювання (0,06 ум. друк. арк.).

12. **Лесун С. М.** Фінансова безпека підприємств в умовах становлення цифрової економіки. *Сучасні критерії оцінки ефективності господарських процесів в нестабільних економічних умовах* : матеріали Всеукр. наук.-практ. конф. (Чернігів, 12 листопада 2024 р.). Чернігів : Коледж транспорту та комп'ютерних технологій НУ «Чернігівська політехніка», 2024. С. 220-222 (0,12 ум. друк. арк.).

13. **Лесун С. М.** Соціально-філософський контекст управління фінансовими ризиками. *Юність науки – 2024: соціально-економічні та гуманітарні аспекти розвитку суспільства* : збірник тез доповідей XIV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 24-26 квітня 2024 р.). Чернігів : НУ «Чернігівська політехніка», 2024. С. 635-638. URL: <https://ir.stu.cn.ua/handle/123456789/30262> (0,2 ум. друк. арк.).

14. Панченко О. І., **Лесун С. М.** Специфіка підприємств ІТ-сфери як об'єкта фінансового управління. *Юність науки – 2025* : збірник тез доповідей XV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 23-25 квітня 2025 р.). Чернігів : НУ «Чернігівська політехніка», 2025. С. 78–80. URL: <https://ir.stu.cn.ua/items/7024c8b0-86f3-4ff4-baa0-3548f8c61574> (0,2 ум. друк. арк.). Особистий внесок: узагальнено специфіку підприємств ІТ-сфери як об'єкта фінансового управління та визначено її вплив на формування фінансової стійкості й безпеки (0,1 ум. друк. арк.).

15. **Лесун С. М.** Цифрова економіка та фінансова безпека: роль інформаційних технологій. *Фінансово-управлінські інновації як драйвер сталого розвитку в умовах сучасних викликів* : матеріали Міжнародної науково-практичної конференції (м. Хмельницький, 7 листопада 2025 року). Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2025. Ч. 1. С. 360-363 (0,2 ум. друк. арк.).

Довідки про впровадженняSendPulse12.05.2026 № 02-15/11

м. Чернігів

ДОВІДКА

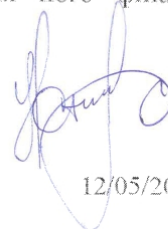
**про впровадження результатів дисертаційного дослідження
Лесуна Сергія Миколайовича
на тему: «Формування системи фінансової безпеки підприємств ІТ-
сфери в умовах становлення цифрової економіки»**

SendPulse Inc. розглянуто результати наукового дослідження Лесуна С.М., присвяченого формуванню системи фінансової безпеки підприємств ІТ-сфери в умовах становлення цифрової економіки та частково використано у практичній діяльності.

Актуальними є методичні положення щодо комплексного оцінювання рівня фінансової безпеки ІТ-підприємства на основі інтегрального показника. У практиці підприємства зазначені розробки враховано при проведенні внутрішньої фінансової діагностики, моніторингу фінансових показників, виявленні негативних тенденцій у фінансово-господарській діяльності та підготовці управлінських рішень щодо покращення фінансового стану і зміцнення його фінансової стійкості.

Устименко М. О.

Технічний директор SendPulse Inc.



12/05/2026

**ФІЗИЧНА ОСОБА-ПІДПРИЄМЕЦЬ
БАЗИЛЕВИЧ ВОЛОДИМИР МАРКОВИЧ**

м. Чернігів

11.05.2026 № 03/05-26

ДОВІДКА

**про використання теоретичних і прикладних результатів
дисертаційного дослідження Лесуна Сергія Миколайовича**

Цим підтверджується, що у діяльності ФОП «Базилевич Володимир Маркович» враховано теоретичні й прикладні результати дисертаційного дослідження аспіранта Національного університету «Чернігівська політехніка» Лесуна Сергія Миколайовича за спеціальністю 072 «Фінанси, банківська справа, страхування», присвяченого ідентифікації зовнішніх загроз та внутрішніх ризиків фінансової безпеки ІТ-підприємств, а також реагуванню на дестабілізаційні чинники цифрового середовища.

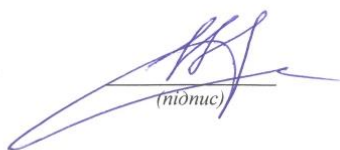
Зокрема, прийнято до використання рекомендації щодо систематизації ризиків і загроз фінансовій безпеці ІТ-підприємств та застосування сценарного підходу під час підготовки фінансових управлінських рішень.

Використання зазначених рекомендацій сприяє підвищенню обґрунтованості управлінських рішень у сфері фінансової безпеки та оцінювання ризиків цифрового середовища.

Довідку видано для подання за місцем вимоги.

Фізична особа-підприємець

М.П. (за наявності)


(підпис)

В.М. Базилевич

ДОВІДКА
про впровадження результатів дисертаційної роботи
Лесуна Сергія Миколайовича
на тему: «Формування системи фінансової безпеки підприємств ІТ-сфери в
умовах становлення цифрової економіки»

Товариством з обмеженою відповідальністю «Айті-Солюшнс» (код ЄДРПОУ 38239436) враховано результати дисертаційного дослідження аспіранта Національного університету «Чернігівська політехніка» (спеціальність 072 «Фінанси, банківська справа та страхування») Лесуна С.М. щодо використання цифрових інструментів у системі забезпечення фінансової безпеки підприємства. Зокрема, практичне значення мають пропозиції щодо автоматизації фінансового планування і бюджетування, удосконалення управлінської звітності та застосування бізнес-аналітики для моніторингу фінансових показників.

Директор ТОВ «АЙТІ-СОЛЮШНС»

5.05.2026р.

Олександр ЧЕРНОВ



МІНІСТЕРСТВО ОСВІТИ І
НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

вул. Шевченка, 95, Чернігів, 14035,
Україна



тел. +38(0462) 665-103;
факс +38(0462) 665-105
E-mail: csu@stu.cn.ua
www.stu.cn.ua
Код ЄДРПОУ 05460798

MINISTRY OF EDUCATION AND
SCIENCE OF UKRAINE

CHERNIHIV POLYTECHNIC NATIONAL
UNIVERSITY

95, Shevchenko str., Chernihiv, 14035,
Ukraine

42054226 № 422/22-235
Па № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження

Лесуна Сергія Миколайовича на тему:

«Формування системи фінансової безпеки підприємств ІТ-сфери в умовах становлення цифрової економіки»

Основні теоретичні та методичні положення і висновки щодо формування системи фінансової безпеки підприємств ІТ-сфери в умовах становлення цифрової економіки, що розроблені в рамках підготовки дисертаційного дослідження Лесуна Сергія Миколайовича з метою отримання ступеня доктора філософії за спеціальністю 072 «Фінанси, банківська справа, страхування», використані в освітньому процесі кафедри фінансів, банківської справи та страхування Національного університету «Чернігівська політехніка» при розробці методичних матеріалів, а також під час проведення лекційних і практичних занять з навчальних дисциплін: «Фінансовий аналіз», «Фінансове планування у бізнесі», «Фінанси підприємств», «Фінансовий менеджмент».



Ректор

Олег НОВОМЛИНЕЦЬ