Міністерство освіти і науки України
Національний університет кораблебудування ім. адмірала Макарова

Кваліфікаційна наукова праця
на правах рукопису
УДК 338.242.4:005.591.6:332.14(477)

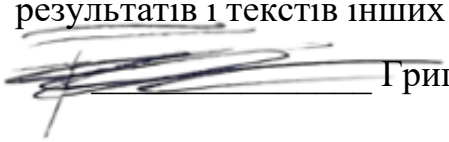
ЧЕРКАСЬКИЙ ГРИГОРІЙ ІГОРОВИЧ

«Організаційно-управлінські механізми забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності»

Спеціальність 073 «Менеджмент»
Галузь знань 07 «Управління та адміністрування»

Подається на здобуття ступеня доктора філософії

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



_____ Григорій ЧЕРКАСЬКИЙ

Науковий керівник: Євгенія БОЙКО, доктор економічних наук, професор

Миколаїв, 2026

АНОТАЦІЯ

Черкаський Г.І. Організаційно-управлінські механізми забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності. Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 073 «Менеджмент». Національний університет кораблебудування ім. адмірала Макарова. Миколаїв. 2026.

Дисертаційна робота присвячена обґрунтуванню теоретико-методичних засад і розробці організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності.

Аналіз теоретико-методичних засад організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності показав, що найбільша частина науковців розглядає інформаційну безпеку як стан захищеності, незначна частина – як функціонування системи засобів. Охарактеризовано інструменти задля підвищення інформаційної безпеки. Наведені принципи інформаційної безпеки є фундаментом, на якому тримається вся система захисту підприємства, і без їх дотримання будь-які дорогі програми чи інструкції стають марними. Визначено елементи механізму формування корпоративної інформаційної безпеки. Аналіз сформованої матриці впливу глобальної економічної турбулентності на систему інформаційної безпеки підприємства демонструє, що кожен дестабілізуючий імпульс глобальної турбулентності містить у собі прихований потенціал для якісного оновлення захисних систем підприємства. Дослідження дозволило чітко диференціювати технічні, фінансові та управлінсько-інформаційні метрики, виявивши їхні обмеження у періоди макроекономічного хаосу та воєнного стану. Для подолання цих обмежень використовують систему з 26 показників-

коефіцієнтів, яка враховує рівень технологічного суверенітету компанії через частку внутрішнього програмно-технічного забезпечення.

Структурно-динамічний аналіз макроекономічних детермінант розвитку бізнес-систем показав, що динаміка Індексу глобалізації KOF України у період 2018–2020 років демонстрували помірне зростання, утримуючи позиції у першій півсотні найбільш глобалізованих країн світу (44–45 місця). Стрімкий підйом України у рейтингу індексу легкості ведення бізнесу з 152-го на 64-те місце з 2014 до 2020 рр. став можливим завдяки тотальній цифровізації (перехід на електронний документообіг, онлайн-реєстрацію, державні цифрові платформи). Проведений аналізі показав, що загальний обсяг валової доданої вартості України за досліджуваний період зріс у фактичних цінах на 4 868 230 млн грн, досягнувши у 2023 році відмітки у 5 822 702 млн грн, що вказує на часткову адаптаційну стабілізацію та відновлення економічної активності бізнес-систем після катастрофічних руйнувань першого року повномасштабного вторгнення. Статистичні дані показують, що в усіх без винятку досліджуваних секторах економіки частка малого підприємництва (разом із мікро-) перевищує 94%, а у середньому по країні становить 99,24% станом на 2024 рік. Здійснено розрахунок коефіцієнта щільності мікробізнесу, який дозволяє розкрити внутрішню глибину структурних деформацій, які відбулися в національній економіці під впливом воєнних та інституційних шоків. Отримані результати демонструють перехід ринкових систем від корпоративно-ієрархічної моделі до ультрадецентралізованої мережевої моделі.

Здійснено оцінку потенціалу розвитку підприємницької діяльності. Визначено, що станом на 2024 рік фіксується часткове відновлення виробничого потенціалу до рівня 9 388,03 млрд грн, але за умови посилення концентрації. Частка великого бізнесу знову зросла до 40,2%, а середнього – утрималася на рівні 39,8%. Економіка адаптувалася, проте її фінансовий потенціал знову сконцентрувався всередині великих корпоративних структур та мереж. Концентрація 80% усього виробничого потенціалу України у 2024

році в руках великого (40,2%) та середнього (39,8%) бізнесу науково доводить, що саме ці дві групи підприємств володіють необхідним інвестиційним ресурсом для побудови повноцінних систем захисту інформації. Аналіз показав, що операційна діяльність мікропідприємств характеризується критичною нестабільністю. Під час системних криз 2014 та 2022 років рівень їхньої операційної рентабельності падав до -30,09% та -6,99% відповідно, що вказує на пряме вимивання капіталу з операційного контуру. Визначено, що протягом 2012–2024 років ключовими драйверами оновлення основних засобів та нематеріальних активів виступали великі корпорації та середні підприємства, які сукупно стабільно контролювали 83–88% усіх капітальних витрат у державі. Зокрема, у 2024 році із загального обсягу інвестицій у 599,97 млрд грн на частку великого бізнесу припало 48,3%, а середнього – 38,2%. Запропоновано методику оцінювання інтегральної фінансово-економічної захищеності підприємств цифрового ринку. Розрахунок інтегрального індексу дозволяє подолати методологічний розрив між фінансовим аналізом і менеджментом безпеки. Розроблена методика оцінки та побудована на її основі стратегічна матриця безпекового позиціонування, що розділяє підприємства за рівнем захищеності.

Запропоновано організаційно-управлінський механізм управління інформаційною безпекою підприємницької діяльності в умовах глобальної економічної турбулентності. Наведено ключові підходи до визначення сутності організаційно-економічного механізму. Запропоновано структурування організаційно-управлінського механізму для забезпечення інформаційної безпеки підприємства, що охоплює три взаємопов'язані субмеханізми, кожен з яких спрямований на усунення відповідного класу дисфункцій.

Досліджено європейський досвід забезпечення інформаційної безпеки підприємницької діяльності та шляхи його імплементації у вітчизняних реаліях. Проаналізовано міжнародні договори та конвенції, що регулюють інформаційну безпеку. Визначено, що ключові елементи європейського

досвіду забезпечення інформаційної безпеки базуються на переході від статичного захисту периметру до філософії комплексної цифрової операційної резилієнтності бізнес-систем. Як показав аналіз, проектування ефективного контуру кіберзахисту та ліквідації цифрових загроз на національному рівні відбувається шляхом адаптації кращих практик країн ЄС та інституційних стандартів Європейського агентства з кібербезпеки. Проведено порівняльний аналіз моделей управління інформаційною безпекою підприємств в ЄС та Україні, який показав наявність суттєвих концептуальних та інституціональних розбіжностей між двома системами. Сформовано стратегічні шляхи імплементації європейського досвіду, що свідчать про модернізацію системи захисту інформаційних ресурсів вітчизняних підприємств в умовах турбулентності та повинно базуватися не на пасивному копіюванні регуляторних вимог, а на принципах цифрової операційної резильєнтності та економічної доцільності.

Розроблено дизайн адаптивної структурно-функціональної моделі розвитку підприємництва в умовах цифрової трансформації. За отриманими результатами проведеного аналізу капітальних інвестицій розроблено концептуальний дизайн адаптивної структурно-функціональної моделі розвитку підприємництва в умовах цифрової трансформації. Модель є багаторівневою системою, що поєднує ресурсні можливості, трансформаційні механізми та стратегічні вектори розвитку підприємницьких структур. Базовий рівень фіксує поточні макроекономічні реалії, а саме потребу у першочерговому фінансуванні основних засобів (обладнання, логістика, інженерні споруди) через безпекові ризики та руйнування та обмеженість вільних фінансових ресурсів у промисловості та будівництві для фінансування класичних ІТ-проєктів «з нуля». Другий рівень, трансформаційні механізми, дозволяє для подолання розриву між потребою в діджиталізації та браком коштів у моделі використання трьох регуляторно-організаційних блоків: механізм технологічного трансферу та абсорбції (B2B-інтеграція), державно-приватне стимулювання та екосистемна платформа хмарної дифузії. На

третьому рівні формуються стратегічні вектори розвитку підприємницької діяльності, які реалізуються через три взаємопов'язані стратегічні вектори, адаптовані під специфіку кожної групи підприємств. Для успішної верифікації запропонованої моделі у межах наукового дослідження розроблено методику оцінки ефективності та моніторингу цифрової трансформації підприємств. Вона переводить якісні теоретичні положення у чіткі кількісні метрики та визначає алгоритм їхнього регулярного відстеження. Доведено, що впровадження запропонованої моделі через механізми B2B-технологічного трансферу, бюджетно-фінансових компенсаторів та екосистемної хмарної дифузії дозволить бізнесу подолати кризові тенденції, забезпечивши високу окупність цифрових інвестицій (ROI_{dig}на рівні 60%) за рахунок системного зниження операційних витрат.

Сформовано стратегічні засади розвитку підприємницької діяльності в умовах глобальної економічної турбулентності. Доведено, що стратегічні засади розвитку підприємств мають бути диференційовані за трьома взаємопов'язаними векторами, що дозволить уникнути уніфікації управлінських рішень та врахувати галузеву специфіку капіталомісткості й поточний рівень діджиталізації бізнесу. Вектор А орієнтований на сектори економіки з високою питомою вагою матеріальних основних засобів, але з критично низьким рівнем інвестування у цифрові активи, а саме переробна промисловість, будівництво, сільське господарство. Особливістю цього вектора є те, що закупівля нового технологічного обладнання, верстатів чи побудова логістичних комплексів має супроводжуватися одночасним розгортанням цифрових систем управління. Вектор Б є базовим для сектору малого та середнього підприємництва (із чисельністю зайнятих 10–249 осіб), а також для підприємств сфери торгівлі та послуг. Особливістю цього вектора є відмова від капіталомістких IT-проєктів «з нуля» на користь готових хмарних рішень. Вектор В орієнтований на високотехнологічні сегменти української економіки: IT-сектор, фінансову діяльність та інноваційні наукомісткі стартапи. Особливістю вектора є сертифікація українських

цифрових продуктів за стандартами GDPR, інтеграцію в європейські цифрові ланцюги створення вартості та масштабування рішень у сферах FinTech, AgTech, GovTech та MilitaryTech; створення консорціумів між національними ІТ-компаніями та вітчизняними індустріальними підприємствами. Сформовано орієнтовані складові стратегії цифрової трансформації для сектору малого підприємництва. Доведено, що згідно з розробленою та верифікованою адаптивною моделлю, на національному рівні державна політика має відійти від уніфікованого (лінійного) підходу до діджиталізації та зосередитися на формуванні трьох стратегічних векторів цифрової трансформації. Запропоновано інтегровану модель забезпечення інформаційною безпекою підприємництва, що не просто фіксує послідовність операцій, а визначає роль, місце та взаємозв'язок процесів підприємництва відповідно до видів економічної діяльності у контексті впливу управлінського чинника. Саме управлінський чинник виступає тим інтегруючим і спрямовуючим вектором, який перетворює розрізнені технологічні та фінансові ресурси на єдину, високоадаптивну систему. Доведено, що від сумарної ефективності процесів на кожному окремому підприємстві безпосередньо залежить не лише його локальна життєздатність, а й загальнонаціональний рівень економічної стійкості, темпи євроінтеграції та динаміка подолання наслідків системної кризи.

Ключові слова: підприємницька діяльність, інформаційна безпека, глобальна турбулентність, організаційно-управлінські механізми, інновації, стратегія розвитку, регіональний розвиток, економіко-математична модель, кібербезпека, бізнес-процеси, цифрова трансформація, цифрові технології, економічна безпека, глобальні та національні виклики.

SUMMARY

Cherkaskyi H. I. Organizational and management mechanisms for ensuring information security in business operations amid global economic turbulence. Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 073 «Management». Admiral Makarov National University of Shipbuilding. Mykolaiv. 2026.

This dissertation is devoted to establishing the theoretical and methodological foundations and developing organizational and managerial mechanisms for ensuring information security in business operations amid global economic turbulence.

The analysis of the theoretical and methodological foundations of organizational and managerial mechanisms for ensuring information security of business activities in conditions of global economic turbulence showed that the majority of scientists consider information security as a state of security, a small part as the functioning of a system of means. The tools for improving information security are characterized. The principles of information security presented are the foundation on which the entire enterprise protection system rests, and without their observance, any expensive programs or instructions become useless. The elements of the mechanism for forming corporate information security are determined. The analysis of the formed matrix of the impact of global economic turbulence on the enterprise information security system demonstrates that each destabilizing impulse of global turbulence contains a hidden potential for a qualitative update of the enterprise's protective systems. The study allowed us to clearly differentiate technical, financial and managerial and information metrics, revealing their limitations during periods of macroeconomic chaos and martial law. To overcome these limitations, a system of 26 indicators-coefficients is used, which takes into account the level of technological sovereignty of the company through the share of internal software and hardware.

Structural and dynamic analysis of macroeconomic determinants of business systems development showed that the dynamics of the KOF Globalization Index of

Ukraine in the period 2018–2020 demonstrated moderate growth, maintaining its position in the top fifty most globalized countries in the world (44–45 places). Ukraine's rapid rise in the Ease of Doing Business Index ranking from 152nd to 64th place from 2014 to 2020 was made possible by total digitalization (transition to electronic document management, online registration, state digital platforms). The analysis showed that the total volume of gross value added of Ukraine during the studied period increased in actual prices by UAH 4,868,230 million, reaching UAH 5,822,702 million in 2023, which indicates a partial adaptive stabilization and restoration of economic activity of business systems after the catastrophic destruction of the first year of the full-scale invasion. Statistical data show that in all sectors of the economy studied without exception, the share of small businesses (including micro-) exceeds 94%, and on average for the country it is 99.24% as of 2024. The microbusiness density coefficient was calculated, which allows us to reveal the internal depth of structural deformations that occurred in the national economy under the influence of military and institutional shocks. The results obtained demonstrate the transition of market systems from a corporate-hierarchical model to an ultra-decentralized network model.

The potential for the development of entrepreneurial activity has been assessed. It has been determined that as of 2024, a partial recovery of production potential to the level of UAH 9,388.03 billion is recorded, but subject to increased concentration. The share of large businesses has again increased to 40.2%, and medium-sized businesses have remained at 39.8%. The economy has adapted, but its financial potential has again concentrated within large corporate structures and networks. The concentration of 80% of the entire production potential of Ukraine in 2024 in the hands of large (40.2%) and medium-sized (39.8%) businesses scientifically proves that it is these two groups of enterprises that have the necessary investment resources to build full-fledged information protection systems. The analysis has shown that the operational activities of micro-enterprises are characterized by critical instability. During the systemic crises of 2014 and 2022, their operating profitability fell to -30.09% and -6.99%, respectively, indicating a

direct leaching of capital from the operating circuit. It was determined that during 2012–2024, the key drivers of the renewal of fixed assets and intangible assets were large corporations and medium-sized enterprises, which together consistently controlled 83–88% of all capital expenditures in the state. In particular, in 2024, out of the total investment volume of UAH 599.97 billion, large businesses accounted for 48.3%, and medium-sized businesses accounted for 38.2%. A methodology for assessing the integral financial and economic security of digital market enterprises is proposed. The calculation of the integral index allows you to overcome the methodological gap between financial analysis and security management. An assessment methodology has been developed and a strategic security positioning matrix has been built on its basis, which divides enterprises by level of security.

An organizational and managerial mechanism for managing information security of business activities in the context of global economic turbulence is proposed. Key approaches to determining the essence of the organizational and economic mechanism are presented. The structuring of an organizational and managerial mechanism for ensuring information security of an enterprise is proposed, which includes three interconnected submechanisms, each of which is aimed at eliminating the corresponding class of dysfunctions.

The European experience of ensuring information security of business activities and ways of its implementation in domestic realities are studied. International treaties and conventions regulating information security are analyzed. It is determined that the key elements of the European experience of ensuring information security are based on the transition from static perimeter protection to the philosophy of comprehensive digital operational resilience of business systems. The analysis showed that the creation of an effective cyber incident response system in Ukraine takes into account the experience of European countries and the recommendations of ENISA (the EU Agency for Cybersecurity). A comparative analysis of enterprise information security management models in the EU and Ukraine was conducted, which showed the presence of significant conceptual and institutional differences between the two systems. Strategic ways of implementing

European experience were formed, which indicate the modernization of the system for protecting information resources of domestic enterprises in turbulent conditions and should be based not on passive copying of regulatory requirements, but on the principles of digital operational resilience and economic feasibility.

A design of an adaptive structural-functional model of entrepreneurship development in the context of digital transformation was developed. Based on the results of the analysis of capital investments, a conceptual design of an adaptive structural-functional model of entrepreneurship development in the context of digital transformation was developed. The model is a multi-level system that combines resource capabilities, transformation mechanisms and strategic vectors of development of business structures. The basic level captures the current macroeconomic realities, namely the need for priority financing of fixed assets (equipment, logistics, engineering structures) due to security risks and destruction and limited free financial resources in industry and construction to finance classic IT projects "from scratch". The second level, transformational mechanisms, allows to overcome the gap between the need for digitalization and the lack of funds in the model using three regulatory and organizational blocks: the mechanism of technology transfer and absorption (B2B integration), public-private stimulation and the ecosystem platform of cloud diffusion. At the third level, strategic vectors of business development are formed, which are implemented through three interconnected strategic vectors adapted to the specifics of each group of enterprises. For the successful verification of the proposed model, a methodology for assessing the effectiveness and monitoring of the digital transformation of enterprises was developed within the framework of scientific research. It translates qualitative theoretical propositions into clear quantitative metrics and defines an algorithm for their regular tracking. It is proven that the implementation of the proposed model through the mechanisms of B2B technology transfer, budgetary and financial compensators and ecosystem cloud diffusion will allow businesses to overcome crisis trends, ensuring a high return on digital investments (ROI_{dig} digat the level of 60%) due to a systematic reduction in operating costs.

Strategic principles for the development of entrepreneurial activity in the conditions of global economic turbulence have been formed. It has been proven that the strategic principles for the development of enterprises should be differentiated according to three interrelated vectors, which will allow avoiding the unification of management decisions and taking into account the industry-specific nature of capital intensity and the current level of business digitalization. Vector A is focused on sectors of the economy with a high share of fixed assets, but with a critically low level of investment in digital assets, namely the processing industry, construction, and agriculture. A feature of this vector is that the purchase of new technological equipment, machine tools, or the construction of logistics complexes should be accompanied by the simultaneous deployment of digital management systems. Vector B is basic for the small and medium-sized business sector (with 10–249 employees), as well as for enterprises in the trade and services sectors. A feature of this vector is the rejection of capital-intensive IT projects "from scratch" in favor of ready-made cloud solutions. Vector B is focused on high-tech segments of the Ukrainian economy: the IT sector, financial activities and innovative science-intensive startups. A feature of the vector is the certification of Ukrainian digital products according to GDPR standards, integration into European digital value chains and scaling solutions in the areas of FinTech, AgTech, GovTech and MilitaryTech; creation of consortia between national IT companies and domestic industrial enterprises. Oriented components of the digital transformation strategy for the small business sector have been formed. It has been proven that according to the developed and verified adaptive model, at the national level, state policy should move away from a unified (linear) approach to digitalization and focus on the formation of three strategic vectors of digital transformation. An integrated model of business processes is proposed, which does not simply record the sequence of operations, but determines the role, place and interrelation of business processes of entrepreneurship in the context of the influence of the management factor. It is the management factor that acts as the integrating and directing vector that transforms disparate technological and financial resources into a single, highly adaptive system.

It is proven that not only its local viability, but also the national level of economic stability, the pace of European integration and the dynamics of overcoming the consequences of the systemic crisis directly depend on the total efficiency of business processes at each individual enterprise.

Keywords: entrepreneurial activity; information security; global turbulence; organizational and management mechanisms; innovation; development strategy; regional development; economic and mathematical model; cybersecurity; business processes; digital transformation; digital technologies; economic security; global and national challenges.

СПИСОК НАУКОВИХ ПУБЛІКАЦІЙ

Статті у наукових фахових виданнях, які включені до міжнародних наукометричних баз

1. Шалухіна В. В., Ляшенко В. М., **Черкаський Г. І.**, Томчук О. О. Сучасні тенденції та вектори цифрової трансформації в Україні. *Ukrainian Journal of Applied Economics and Technology.* 2022. Vol. 7. No 2. pp. 219–225. DOI: https://doi.org/10.36887/2415-8453-2022-2-26 *(0,37 друк. арк., особистий внесок:* формування векторів цифрової трансформації – *0,15 друк. арк.).* **Входить до наукометричних баз реферування та індексування: Index Copernicus International (ICI), Google Scholar, Crossref.**

2. Шалухіна В. В., Ляшенко В. М., **Черкаський Г. І.**, Ващиленко А. М., Сумара А. О. Формування інноваційного потенціалу на макро-, мезо- та мікрорівнях в умовах цифровізації. *Український журнал прикладної економіки та техніки.* 2023. Том 8. No 1. С. 41–46. DOI: https://doi.org/10.36887/2415-8453-2023-1-6 *(0,37 друк. арк., особистий внесок:* визначення складових інноваційного потенціалу суб'єктів господарювання – *0,15 друк. арк.).* **Входить до наукометричних баз реферування та індексування: Index Copernicus International (ICI), Google Scholar, Crossref.**

3. Dubinska, I., Irtyshchev, O., & **Cherkaskyi, H.** (2025). Prerequisites for securing business activities in the conditions of global economic turbulence. *Baltic Journal of Economic Studies*, *11*(1), 86–94. DOI: https://doi.org/10.30525/2256-

0742/2025-11-1-86-94. *(0,56 друк. арк., особистий внесок:* визначено чинники впливу глобальної економічної турбулентності – *0,2 друк. арк.).* **Входить до міжнародних наукометричних баз Web of Science.**

4. Ващиленко А. М., Шалухіна В. В., **Черкаський Г. І.**, Михасько Т. Ю., Бездольний Д. С. Регіональне управління в умовах віртуалізації економіки: роль у інноваційному відновленні, принципи та проблеми. *Актуальні проблеми інноваційної економіки та права*. 2025. № 4. С. 32–37. DOI: https://doi.org/10.36887/2524-0455-2025-4-8 *(0,37 друк. арк., особистий внесок:* напрями віртуалізації економіки в Україні – *0,15 друк. арк.).* **Входить до наукометричних баз реферування та індексування: Index Copernicus International (ICI), Google Scholar, Crossref.**

5. Бойко Є. О., Павленко О. П., Бойко О. С., Арчибісова Д. С., **Черкаський Г. І.** Європейський досвід цифрової трансформації бізнес-процесів в аграрій сфері та шляхи його імплементації у національних реаліях. *Український журнал прикладної економіки та техніки*. 2025. Том 10. No 2. С. 284–288. DOI: https://doi.org/10.36887/2415-8453-2025-2-55 *(0,31 друк. арк., особистий внесок:* європейській досвід цифрової трансформації бізнесу – *0,15 друк. арк.).* **Входить до наукометричних баз реферування та індексування: Index Copernicus International (ICI), Google Scholar, Crossref.**

6. **Черкаський Г. І.** Організаційно-управлінські механізми забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності. *Актуальні питання економічних наук.* 2026. № 23. DOI: https://doi.org/10.5281/zenodo.20456912 *(0,75 друк. арк.).* **Входить до наукометричних баз реферування та індексування: Google Scholar, Index Copernicus International (ICI), Crossref, Національна бібліотека України імені В. І. Вернадського(Наукова періодика України.**

Матеріали апробаційного характеру:

1. Іртищев О. С., Гарагуля А. В., Христофоров В. О., **Черкаський Г. І.** Управління підприємствами в умовах цифрової трансформації. *Менеджмент XXI століття: глобалізаційні виклики:* матеріали VII Міжнародної науково-

практичної конференції (м. Полтава, 18 травня 2023 р.). Полтава: ПДАУ, 2023. С. 202–204.

2. Михасько Т. Ю., Курбатов О. В., Ляшенко В. М., **Черкаський Г. І.**, Іртищев О.С. Управління бізнес-процесами цифрової трансформації. *Сучасні інноваційно-інвестиційні механізми розвитку національної економіки в умовах євроінтеграції*: матеріали X Міжнародної науково-практичної Інтернет-конференції (м. Полтава, 09 листопада 2023 р.) Полтава: Національний університет «Полтавська політехніка імені Юрія Кондратюка», 2023. С.72–74.

3. Іртищев О., Гарагуля А., Бандюк М., Михасько Т., **Черкаський Г.**, Білінський В. Діджиталізація бізнес-процесів в умовах викликів та загроз. *Актуальні вектори відновлювальної трансформації економіки України:* збірник матеріалів наукових економічних читань (м. Миколаїв, 30.11–01.12.2023 р.): у 2 т. Т. 1. Миколаїв: Іліон, 2023. С.60–65.

4. Бандюк М. В., Білінський В. І., **Черкаський Г. І.** Managing business development in a time of global economic turbulence. *Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки*: IX Всеукраїнська науково-практична Інтернет-конференція (м. Полтава, 13 листопада 2024 р.). Полтава, 2024. С. 115–117

5. Paliy V. S., Mykhasko T. U., **Cherkaskyi H. I.,** Sumara A. O. Digitization of business processes as a prerequisite for their development in an unstable environment. *Актуальні аспекти науково-технічного і соціально-економічного розвитку України: погляд молоді*: Всеукраїнська науково-практична конференція молодих вчених і здобувачів вищої освіти (м. Первомайськ, 15 травня 2025 р). Первомайськ, 2025.

ЗМІСТ

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКИХ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ГЛОБАЛЬНОЇ ЕКОНОМІЧНОЇ ТУРБУЛЕНТНОСТІ

1.1. Інформаційна безпека суб'єктів підприємницької діяльності: сутність, складові та інструменти……17

1.2. Глобальна економічна турбулентність: виклики та можливості..26

1.3. Методичні підходи щодо оцінювання рівня інформаційної безпеки в умовах глобальної економічної турбулентності…… 51

Висновки до розділу 1…….63

Список використаних джерел до розділу 1……..65

РОЗДІЛ 2. АНАЛІЗ ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКИХ ПЕРЕДУМОВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ГЛОБАЛЬНОЇ ЕКОНОМІЧНОЇ ТУРБУЛЕНТНОСТІ

2.1. Структурно-динамічний аналіз макроекономічних детермінант розвитку бізнес-систем……69

2.2. Оцінка потенціалу розвитку підприємницької діяльності Причорноморського регіону……96

2.3. Організаційно-управлінський механізм управління інформаційною безпекою підприємницької діяльності в умовах глобальної економічної турбулентності……119

Висновки до розділу 2……...128

Список використаних джерел до розділу 2……133

РОЗДІЛ 3. СТРАТЕГІЧНІ ВЕКТОРИ ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКИХ ЗАСАД ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ГЛОБАЛЬНОЇ ЕКОНОМІЧНОЇ ТУРБУЛЕНТНОСТІ

3.1. Європейський досвід забезпечення інформаційної безпеки підприємницької діяльності та шляхи його імплементації у вітчизняних реаліях……137

3.2. Дизайн адаптивної моделі розвитку підприємницької діяльності в умовах цифрової трансформації……147

3.3. Стратегічні засади розвитку підприємницької діяльності в умовах цифрової трансформації……168

Висновки до розділу 3……..184

Список використаних джерел до розділу 3……186

ВИСНОВКИ……...191

ДОДАТКИ……..199

ВСТУП

Актуальність теми дослідження. Розвиток підприємницької діяльності є важливою складовою національної економіки України та підґрунтям для смарт-спеціалізації окремих її регіонів. Розвиток підприємницької діяльності може забезпечувати не тільки продовольчу безпеку, а й виступати платформою для забезпечення енергетичної, екологічної та, в цілому, економічної безпеки України. На сучасному етапі стрімкого розвитку та поширення цифрових технологій, продуктивність та конкурентоспроможність підприємницької діяльності залежить від здатності галузі та окремих виробників ефективно упроваджувати новітні технології виробництва та управління засновані на нових знаннях й досягненнях у цій сфері.

В умовах сучасного геополітичного та економічного хаосу інформація стала головним стратегічним ресурсом і водночас найбільш уразливим активом бізнесу. Традиційні технічні засоби захисту вже не здатні самостійно протидіяти комплексним кіберзагрозам, масштабним дезінформаційним кампаніям та ризикам витоку даних, які посилюються через кризу. Глобальна турбулентність вимагає від підприємств трансформації підходів до безпеки – переходу від статичної оборони до побудови гнучких, адаптивних систем управління. Саме організаційно-управлінські механізми дозволяють інтегрувати інформаційну безпеку безпосередньо в бізнес-стратегію компанії, забезпечуючи швидку реакцію на інциденти та безперервність процесів. Вони трансформують корпоративну культуру, мінімізують людський фактор як головне джерело ризиків і оптимізують розподіл обмежених фінансових ресурсів під час кризи. Відтак, розробка та впровадження таких комплексних управлінських рішень є критично важливою умовою для виживання, збереження конкурентоспроможності та сталого розвитку вітчизняних підприємств на світовому ринку.

Питання сутності інформаційної безпеки, захисту цифрових активів та специфіки управління процесами в підприємницькій діяльності є предметом прискіпливої аналітичної уваги широкого кола науковців. Зокрема,

фундаментальні засади формування систем кіберзахисту та моделювання інформаційних загроз досліджували такі вчені, як В. П. Горбулін, О. Г. Додонов, О. В. Котенко, Р. В. Грищук, В. А. Хорошко, С.І. Міненко, а також зарубіжні фахівці Д. Блаклі, М. Е. Вітмен та Г. Дж. Маттіорд. Проблеми стратегічного менеджменту, реінжинірингу та конструювання наскрізних бізнес-процесів в умовах становлення цифрової економіки висвітлено у працях М. Хаммера, Дж. Чампі, Т. Давенпорта, В. М. Гейця, І.І. Надточій, І.С. Крамаренко, І.О. Іртищева, К.С. Шапошнікова, О. С. Федоніна, Л. І. Федулової, а сучасні аспекти проактивної адаптації бізнесу до воєнних шоків та оцінки індексів цифрової інтенсивності малих суб'єктів підприємництва відображено у дослідженнях О. В. Романюк, Ю. О. Джерелюк та Н. Н. Попович. Водночас інституційні засади забезпечення економічної безпеки підприємництва та мінімізації управлінських ризиків малого і середнього бізнесу детально проаналізовано у працях Є.О. Бойко, З. С. Варналія, Т. Г. Васильціва, О. М. Ляшенко та Г. В. Козаченко.

Разом з тим, незважаючи на наявні результати теоретико-методичного обґрунтування організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності, на сьогоднішній день відсутні чіткі концептуальні засади формування інтегрованих цифрових систем на принципах кластеризації бізнесу та наскрізного процесного управління. Більшість існуючих підходів є фрагментальними, розглядають інформаційну безпеку виключно як технологічну функцію, відірвану від загальної фінансово-економічної стратегії підприємства та цілей сталого розвитку. Залишаються невизначеними механізми безшовної комунікації між рівнями реалізації стратегічних цілей малого та середнього підприємництва, що унеможливлює оперативне усунення ринкових асиметрій та подолання безпекових шоків. Крім того, гостро відчувається брак комплексних моделей, які б пов'язували технологічний трансфер, мінімізацію виробничого браку та впровадження процесних інновацій із чіткими критеріями економічної

ефективності й окупності інвестицій, що стримує системну капіталізацію реального сектору економіки в умовах євроінтеграції.

Метою дослідження є обґрунтування теоретико-методичних та практичних засад організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності. Відповідно до поставленої мети визначені наступні завдання:

- розкрити теоретичні основи інформаційної безпеки підприємницької діяльності;
- провести структурно-динамічний аналіз макроекономічних детермінант розвитку бізнес-систем;
- здійснити оцінювання потенціалу розвитку підприємницької діяльності регіонів;
- обґрунтувати організаційно-управлінський механізм забезпечення інформаційної безпеки підприємницької діяльності;
- систематизувати закордонний досвід інформаційної безпеки підприємницької діяльності в контексті глобальної економічної турбулентності;
- розробити дизайн адаптивної моделі розвитку підприємницької діяльності в умовах цифрової трансформації;
- обґрунтувати стратегічні пріоритети інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності.

Об'єктом дослідження є процес формування організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності.

Предметом дослідження є теоретико-методичні основи та науково-практичні підходи щодо формування організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності.

Методи дослідження. Теоретико-методологічний фундамент

дослідження сформовано на основі фундаментальних положень сучасної економічної теорії, концепції сталого розвитку, загального та стратегічного менеджменту, а також фундаментальних праць провідних вітчизняних і зарубіжних учених у сфері цифровізації та безпеки економічних систем. Для досягнення окресленої мети та виконання завдань, в роботі використано загальнонаукові та економічні методи: *аналізу та синтезу* – для здійснення економічної оцінки розвитку підприємницької діяльності; *систематизації та узагальнення* – для виявлення передумов, індикаторів та формуючих факторів глобальної турбулентності для економіки України; *просторовий підхід*— застосовано з метою комплексного аналізу дифузії цифрових інструментів у межах організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності, а також для визначення географічних та секторальних меж технологічного трансферу в реальному секторі економіки; *статистичні* – для структурно-динамічний аналіз макроекономічних детермінант розвитку бізнес-систем; *графічний і картографічний* – для наочного відображення результатів дослідження розвитку підприємництва в умовах турбулентної економіки; *рейтингування* – для впорядкування характеристик, індикаторів, що мають вплив на інформаційну безпеку підприємницької діяльності, комп'ютерної обробки та аналізу інформації за допомогою пакету прикладних програм (MS Office, Statistica) для здійснення економічних розрахунків в процесі дослідження, для виконання завдань дослідження.

Інформаційно-емпіричну основу дослідження становлять фундаментальні праці вітчизняних і зарубіжних учених, присвячені обґрунтуванню та практичній реалізації організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємництва в умовах глобальної турбулентності. Джерельну базу роботи також формують законодавчі та нормативно-правові акти України, інституційні директиви ЄС, офіційні статистичні матеріали Державної служби статистики України, аналітичні доповіді профільних міністерств і відомств, монографічні

дослідження, матеріали міжнародних науково-практичних конференцій, тематична періодика, а також релевантні ресурси глобальної мережі Інтернет.

Наукова новизна одержаних результатів. У дисертаційній роботі викладено теоретико-методичні засади і практичні рекомендації щодо удосконалення організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності. Наукові результати дослідження орієнтовані на розроблення комплексу сучасних економічних механізмів та моделей інформаційної безпеки підприємницької діяльності. Найбільш важливими науковими результатами, що характеризуються новизною, є наступні положення:

удосконалено:

- адаптивну модель розвитку підприємництва в умовах цифрової трансформації, яка, на відміну від існуючих підходів, інтегрує макроекономічні тренди капіталізації з мікроекономічними важелями ефективності. Для верифікації моделі розроблено систему індикаторів та моніторингу, що дозволила зафіксувати глибокі структурні диспропорції у вітчизняному реальному секторі, зокрема критично низьку частку інвестицій у нематеріальні активи переробної промисловості та регрес у використанні передових технологій. Виявлено негативні тенденції розвитку е-комерції через надмірне зростання кількості онлайн-платформ на 8,2% на тлі низької частки інтернет-продажів (3,8%). Це доводить, що стихійна цифровізація без оптимізації операційних витрат є неефективною.

- організаційно-управлінський механізм управління інформаційною безпекою підприємницької діяльності в умовах глобальної економічної турбулентності, що на відміну від існуючих, розуміють як складну систему впливу на функціонування підприємництва, що охоплює законодавче, цифрове, інформаційно-методичне та інституційне забезпечення, інструменти (аналітичні, фінансові, організаційні, технологічні), фактори впливу (воєнно-політичні, геополітичні, макроекономічні, ринкові, регуляторні, фінансово-

економічні, організаційно-технологічні, соціально-психічні) та специфічні особливості (фінансово-економічний моніторинг виступає основною для трансформації контуру технологічного захисту), а також зорієнтована на зміну особистих та спільних ціннісних орієнтирів колективної відповідальності за збереження інформаційного капіталу та трансформація системи інформаційної безпеки із системи обмежень у систему спільної життєстійкості (резильєнтності). Це забезпечує внутрішню консолідацію підприємства та підтримує стабільні індекси його ділової активності та глобальної конкурентоспроможності незалежно від амплітуди коливань зовнішнього турбулентного середовища.

- систему стратегічних векторів підприємницької діяльності в умовах глобальної економічної турбулентності, що на відміну від існуючих, диференційовано за трьома взаємопов'язаними векторами, що дозволить уникнути уніфікації управлінських рішень та врахувати галузеву специфіку капіталомісткості й поточний рівень діджиталізації бізнесу. Особливістю вектора А є те, що закупівля нового технологічного обладнання, верстатів чи побудова логістичних комплексів має супроводжуватися одночасним розгортанням цифрових систем управління та спрямованим на переробну промисловість, будівництво, сільське господарство. Вектор Б є базовим для сектору малого та середнього підприємництва (із чисельністю зайнятих 10–249 осіб), а також для підприємств сфери торгівлі та послуг, що передбачає відмову від капіталомістких ІТ-проєктів «з нуля» на користь готових хмарних рішень. Вектор В орієнтований на високотехнологічні сегменти української економіки (ІТ-сектор, фінансову діяльність та інноваційні наукомісткі стартапи) особливістю є сертифікація українських цифрових продуктів за стандартами GDPR, інтеграцію в європейські цифрові ланцюги створення вартості та масштабування рішень у сферах FinTech, AgTech, GovTech та MilitaryTech; створення консорціумів між національними ІТ-компаніями та вітчизняними індустріальними підприємствами;

- методику оцінки інтегральної фінансово-економічної захищеності підприємств, яка, на відміну від існуючих підходів фінансового аналізу, пов'язує коефіцієнти ліквідності та капітальних інвестицій із вартісною оцінкою безпекових ризиків. Це дозволяє диференціювати управлінські стратегії системи інформаційної безпеки між капіталомісткою (CAPEX) та сервісною (OPEX) моделями захисту на основі масштабу та реального фінансового буфера підприємства;

набули подальшого розвитку:

- теоретико-методичні засади організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності, що дозволяють диференціювати технічні, фінансові та управлінсько-інформаційні метрики, виявивши їхні обмеження у періоди макроекономічного хаосу та воєнного стану. Сформована матриці впливу глобальної економічної турбулентності на систему інформаційної безпеки підприємства демонструє, що кожен дестабілізуючий імпульс глобальної турбулентності містить у собі прихований потенціал для якісного оновлення захисних систем підприємства;

- порівняльний аналіз моделей управління інформаційною безпекою підприємств в ЄС та Україні, який показав наявність суттєвих концептуальних та інституціональних розбіжностей між двома системами, що дозволило сформувати стратегічні шляхи імплементації європейського досвіду. Це свідчать про необхідність модернізації системи захисту інформаційних ресурсів вітчизняних підприємств в умовах турбулентності та базування не на пасивному копіюванні регуляторних вимог, а на принципах цифрової операційної резельєнтності та економічної доцільності;

- результати структурно-динамічного аналізу макроекономічних детермінант розвитку бізнес-систем, що дозволять виокремити децентралізований контур контрагентів та партнерів, враховують критично високу щільність мікросуб’єктів та фізичних осіб-підприємців у структурі національної економіки. Впровадження цього контуру науково обґрунтовує

необхідність відмови від застарілих концепцій локального захисту корпоративного периметра на користь гнучкої архітектури нульової довіри. Практична реалізація сформованого підходу дозволяє великим та середнім підприємствам здійснювати безперервний експрес-скоринг рівня кібергігієни зовнішніх суб'єктів, що підключаються до їхніх інформаційних ресурсів. Представлена модель мінімізує вразливість бізнес-систем до масових і скоординованих атак через ланцюги постачання в умовах воєнного стану.

- **Практичне значення одержаних результатів** полягає в можливості застосування сформульованих практичних рекомендацій щодо управління інформаційною безпекою підприємницької діяльності. Вищевказані рекомендації використовуються у практичній діяльності ГО “Українська асоціація центрів підтримки бізнесу” (довідка впровадження 2406/01-002 від 24.06.2026 року), ГО “ВГО “Поруч”” (24.02.2026 № 15-ВНА/07-25). Теоретико-методичні засади організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності впроваджено в освітній процес Національного університету кораблебудування імені адмірала Макарова МОН України.

Особистий внесок дисертанта. Всі наукові результати, викладені в дисертації, належать автору особисто. З наукових публікацій, що у співавторстві, використані лише ті матеріали, які є результатом особистої праці здобувача.

Апробація результатів дисертації. Основні положення і результати дисертаційного дослідження доповідались і обговорювались на VI Всеукраїнській науково-практичній Інтернет-конференції з міжнародною участю «Управління ресурсним забезпеченням господарської діяльності підприємства реального сектора економіки» (м. Полтава, 27 жовтня 2022 р); VII Міжнародній науково-практичній конференції «Менеджмент XXI століття: глобалізаційні виклики» (м. Полтава, 18 травня 2023 р.); X Міжнародній науково-практичній Інтернет-конференції «Сучасні

інноваційно-інвестиційні механізми розвитку національної економіки в умовах євроінтеграції» (м. Полтава, 09 листопада 2023 р.); наукових економічних читаннях «Актуальні вектори відновлювальної трансформації економіки України» (м. Миколаїв, 30.11-01.12.2023 р.); IX Всеукраїнській науково-практичній Інтернет-конференції «Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки», (м. Полтава, 13 листопада 2024 р.); Всеукраїнській науково-практичній конференції молодих вчених і здобувачів вищої освіти «Актуальні аспекти науково-технічного і соціально-економічного розвитку України: погляд молоді» (м. Первомайськ, 15 травня 2025 р.).

Публікації. За результатами дисертаційного дослідження опубліковано 11 наукових праць загальним обсягом 2,73 авт. арк., з яких особисто автору належить 1,55 авт. арк. Із них: 5 статей у наукових фахових виданнях, 1 – стаття у наукометричній базі Web of Science, 5 – у матеріалах науково-практичних конференцій.

Структура та обсяг роботи. Дисертація складається з анотації, вступу, трьох розділів, висновків, списку використаних джерел (у першому розділі 35 найменувань, у другому – 19 найменувань і у третьому – 28 найменувань), 3 додатки. Повний обсяг дисертації становить 205 сторінок, з них основний текст 175 – сторінок, анотація – 14 сторінок, список використаних джерел – 10 сторінок, додатки – 6 сторінок.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКИХ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ГЛОБАЛЬНОЇ ЕКОНОМІЧНОЇ ТУРБУЛЕНТНОСТІ

1.1. Інформаційна безпека суб'єктів підприємницької діяльності: сутність, складові та інструменти

Сьогодні інформаційна безпека – це вже не просто робота системного адміністратора, який оновлює антивіруси, а питання виживання всього бізнесу. Коли компанія чітко розуміє сутність цієї безпеки, вона перестає сприймати захист даних як статтю збитків і починає бачити в ньому стратегічну перевагу. Розбір безпеки на конкретні складові (технічну, правову, кадрову) допомагає керівнику закрити реальні діри, через які зазвичай витікають гроші та репутація. Без цього фірма захищається наосліп, витрачаючи бюджети на дорогі програми, але залишаючи відкритими двері для банальних помилок персоналу чи юридичних пасток. Правильно підібрані інструменти – від шифрування до чітких посадових інструкцій – створюють реальний імунітет проти кібератак чи зливу бази клієнтів конкурентам. Зрештою, саме сильна система захисту інформації робить бізнес надійним партнером в очах інвесторів та клієнтів, які сьогодні найбільше цінують конфіденційність. У підсумку, вивчення цих інструментів дає компанії реальну стійкість, дозволяючи їй працювати без паніки навіть під час серйозних ринкових потрясінь.

Цілком обґрунтованою є позиція М. О. Шевчука, який наголошує, що в умовах тривалого протистояння гібридним та повномасштабним формам військової агресії рф, Україна зіткнулася з імперативом експрес-модернізації сектору безпеки й оборони. Дослідник справедливо зауважує, що захист суверенітету, територіальної цілісності та базових суспільно-економічних цінностей держави має реалізуватися у стислі терміни та в умовах жорсткого лімітування ресурсного забезпечення [1, с. 136].

Сьогодні інформаційна безпека підприємств перестає бути суто корпоративним питанням. У теперішніх реаліях кібератаки, дезінформація та спроби дестабілізувати роботу комерційного сектору є прямим продовженням цієї гібридної агресії. Для будь-якої компанії захист власних даних – від технологічних секретів до баз даних клієнтів – став питанням збереження працездатності в умовах жорсткого дефіциту часу та грошей, про які згадує дослідник. Саме тому організаційні та управлінські рішення сьогодні мають бути максимально гнучкими: коли ресурси обмежені, перемагає не той, хто купує найдорожче софт-забезпечення, а той, хто вміє швидко адаптувати структуру управління під нові загрози.

Розглядаючи чинники стратегічної стійкості, В. А. Ліпкан, Л. С. Харченко та О. В. Логінов справедливо підкреслюють, що ефективна протидія масштабній агресії та збалансований розвиток національного інформаційного простору визначаються не стільки механічним нарощуванням технічних потужностей обміну даними, скільки формуванням високої культури безпеки. На думку дослідників, ключовою умовою захисту критичних інформаційних ресурсів є усвідомлена й скоординована діяльність усіх учасників інформаційних відносин, що безпосередньо актуалізує потребу в глибокому теоретичному осмисленні сутності категоріального апарату інформаційної безпеки [2, с. 46].

Погляди дослідників чітко вказують на те, що технічний захист – це лише верхівка айсберга. Справжня безпека починається тоді, коли кожен менеджер і рядовий працівник підприємства усвідомлює цінність інформації та наслідки її втрати. У часи, коли бізнес змушений оперувати в умовах воєнного стану та економічної нестабільності, саме людський фактор та організаційні прорахунки стають найслабшою ланкою. Тому «чітке розуміння сутності», про яке пишуть автори, має трансформуватися у конкретні управлінські дії: створення зрозумілих інструкцій, регулярне навчання персоналу та побудову такої корпоративної культури, де безпека є спільним

обов'язком, а не просто турботою ІТ-відділу. Розглянемо дефініцію поняття «інформаційна безпека» наведену в табл. 1.1.

Таблиця 1.1

Дефініція поняття «інформаційна безпека»

Автор	Визначення поняття
Шевчук М. О. [1]	«стійкий стан інформаційної сфери, що забезпечує її цілісність і захищеність об’єктів за наявності негативних внутрішніх і зовнішніх впливів» [1, с. 136]. Важливою методологічною перевагою такого формулювання є те, що в його основу покладено суб'єктивний чинник — усвідомлення людиною власних цінностей, потреб (життєво важливих інтересів) та цілей розвитку.
Ліпкан В. А., Харченко Л. С., Логінов О. В. [2]	структурують цю категорію через призму захищеності інформаційного середовища, забезпечення інформаційного суверенітету та підтримання легітимно встановлених правил перебігу інформаційних процесів. Узагальнення їхніх поглядів дозволяє стверджувати, що інформаційна безпека є складною функцією держави та водночас специфічною системою суспільних відносин, яка покликана нівелювати потенційні й реальні деструктивні впливи на інтереси особи, соціуму та економічних суб'єктів.
Данильян О. Г., Дзьобань О. П., Панов М. І.[3]	«Захищеність об’єкта від інформаційних загроз або негативних впливів, пов’язаних з інформацією та збереженням у таємниці даних про певний об’єкт, що становлять державну таємницю».
Гурковський В.І. [4]	як динамічну систему суспільних відносин, спрямовану на нівелювання інформаційних загроз інтересам особи, суспільства та владних інститутів [4, с. 82]. Науковець доводить, що належний рівень захищеності інформаційного середовища є першоосновою для збереження духовного та матеріального капіталу країни, її суверенітету й прогресивного поступу. При цьому ключовим рушієм підтримання цього стану вчений визначає системну та цілеспрямовану державну політику із захисту й гарантування національних інтересів в інформаційній сфері.
Баранов О. П. [5]	«стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі» [5, с. 112]. Важливою теоретико-методологічною перевагою концепту автора є чітка типізація джерел деструктивного впливу. Зокрема, дослідник пов'язує загрози із «неповнотою, несвоєчасністю, недостовірністю інформації та несанкціонованим її поширенням», а також із «негативними наслідками функціонування інформаційних технологій» [5, с. 112]
Шатун В. Т. [6]	«стан захищеності національних інтересів України в інформаційній сфері від загроз особі, суспільству і державі» [6, с. 94]. Цінність цього визначення полягає у предметній типізації деструктивних тригерів, які автор пов'язує із «неповнотою, несвоєчасністю інформації, несанкціонованим її поширенням і використанням», а також із «негативним інформаційним впливом та негативними наслідками функціонування інформаційних технологій» [6, с. 94].

Джерело: узагальнено автором на основі [1, с. 138; 2, с. 25–30; 3, с. 165; 4, с. 74; 5, с. 60–62; 6, с. 175;]

Отже, найбільша частина науковців розглядає інформаційну безпеку як стан захищеності, незначна частина – як функціонування системи засобів. Такий поділ у наукових поглядах чітко підкреслює подвійну природу інформаційної безпеки. З одного боку, підприємству дійсно необхідний певний стабільний рівень або «стан» захищеності, за якого конфіденційні дані та комерційна таємниця перебувають під надійним контролем. З іншого боку, в умовах постійних криз та гібридних загроз жоден статичний стан не може тривати довго, тому безпеку варто сприймати саме як безперервне «функціонування системи». Якщо компанія зациклиться лише на першому підході, вона ризикує побудувати занадто жорстку оборону, яка швидко застаріє під натиском нових викликів. Тому сучасний організаційно-управлінський механізм має об'єднати ці дві концепції: створити міцну базу захисту, але водночас забезпечити її постійне, гнучке функціонування та швидку адаптацію до змін у зовнішньому середовищі.

Вважаємо, що інформаційна безпека суб’єкта підприємницької діяльності в умовах глобальної економічної турбулентності необхідно розглядати як динамічний стан захищеності та одночасно безперервний процес функціонування системи організаційно-управлінських, технічних і правових засобів, що забезпечує цілісність, конфіденційність і доступність інформаційних ресурсів підприємства, а також його здатність гнучко адаптуватися до нових кіберзагроз і зберігати стабільність бізнес-процесів у кризовому середовищі.

Ясінська А. І. вважає, що «Задля захисту інформації і з метою збереження її конфіденційності та неправомірного використання доцільним є аналізування в першу чергу джерел загроз та визначення наслідків від їхнього впливу, тому для глибшого розуміння даного процесу варто системно впроваджувати певні заходи щодо інформаційної безпеки шляхом реалізації концептуальної моделі» (рис. 1) [8].

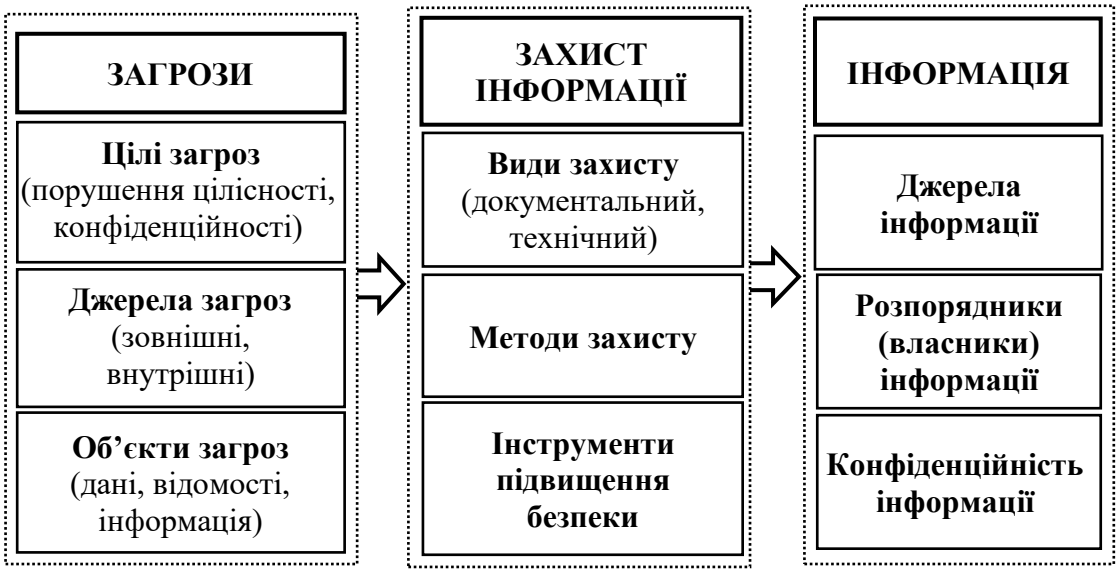


Рис. 1.1. Концептуальна модель інформаційної безпеки підприємства

Джерело: [8].

Логіка запропонованого дослідницею підходу є критично важливою для сучасного бізнесу, адже в умовах хаотичних змін підприємства не мають розкоші витрачати ресурси на захист від уявних чи другорядних ризиків. Системний аналіз джерел загроз дозволяє чітко розділити їх на зовнішні (цілеспрямовані кібератаки, промислове шпигунство, збої в критичній інфраструктурі) та внутрішні (помилки або умисні дії власного персоналу). Концептуальна модель інформаційної безпеки, представлена на рисунку 1.1, якраз і виступає тим каркасом, який пов'язує виявлені загрози із конкретними організаційними діями. Вона дозволяє менеджменту бачити повну картину: від моменту виникнення ризику до впровадження захисного інструменту, перетворюючи хаотичні спроби захиститися на чітку й керовану систему.

Використання сучасних інструментів інформаційної безпеки є головною умовою для переходу від теоретичних планів захисту до реальної відсічі загрозам на підприємстві. Без чітко підібраного інструментарію навіть найкраща безпекова стратегія залишається лише набором декларацій на папері, який не захистить від реального злому чи витоку даних. У кризових умовах ці інструменти, що включають технічні програми, правові обмеження

та кадрові перевірки, діють як єдиний щит, мінімізуючи вплив людського фактора та системних збоїв.

Правильний вибір засобів автоматизації безпеки дозволяє бізнесу миттєво виявляти аномалії в мережі та блокувати кібератаки ще на етапі їхнього зародження, що критично важливо в умовах дефіциту часу. Окрім того, наявність дієвих інструментів захисту інформації суттєво знижує фінансові ризики компанії, оберігаючи її від мільйонних збитків через простої або судові позови за злив клієнтських баз. Зрештою, саме практичне впровадження надійних захисних інструментів демонструє зрілість менеджменту та робить підприємство прогнозованим і життєздатним партнером на нестабільному ринку. Інструменти підвищення інформаційної безпеки наведено на рис. 1.2.

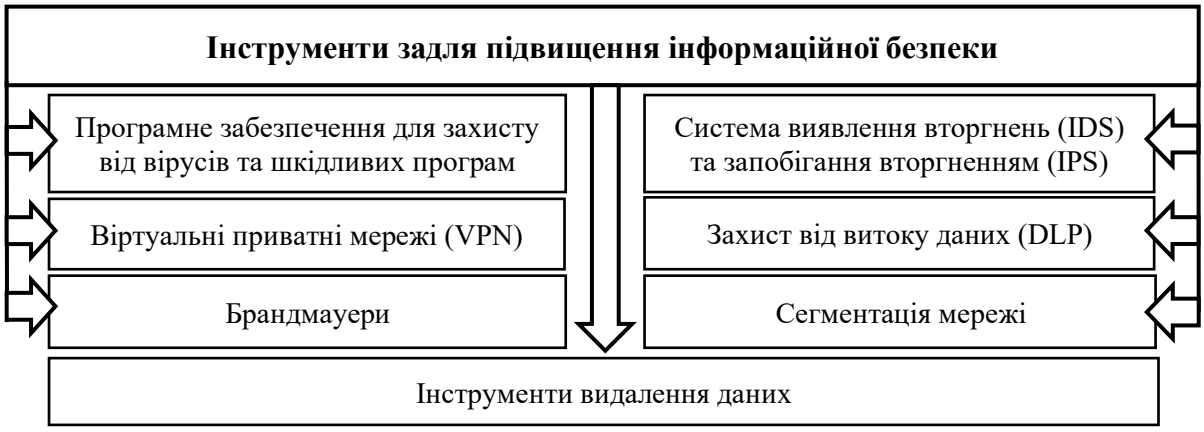


Рис. 1.2. Інструменти задля підвищення інформаційної безпеки

Джерело: узагальнено автором на основі [8].

Загалом увесь масив інструментів інформаційної безпеки підприємства можна розділити на три взаємопов'язані групи, де кожна закриває свій спектр уразливостей. Першу групу становлять технічні та програмні засоби, які безпосередньо захищають цифрову інфраструктуру: сюди відносяться антивірусні комплекси, брандмауери, системи шифрування каналів зв'язку, резервне копіювання даних та DLP-системи, що блокують несанкціоноване перенесення файлів. Друга група охоплює організаційно-кадрові інструменти, спрямовані на роботу з персоналом та побудову бізнес-процесів, оскільки саме

люди найчастіше стають причиною інцидентів. До них належать регулярний інструктаж працівників, моделювання фішингових атак для перевірки пильності, розмежування прав доступу за принципом мінімальної необхідності та чіткий алгоритм дій команди у разі виявлення кризової ситуації. Нарешті, третя група включає нормативно-правові інструменти, які створюють легітимне поле для захисту комерційної таємниці. Це підписання з працівниками та контрагентами договорів про нерозголошення (NDA), розробка внутрішніх регламентів поводження з конфіденційною інформацією та приведення політик компанії у відповідність до національного законодавства та міжнародних стандартів безпеки. Тільки одночасне використання цих трьох груп інструментів дозволяє перекрити більшість векторів атак і забезпечити реальну стійкість бізнесу.

Принципи інформаційної безпеки є фундаментом, на якому тримається вся система захисту підприємства, і без їх дотримання будь-які дорогі програми чи інструкції стають марними. Вони визначають логіку поведінки компанії у цифровому просторі, перетворюючи розрізнені технічні налаштування на чітку, послідовну філософію бізнесу. Класична тріада цих принципів – конфіденційність, цілісність і доступність даних – гарантує, що важлива інформація потрапить лише до потрібних рук, не буде непомітно змінена зловмисниками та залишиться доступною для роботи в будь-який момент. Усвідомлення цих орієнтирів керівництвом дозволяє правильно розставити пріоритети, інвестуючи ресурси у захист дійсно критичних активів, а не всього підряд. Більше того, чіткі принципи безпеки формують здорову корпоративну культуру, де кожен працівник розуміє межі своєї відповідальності та не вчиняє дій, які можуть загрожувати фірмі. Зрештою, саме непохитне дотримання базових принципів забезпечує компанії довгострокову стійкість, дозволяючи зберігати репутацію та довіру клієнтів навіть під час масштабних криз. Принципи інформаційної безпеки в компанії наведено на рис.1.3.

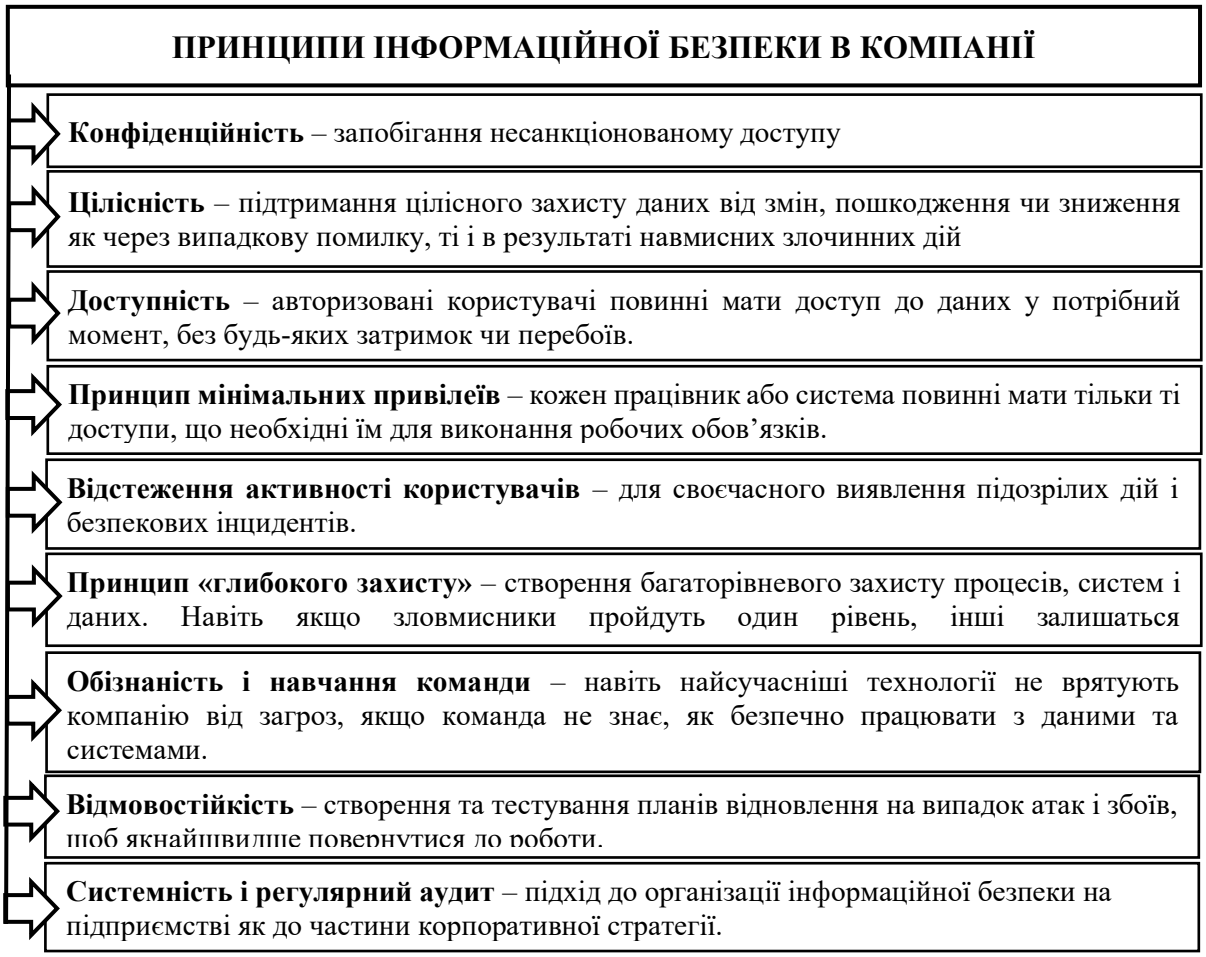


Рис. 1.3. Принципи інформаційної безпеки в компанії

Джерело: узагальнено автором на основі [9].

Таким чином, ефективність інформаційного захисту компанії досягається лише тоді, коли відстеження активності користувачів, «глибокий захист», мінімальні привілеї, навченість команди, відмовостійкість та регулярний аудит діють не окремо, а в синергії як єдиний управлінський комплекс. Жоден, навіть найсучасніший інструмент ешелонованої оборони не спрацює, якщо рядовий співробітник через низьку обізнаність відкриє фішинговий лист, або якщо через відсутність чіткого аудиту менеджмент вчасно не помітить надмірних прав доступу в системі. Обмеження прав до мінімально необхідного рівня суттєво звужує простір для внутрішніх помилок, а постійний моніторинг дій користувачів та забезпечення відмовостійкості інфраструктури дозволяють бізнесу миттєво реагувати на інциденти та продовжувати роботу навіть під час технічних збоїв чи цілеспрямованих атак.

У підсумку, саме системне поєднання цих принципів перетворює інформаційну безпеку з хаотичного гасіння кризових пожеж на керований, гнучкий та життєздатний механізм, здатний тримати удар в умовах загальної економічної турбулентності.

У своїх наукових працях В. І. Чубаєвського обґрунтовує, що еволюція та систематизація теоретичних підходів до забезпечення економічної і, зокрема, інформаційної безпеки бізнесу заклали теоретичний фундамент для проектування цілісних механізмів захисту корпоративних даних [7, с. 54]. Науковець формує компонентну структуру цього механізму, пропонуючи розглядати його крізь призму взаємозв'язку цільових, суб'єктно-об'єктних, функціональних та інструментальних (методичних) складових (табл. 1.2)» [10].

Системний підхід дозволяє чітко розмежувати ролі та зони відповідальності всередині компанії, що є критично важливим під час кризи. Суб’єкти цього механізму (керівництво, служба безпеки, IT-фахівці та кожен окремий працівник) мають діяти як злагоджена команда, де кожен розуміє свої завдання та функції. Водночас об’єктами захисту стають не лише сервери чи бази даних, а й самі бізнес-процеси та канали комунікації, які в умовах нестабільності є найбільш вразливими. Запропонована у таблиці 1.2 структура елементів дає менеджменту готовий алгоритм дій: вона дозволяє підпорядкувати методи управління конкретним завданням, а самі завдання – головній меті підприємства, якою сьогодні є збереження життєздатності та безперервності бізнесу. Такий підхід перетворює інформаційну безпеку з ізольованого технічного процесу на невіддільну частину загальної системи економічної безпеки корпорації.

Характеристика методів моделювання є тим інструментом, який дозволяє бізнесу перестати вгадувати, звідки прийде наступна загроза, і почати діяти на випередження. Без попереднього моделювання будь-які безпекові заходи впроваджуються наосліп, що в умовах кризи веде до перевитрати бюджетів та появи «сліпих зон» у захисті компанії.

Таблиця 1.2

Елементи механізму формування корпоративної інформаційної безпеки

Елементи	Коротка характеристика
Об’єкти	Структурні елементи корпоративного інформаційного простору: інформаційне поле; віртуальна реальність; інформаційний процес; інформаційна культура; технічні засоби; технологічні засоби; регламенти та норми
Суб’єкти	Служба безпеки, ІТ-служба, юридична служба, топ-менеджери, відповідальні за процеси та центри фінансової відповідальності, окремі особи, що мають доступ до конфіденційної інформації
Мета	комплексного організаційно-управлінського інструментарію захисту корпоративних інформаційних ресурсів суб’єктів підприємництва, що забезпечує мінімізацію ризиків, нівелювання ринкових асиметрій та безперешкодну реалізацію їхніх стратегічних економічних інтересів.
Завдання	Забезпечення цілісності, конфіденційності та доступності інформації
Функції	Ідентифікація загроз інформаційній безпеці; формування організаційної структури служби безпеки; оцінювання та аналіз загроз інформаційній безпеці; розробка стратегії захисту та планів захисту корпоративної інформації; координація роботи служби безпеки з іншими службами підприємства
Методи впливу	Економічні методи впливу в межах організаційно-управлінських механізмів цифрової трансформації спрямовані на оцінювання фінансової доцільності інвестицій у безпеку, моніторинг ефективності використання капіталу суб’єктів малого та середнього підприємництва та мінімізацію трансакційних витрат у межах інтегрованих цифрових систем. Інструментарій стратегічного позиціонування та ризик-менеджменту в цій групі базується на комплексному аналізі бізнес-процесів, застосуванні системи збалансованих показників, розробці стратегічних карт, побудові інтерактивних карт ризиків, а також на використанні методів інтегрального та прикладного інформаційного аналізу, що дозволяє декомпозувати загальні безпекові цілі до рівня конкретних бізнес-операцій.
	Організаційно-правові методи впливу формують нормативно-інституційну платформу функціонування суб’єктів підприємництва, легітимізують інформаційні процеси та забезпечують безшовну взаємодію рівнів управління в умовах цифрової трансформації. Процесний контур цієї групи методів базується на моделюванні бізнес-процесів (зокрема, з використанням сучасних графічних нотацій BPMN 2.0 та IDEF0), що дозволяє здійснити чіткий наскрізний розподіл функцій, декомпозувати завдання менеджменту та оперативно виявити «вузькі місця» й потенційні зони витоку інформації.

Джерело: [10].

Моделювання дає змогу створити точний цифровий чи логічний дублікат безпекової інфраструктури підприємства та протестувати її на міцність у безпечних умовах, без реального ризику для бізнес-процесів. Завдяки цьому менеджмент може заздалегідь прорахувати сотні сценаріїв розвитку подій – від банальної технічної помилки чи фішингової атаки на

персонал до масштабного збою інфраструктури через воєнні дії. Особлива цінність цих методів під час глобальної турбулентності полягає в оптимізації ресурсів: вони чітко показують, які діри в обороні є критичними й вимагають негайних інвестицій, а які ризики є мінімальними. Зрештою, саме детальна характеристика та застосування методів моделювання перетворюють інформаційну безпеку з пасивного захисту на проактивну стратегію, дозволяючи компанії зберігати стійкість та керованість за будь-яких зовнішніх штормів. Характеристика методів моделювання корпоративної інформаційної безпеки наведено в таблиці 1.3.

У науковій практиці та реальному управлінні методи моделювання корпоративної інформаційної безпеки традиційно поділяють на два взаємопов'язані рівні: фундаментальний та аналітичний. Перший рівень базується на класичних теоретичних моделях розмежування доступу, серед яких ключове місце посідають концепції Bell-LaPadula та Biba, що забезпечують жорсткий контроль конфіденційності та цілісності даних через систему мандатних обмежень за принципом «не читай/не пиши» вище або нижче визначеного рівня повноважень. Комерційний сектор частіше схиляється до гнучкішої Дискреційної (матричної) моделі, де права делегуються безпосередньо власником інформації, а також до моделі Clark-Wilson (CW) та історичної архітектури Адепт-50, які орієнтовані на збереження точності бізнес-процесів і запобігання внутрішньому шахрайству через автоматизовану перевірку операцій та суворий розподіл обов'язків персоналу. Другий рівень охоплює сучасні аналітичні моделі кіберрозвідки та проактивної протидії загрозам, де базовим інструментом виступає концепція «глибинного захисту» (Defense-in-Depth), яка передбачає побудову багаторубежної ешелонованої оборони підприємства. Для оцінки зовнішніх ризиків цей підхід доповнюється матричною базою знань MITRE ATT&CK™, що дозволяє покроково реконструювати тактики й техніки хакерів, та «Моделлю алмазу» (Diamond Model), яка встановлює причинно-наслідкові

зв'язки між зловмисником, його інструментами, інфраструктурою та компанією-жертвою.

Таблиця 1.3

Характеристика методів моделювання корпоративної інформаційної безпеки

Назва	Науково-методична характеристика та управлінський зміст
Модель Bell-LaPadula (BLP)	Фундаментальна математично формалізована модель, що базується на строгій політиці конфіденційності інформаційних потоків. Визначає захищений стан системи за допомогою правил розмежування доступу: заборона читання даних вищого рівня секретності («no read up») та заборона запису даних на нижчі рівні («no write down»).
Модель Biba	Математична модель, спрямована на забезпечення цілісності інформації та захист від несанкціонованої модифікації. Оперує рівнями цілісності суб'єктів та об'єктів (заборона читання нижчого рівня, заборона запису на вищий), а також містить додаткову властивість виклику, що регламентує право суб’єкта надсилати сервісні запити.
Модель Clark-Wilson (CW)	Процесно-орієнтована модель, яка забезпечує цілісність, безпеку та підзвітність трансакційних переходів у системі. Захист реалізується через механізм обов'язкового посередництва програмних агентів між користувачем і даними, а також за рахунок вибору адаптивного режиму роботи з масивами інформації.
Дискреційна (матрична) модель	Прагматично орієнтована модель доступу, в якій стан системи захисту описується через математичну тріаду (суб'єкти, об'єкти, права доступу). Права суб'єктів щодо об'єктів чітко специфікуються у формі матриці, що дозволяє гнучко налаштовувати доступ користувачів на практиці.
Модель «Адепт-50»	Багаторівнева модель безпеки, розроблена для розподілених комп'ютерних систем. Вона структурує контур захисту шляхом категоризації та контролю взаємодії чотирьох ключових груп об’єктів: користувачів, завдань (процесів), терміналів (апаратних засобів) та файлів (даних).
Модель MITRE ATT&CK™	Глобальна таксономія та емпірична база знань про тактики, техніки й процедури (TTPs) кіберзловмисників, сформована на основі реальних спостережень. Використовується приватним сектором та урядовими інституціями як методологічна основа для аудиту захищеності, моделювання загроз та проактивного формування політики безпеки.
«Модель алмазу»	Матриця аналізу кіберінцидентів, яка структурує та формалізує інформаційну політику об’єкта через декомпозицію будь-якої атаки на чотири взаємопов'язані вершини («алмаз»): зловмисник (adversary), інформаційна інфраструктура, технологічні можливості (capabilities) та жертва (victim).
«Піраміда болю» (The Pyramid of Pain)	Концептуальна модель вибору політики безпеки, яка градуює індикатори компрометації (IoCs) за рівнем складності їхньої зміни для зловмисника (від простих хеш-функцій до критичних — тактик і методів дій). Дозволяє оптимізувати витрати на захист, фокусуючись на нанесенні максимальних «втрат» атакуючій стороні.
Модель «глибинного захисту»	Стратегічний підхід, який передбачає створення багаторівневих (розшарованих) бар'єрів інформаційної безпеки (фізичний, мережевий, хостовий, прикладний рівні та рівень даних). Нівелює ризик «єдиної точки відмови», суттєво підвищуючи стійкість та життєздатність системи в цілому.

Джерело: [10].

Практична оптимізація захисних ресурсів у межах цієї системи координується за допомогою «Піраміди болю» (The Pyramid of Pain), яка допомагає менеджменту концентрувати зусилля не на блокуванні легкозамінних дрібних індикаторів на кшталт IP-адрес, а на руйнуванні самих поведінкових алгоритмів нападників. У підсумку, інтеграція класичних моделей допуску із сучасними матрицями кібератак дозволяє підприємству створити адаптивну архітектуру безпеки, здатну витримувати дестабілізуючі удари під час глобальної економічної турбулентності.

Аналіз чинників забезпечення інформаційної безпеки є критично важливим, оскільки він дозволяє підприємству чітко зрозуміти, які саме внутрішні та зовнішні сили безпосередньо впливають на захищеність його даних (рис. 1.4). Без детального вивчення цих факторів менеджмент ризикує діяти наосліп, хаотично витрачаючи бюджети на захист від неіснуючих загроз і водночас ігноруючи реальні вразливості.

Рис. 1.4. Чинники забезпечення інформаційної безпеки на сучасних підприємствах

Джерело: узагальнено автором на основі [11, с. 84-85].

У часи глобальної турбулентності та воєнного стану структура цих чинників кардинально змінюється: на перший план виходять не лише суто технічні аспекти, а й геополітичні ризики, надійність ланцюгів постачання софту та стабільність критичної інфраструктури. Чітка класифікація та оцінка цих факторів допомагає компанії трансформувати свою систему захисту із пасивної оборони у гнучку, проактивну модель, здатну адаптуватися до змін у режимі реального часу. Окрім того, розуміння внутрішніх чинників, таких як рівень цифрової грамотності працівників чи якість корпоративних регламентів, дозволяє усунути людський фактор як головну причину безпекових інцидентів. Зрештою, саме постійний моніторинг та врахування ключових чинників безпеки забезпечують підприємству довгострокову стійкість, захищаючи його від катастрофічних фінансових збитків та втрати репутації на нестабільному ринку.

«У Стратегії національної безпеки України виокремлено ряд поточних і прогнозованих загроз національній безпеці та національним економічним інтересам. Згідно зі Стратегією загрозами інформаційній безпеці стратегічно важливих підприємств правомірно визначити стрімкий розвиток інформаційних технологій, що є причиною поширенню злочинності у кіберпросторі та деструктивної пропаганди в інформаційному середовищі; слабкість системи стратегічних комунікацій; зростання несанкціонованих втручань кіберхарактеру в функціонування об’єктів критичної інфраструктури; відсутність цілісної інформаційної політики держави» [12].

Офіційне закріплення зазначених загроз на рівні Стратегії національної безпеки України свідчить про те, що інформаційна безпека стратегічно важливих підприємств є невіддільним елементом захисту національних економічних інтересів держави. Окреслені в документі виклики – від деструктивної пропаганди до скоординованих кібератак на об'єкти критичної інфраструктури – в умовах тривалого воєнного стану набули максимальної гостроти. Для сучасного корпоративного сектору це означає, що побудова системи захисту інформації не може обмежуватися локальними заходами.

Менеджмент підприємств змушений враховувати загальнодержавний контекст: компенсувати слабкість зовнішніх стратегічних комунікацій посиленням власної цифрової стійкості, впроваджувати проактивні інструменти протидії кібервтручанням та інтегрувати корпоративні системи безпеки у загальну архітектуру кібероборони країни. Таким чином, державні орієнтири стають обов'язковим підґрунтям для формування локальних стратегій захисту інформаційних ресурсів на кожному життєво важливому підприємстві.

Відповідно до Стратегії кібербезпеки України доцільно виокремити такі види загроз інформаційній безпеці стратегічно важливих підприємств як кібервійна, кібертероризм, кіберзлочинність, кібершпигунство [13].

Комплексний аналіз Стратегії інформаційної безпеки та Стратегії кібербезпеки України дозволяє констатувати, що загрози корпоративному сектору сьогодні мають наскрізний характер і загрожують як окремому суб’єкту господарювання, так і економічній стабільності держави в цілому. Запропонований поділ викликів на глобальні та національні чітко вказує на зміну парадигми захисту: корпоративна безпека більше не є локальною проблемою бізнесу, оскільки підприємства опинилися на передовій повномасштабної кібервійни та кібершпигунства з боку рф. Особливо показовим є те, що державні стратегії прямо пов'язують зовнішні деструктивні впливи із внутрішніми слабкостями самих підприємств, такими, як недостатня обізнаність менеджменту та відсутність ефективних локальних систем захисту інформації. Отже, виокремлені види загроз, від кібертероризму до кіберзлочинності, вимагають від стратегічно важливих підприємств відмови від пасивного очікування загальнонаціональних рішень. Натомість бізнес має проактивно впроваджувати розглянуті раніше методи моделювання та ешелонованої оборони, трансформуючи державні безпекові імперативи у конкретні внутрішні регламенти, технічні фільтри та програми навчання власного персоналу.

Підсумовуючи вищевикладене, можна стверджувати, що формування дієвої архітектури інформаційної безпеки підприємства в умовах глобальної економічної турбулентності та воєнного стану вимагає системного переходу від фрагментарного технічного захисту до комплексної, проактивної моделі управління. Опрацювання фундаментальних теоретичних засад та нормативно-правового базису, закріпленого у стратегічних державних документах, доводить, що корпоративна інформаційна безпека є критично важливим складником загальної економічної безпеки суб'єкта господарювання. Реалізація цієї безпеки можлива лише за умови синергетичного поєднання базових принципів – від мінімальних привілеїв та глибокого ешелонованого захисту до постійного навчання персоналу та регулярного аудиту. Використання сучасних аналітичних методів моделювання і чітко типізованих інструментів кіберрозвідки дозволяє бізнесу не просто реагувати на інциденти, а діяти на випередження, нейтралізуючи зовнішні та внутрішні загрози кіберхарактеру. У кінцевому підсумку, саме така інтегрована й адаптивна система забезпечує стабільність ключових бізнес-процесів, мінімізує фінансові та репутаційні ризики підприємства та гарантує його життєздатність у хаотичному ринковому середовищі.

1.2. Глобальна економічна турбулентність: виклики та можливості

Сучасний етап розвитку світового господарства характеризується безпрецедентним рівнем невизначеності, нестабільності та динамізму, що в науковому дискурсі описується концептом глобальної економічної турбулентності. Традиційні ринкові закономірності та класичні моделі стратегічного планування втрачають свою ефективність під тиском системних криз, спричинених геополітичними конфліктами, руйнуванням глобальних ланцюгів постачання, макроекономічними коливаннями та стрімким розгортанням цифрової революції. Для вітчизняних підприємств, які змушені функціонувати в умовах тривалого воєнного стану та одночасно інтегруватися

у світовий економічний простір, дослідження природи цієї турбулентності є питанням не просто конкурентоспроможності, а фізичного виживання та збереження життєздатності бізнесу.

Особливої гостроти ця проблема набуває у контексті забезпечення інформаційної безпеки корпоративного сектору. Економічна нестабільність та дефіцит ресурсів змушують компанії оптимізувати витрати, водночас хаотизація зовнішнього середовища провокує лавиноподібне зростання кіберзагроз, промислового шпигунства та деструктивних інформаційних впливів. У таких жорстких умовах виникає об'єктивна необхідність переосмислення сутності турбулентності: її слід розглядати не лише як джерело катастрофічних ризиків та викликів, а й як специфічне вікно можливостей для проведення внутрішніх структурних трансформацій, диверсифікації діяльності та впровадження гнучких, адаптивних інструментів захисту інформаційних активів.

Таким чином, теоретико-методологічний аналіз викликів та можливостей глобальної турбулентності є критично важливим для формування проактивної парадигми управління підприємством. Без чіткого розуміння архітектури сучасних макроекономічних штормів неможливо побудувати життєздатну систему економічної та інформаційної безпеки, яка б дозволяла бізнесу ефективно тримати зовнішні удари, мінімізувати збитки та оперативно капіталізувати нові ринкові ніші, що виникають під час кризової перебудови глобальних ринків.

Шуст О. А., Варченко О. М. та Крисанов Д. Ф. вважають, що «На сучасному етапі під впливом посилення турбулентності (інколи навіть без цього) в економічній системі можуть виникати і поширюватися різні форми диспропорцій, перекосів, асиметричностей та розривів. Термін «турбулентність» спершу почали застосовувати у природничих науках (газо-, гідро- і термодинаміці), а пізніше відбулася термінологічна дифузія в інші сектори науки: біологічні, соціальні, економічні. Цей термін перекладається з латинської мови як бурхливий, хаотичний, непередбачуваний,

невпорядкований. Як правило, хаотичні та безсистемні зміни у будь-якому середовищі можуть викликати не лише його поступову трансформацію, посилювати нестабільність й непередбачуваність, але, при досягненні певної межі (інтенсивності чи глибини, масштабності охоплення чи накопиченні критичної маси змін), породжувати кризу або ж навіть катастрофу» [14, с. 292].

Спираючись на дефініцію дослідників, слід підкреслити, що запозичена з природничих наук концепція турбулентності якнайкраще описує сучасний стан корпоративного середовища, де хаотичність і непередбачуваність стають новою нормою функціонування. Зазначені авторами «диспропорції, перекоси та розриви» в контексті інформаційної складової економічної безпеки матеріалізуються у вигляді критичних вразливостей IT-інфраструктури, розривів у ланцюгах постачання програмного забезпечення та асиметрії між стрімким розвитком кібератак і обмеженими ресурсами підприємства для захисту від них.

Накопичення цієї «критичної маси змін» в умовах загального макроекономічного шторму та воєнного стану здатне миттєво перерости у катастрофу для бізнесу – повну зупинку операційних процесів через успішну хакерську атаку або втрату ринкових позицій внаслідок зливу комерційної таємниці. Водночас розуміння сутності турбулентності як безперервного процесу трансформації середовища змушує менеджмент відмовитися від статичних моделей безпеки. Підприємство має адаптувати свої захисні механізми до цього «бурхливого» темпу, сприймаючи хаос не лише як джерело руйнівних криз, а й як стимул для побудови принципово нової, гнучкої та відмовостійкої системи корпоративного захисту.

Сформульована дослідниками дуалістична концепція економічної турбулентності дозволяє глибше розкрити специфіку функціонування системи інформаційної безпеки підприємства як динамічного механізму, що перебуває у постійному русі між безладом і порядком. Теза авторів про те, що хаотичні процеси неминуче «оголюють слабкі місця», знаходить своє пряме відображення у сфері кіберзахисту: під час загальноекономічних штормів та

криз будь-які прорахунки в налаштуванні прав доступу, слабкість антивірусного софту чи низька цифрова грамотність персоналу миттєво стають явними під тиском зовнішніх атак. Для компаній, які виявляються неготові виробляти «своєчасні моделі поведінки», цей хаос завершується деструктивно – критичними витоками комерційних даних або повною втратою контролю над операційними процесами. Проте, якщо екстраполювати погляди науковців на проактивне управління ризиками, то здатність системи захисту вчасно виявляти й усувати ці уразливості перетворює турбулентність на «вікно можливостей». У таких умовах криза стимулює підприємство відмовитися від застарілих шаблонів безпеки та впроваджувати новітні інструменти – від систем поведінкового моніторингу активності користувачів до інтегрованих аналітичних моделей кіберрозвідки, що зрештою дозволяє компанії не просто вижити, а набути якісно нового рівня цифрової стійкості (кібервитривалості). [15, с. 511].

«Численні дослідження демонструють важливість забезпечення продовольчої безпеки. Вирішення цієї проблеми є актуальним і складним. Це терміново, оскільки до 2050 року сільське господарство має прогодувати понад 9 мільярдів людей [16]. Це складно, оскільки продовольча безпека залежить від сукупності економічних, політичних, соціальних та інших факторів. Наприклад, Ван Бавел [17] показали, що ігнорування оптимізації ресурсів виробництва та відмова від інвестицій у відповідні наукові дослідження спричиняє зростання бідності та голоду, збільшення забруднення та виснаження природних ресурсів, а також прискорює різке зростання міграційного тиску. Подібним чином Гарднер [18] і Мейерс і Калайтзандонакес [19] досліджували шляхи виробництва принаймні на 50% більше продовольства до 2050 року, незважаючи на несприятливі зміни клімату, збільшення вартості енергії та триваючу турбулентність у міжнародній торговій політиці сільськогосподарської продукції. Альфієрі [20] запропонував дії, які могли б підтримувати стійкість і гарантувати глобальну продовольчу безпеку як за рахунок компонентів доступності, так і

доступності. Це включало стратегічні цілі щодо обмеження розширення сільського господарства, сприяння генетичному різноманіттю сільськогосподарських культур, сприяння різним формам і можливостям сільського господарства, збалансованості споживання, харчових відходів і втрат після збору врожаю, організації еластичних і справедливих режимів торгівлі та контролю темпів урбанізації.» [21].

Окреслений у праці Н. Васильєвої та Х. Джеймса масив фундаментальних досліджень наочно демонструє, що продовольча безпека є одним із найбільш чутливих та критично важливих секторів глобальної економіки, який першим відчуває на собі дестабілізуючі удари міжнародної турбулентності. Проте в умовах сучасної цифрової трансформації забезпечення стійкості продовольчого комплексу та стратегічних підприємств загалом уже неможливе виключно через оптимізацію фізичних ресурсів чи контроль урбанізації. Сьогодні аграрний сектор та суміжні галузі критичної інфраструктури критично залежать від інформаційних технологій (автоматизованих систем управління, точного землеробства, цифрових логістичних ланцюгів та хмарних баз даних).

Як наслідок, зазначена авторами «турбулентність у міжнародній торговій політиці», дефіцит енергії та кліматичні виклики накладаються на нову, суто цифрову загрозу. Будь-які «перекоси та розриви» в управлінні інформаційною безпекою на підприємствах життєзабезпечення здатні спровокувати глобальний кумулятивний ефект. Наприклад, успішна кібератака на логістичну систему великого постачальника або блокування даних вірусом-вимагачем в умовах воєнного стану може миттєво паралізувати ланцюги розподілу продовольства, перетворюючи технічний інцидент на масштабну соціально-економічну кризу. З іншого боку, згадувана дослідниками «оптимізація ресурсів виробництва» та «інвестиції у відповідні наукові дослідження» в умовах турбулентності мають включати й фінансування кібервитривалості бізнесу. Лише за умови побудови гнучкої системи захисту корпоративної інформації, здатної протидіяти

кібершпигунству та цифровим диверсіям, стратегічно важливі підприємства зможуть реалізувати пропоновані Ф. Альфієрі кроки щодо підтримання стійкості, гарантуючи еластичність торговельних режимів та безперервність постачання у кризові періоди.

«Важливість переходу до стійкої економіки, заснованої на нових можливостях, які дозволяють впоратися з поточними турбулентними змінами, є першочерговою. Вважається, що підприємці, які піклуються про стійкий розвиток, відіграють ключову роль у цьому процесі, створюючи інноваційні, проактивні та ризиковані рішення, які мають як екологічну, так і економічну цінність. На сьогоднішній день немає консенсусу щодо того, які здібності має надати освіта, щоб створити стійких підприємців, щоб справлятися з проблемами сталого розвитку». [22].

Погляди дослідників щодо першочергової важливості переходу до стійкої економіки через формування проактивного підприємництва дозволяють по-новому оцінити роль людського капіталу в системі забезпечення інформаційної безпеки. Зазначена авторами необхідність створення «інноваційних, проактивних та ризикованих рішень» в умовах ринкових штормів вимагає від сучасного менеджменту принципово нових компетенцій. Будь-які спроби впровадити екологічно чисті технології, оптимізувати ресурси чи вийти на нові цифрові ринки під час кризи будуть нівельовані, якщо лідери бізнесу не володітимуть навичками стратегічного управління кіберризиками.

Водночас виокремлена науковцями проблема відсутності консенсусу щодо освітніх стандартів для стійких підприємців прямо екстраполюється на сферу корпоративної безпеки підприємств. Концепція сталого розвитку в епоху турбулентності вже не може обмежуватися лише екологічними чи класичними фінансовими аспектами; її обов'язковим елементом стає «цифрова життєздатність» (кібервитривалість). Відтак, подолання згаданого освітнього дефіциту на рівні конкретного суб'єкта господарювання має відбуватися через розбудову внутрішніх систем безперервного навчання команди.

Підприємство, що прагне зберегти стійкість, змушене самостійно інтегрувати інструменти медіаграмотності, знання сучасних аналітичних моделей загроз та навички протидії соціальній інженерії у програми підготовки свого персоналу. Тільки через поєднання підприємницької інноваційності із суворими стандартами інформаційного захисту стає можливим створення довгострокової економічної цінності, здатної протистояти руйнівним імпульсам глобального хаосу.

На основі критичного аналізу та узагальнення існуючих наукових підходів до розуміння сутності глобальних дестабілізаційних процесів, сформульовано власну авторську позицію щодо дефініції та природи економічної турбулентності у контексті забезпечення інформаційної безпеки підприємства.

Вважаємо, що економічну турбулентність неправомірно розглядати як суто деструктивний, форс-мажорний чи тимчасовий стан зовнішнього середовища. Визначаємо економічну турбулентність як перманентну (постійну) форму існування сучасної глобальної та національної економіки, яка характеризується нелінійним рухом ринкових процесів, високою частотою появи непередбачуваних кіберзагроз та неминучим виникненням структурних асимптот (розривів) у системах захисту підприємств.

У межах дослідження авторський підхід базується на трьох засадничих постулатах:

1. Ендогенність (внутрішня природа) вразливостей. Зовнішня турбулентність не створює нові проблеми на порожньому місці, а виступає в ролі «каталізатора-проявника». Вона індукує миттєве розкриття тих системних дефектів та «сліпих зон» в інформаційній безпеці підприємства (слабка цифрова гігієна, застарілі моделі доступу), які ігнорувалися менеджментом у відносно стабільні періоди.

2. Концепція «керованого хаосу». Оскільки повністю нівелювати зовнішній хаос неможливо, завдання підприємства полягає не в пасивному очікуванні стабілізації, а в адаптації внутрішньої архітектури безпеки до

параметрів цього хаосу. Тобто система безпеки має стати такою ж динамічною та гнучкою, як і саме турбулентне середовище.

3. Трансформація викликів у капітал стійкості. Стверджуємо, що турбулентність має глибоку дуальну природу. Її небезпека є обернено пропорційною швидкості управлінської реакції: для статичного бізнесу вона є синонімом катастрофи та банкрутства, тоді як для проактивного підприємництва вона стає унікальним джерелом інновацій, змушуючи впроваджувати ешелонований захист (Defense-in-Depth), передові методи кіберрозвідки (MITRE ATT&CK™) та безперервно підвищувати кваліфікацію персоналу.

Таким чином, авторська позиція полягає в тому, що в умовах глобальних штормів та воєнного стану економічна турбулентність має сприйматися менеджментом як стратегічний імператив для негайної перебудови корпоративного захисту. Вона перетворює інформаційну безпеку з витратної статті бюджету на базову передумову забезпечення загальної економічної життєздатності та конкурентоспроможності суб'єкта господарювання.

Для систематизації виявлених деструктивних факторів та визначення векторів адаптації суб'єктів господарювання, у таблиці 1.4 сформовано матрицю взаємозв'язку між джерелами глобальної турбулентності та механізмами забезпечення інформаційної безпеки підприємства.

Аналіз сформованої матриці (табл. 1.4) наочно демонструє, що кожен дестабілізуючий імпульс глобальної турбулентності містить у собі прихований потенціал для якісного оновлення захисних систем підприємства. Оцінюючи наведені дані, можна констатувати, що ключова помилка більшості суб'єктів господарювання полягає у спробах ліквідувати наслідки криз суто технічними методами, ігноруючи організаційні та теоретико-методологічні аспекти. Натомість представлена систематизація доводить, що ефективна протидія зовнішньому хаосу та кібератакам в умовах воєнного стану лежить у площині інтеграції класичних моделей розмежування доступу із сучасними концепціями кіберрозвідки.

Таблиця 1.4.

Матриця впливу глобальної економічної турбулентності на систему інформаційної безпеки підприємства

Джерело турбулентності (за науковими джерелами)	Оголені слабкі місця та виклики (Вплив хаосу та деструкції)	Нові можливості та проактивні рішення (Вплив самоорганізації та розвитку)	Інструменти реалізації (Моделі та стратегії)
Геополітичні конфлікти та кібервійна (Стратегії національної, інформаційної та кібербезпеки України, 2020–2021 рр.)	Прямі скоординовані атаки рф на об'єкти критичної інфраструктури. Ризики кібершпигунства та цифрових диверсій проти стратегічних підприємств.	Інтеграція корпоративного захисту в загальнонаціональну систему кібероборони. Перехід до жорстких режимів ізоляції критичних бізнес-процесів.	Концепція «глибинного захисту» (Defense-in-Depth). База знань MITRE ATT&CK™
Дестабілізація світових ринків та ланцюгів постачання (Vasylieva & James, 2021; Шуст, Варченко, Крисанов, 2022)	Виникнення «диспропорцій та розривів» у постачанні іноземного софту й обладнання. Ризик каскадних збоїв (атака на постачальника паралізує ланцюг виробництва).	Перегляд архітектури систем на користь відмовостійкості. Проведення повного аудиту та імпортозаміщення вразливих компонентів IT-інфраструктури.	Модель Clark-Wilson (CW) (контроль цілісності операцій). Регулярний аудит допусків
Хаотизація інформаційного простору (Ostrovska et al., 2022; Стратегія ІБ, 2021 р.)	Масштабні дезінформаційні кампанії та пропаганда. Зростання активності кіберзлочинців, які використовують паніку для фішингу та соціальної інженерії.	Впровадження систем поведінкового моніторингу всередині компанії. Розробка чітких внутрішніх регламентів реагування на маніпулятивні виклики.	«Піраміда болю» (The Pyramid of Pain) Модель «Алмазу» (Diamond Model)
Освітній дефіцит та людський фактор (Rosário & Raimundo, 2024)	Недостатній рівень обізнаності суб'єктів господарювання в питаннях кібергігієни. Рядовий персонал стає головною точкою входу для хакерських атак.	Створення систем безперервного навчання команди (підвищення кібервіривалості лідерів). Автоматичне обмеження прав користувачів для запобігання внутрішнім помилкам.	Модель Bell-LaPadula (захист конфіденційності) Модель Biba (контроль точності даних)

Джерело: згруповано автором.

Уразливість людського фактора чи розриви в логістичних ланцюгах постачання софту успішно нівелюються не просто закупівлею нового програмного забезпечення, а впровадженням суворих алгоритмів моделей Bell-LaPadula та Clark-Wilson у поєднанні з безперервним навчанням персоналу. Таким чином, таблиця 1.4 підтверджує наукову гіпотезу про те, що за умови проактивного підходу менеджменту макроекономічна нестабільність перетворюється з фактора руйнування на потужний стимул для капіталізації внутрішніх резервів та побудови відмовостійкої, адаптивної архітектури корпоративної інформаційної безпеки.

Таким чином, проведене дослідження сутності та архітектури глобальної економічної турбулентності дозволяє констатувати, що вона виступає ключовим дестабілізуючим фактором для сучасного корпоративного сектору, кардинально змінюючи правила забезпечення безпеки підприємств. Екстраполяція фундаментальних наукових підходів – від природничого розуміння хаосу як накопичення критичної маси змін до галузевих викликів продовольчої та технологічної стійкості – доводить дуальну природу цього явища. З одного боку, турбулентність формує безпрецедентні виклики кіберхарактеру, екстраординарно посилюючи ризики кібервійни, промислового шпигунства та деструктивних інформаційних кампаній, які миттєво оголюють будь-які слабкі місця в захисті компаній. З іншого боку, цей стан безперервних трансформацій руйнує неефективні статичні шаблони, створюючи для проактивних підприємців унікальне вікно можливостей для впровадження гнучких інструментів ешелонованої оборони, оптимізації внутрішніх ресурсів та переформатування систем навчання команди. У підсумку, виживання та подальший розвиток стратегічно важливих підприємств в умовах макроекономічного шторму залежить не від спроб пасивно перечекати кризу, а від здатності менеджменту трансформувати виявлені вразливості у проактивну стратегію кібервитривалості, яка інтегрує інформаційну безпеку в загальний контур економічної життєздатності бізнесу.

1.3. Методичні підходи щодо оцінювання рівня інформаційної безпеки в умовах глобальної економічної турбулентності

Стрімке розгортання глобальної економічної турбулентності, що посилюється військово-політичними кризами та інтенсифікацією кіберпротистояння, висуває жорсткі вимоги до якості та швидкості управлінських рішень у сфері захисту корпоративних інтересів. У цих умовах традиційні, статичні підходи до моніторингу безпекового контуру підприємств виявляються неспроможними адекватно реагувати на динамічні загрози нелінійного характеру. Виникає об'єктивна наукова та практична потреба у глибокій ревізії наявного методичного інструментарію.

Наявність значної кількості міжнародних стандартів (ISO, NIST, COBIT) та вітчизняних наукових розробок у галузі аудиту інформаційних систем ще не гарантує формування відмовостійкості бізнесу, оскільки більшість із них не враховують синергетичного ефекту, коли фінансові дефіцити накладаються на цілеспрямовані хакерські диверсії. Таким чином, дослідження та систематизація методичних підходів щодо оцінювання рівня інформаційної безпеки є критично важливими для формування адаптивних систем оцінки. Це дозволить трансformувати кількісні параметри технічних уразливостей у якісні показники економічної життєздатності суб'єктів господарювання, забезпечуючи менеджмент надійним аналітичним базисом для прийняття проактивних рішень під час макроекономічного шторму.

Вагоме методологічне значення для нашого дослідження мають напрацювання В. Г. Горника та С. О. Кравченка, які визначають інформаційну безпеку через призму «міри захищеності держави (суспільства) та стійкості основних сфер життєдіяльності відносно небезпечних інформаційних впливів» [23, с. 206]. Особливою цінністю підходу авторів є двовекторна детермінація загроз, що охоплює процеси «як з упровадження, так і добування інформації». Науковці справедливо акцентують увагу на тому, що джерелами деструктивного впливу виступають як персоніфіковані суб'єкти (окремі

особи), так і інституційні структури (організації та їхні об’єднання), які у сукупності формують цілісний «спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави» [23, с. 206]. Це дозволяє розглядати інформаційну безпеку не як локальну функцію захисту даних, а як системну характеристику життєстійкості соціоекономічного середовища.

Визначена дослідниками дефініція закладає важливий методологічний фундамент для формування методичних підходів до оцінювання рівня інформаційної безпеки суб'єктів господарювання. Оскільки автори розглядають інформаційну безпеку не як статичний стан, а як динамічну «здатність нейтралізувати деструктивні впливи», то й архітектура оцінювання на рівні окремого підприємства має трансформуватися.

Традиційні підходи, орієнтовані на фіксацію формальної наявності захисних засобів (наприклад, наявність антивірусних ліцензій чи затверджених інструкцій), в умовах глобальної турбулентності виявляються безглуздими. Замість цього, методичний інструментарій повинен оцінювати саме коефіцієнт стійкості та швидкість реакції системи на двовекторні загрози: як на спроби несанкціонованого «добування» (ексфільтрації) комерційних даних, так і на ризики «впровадження» деструктивного коду чи маніпулятивних інформаційних впливів через канали соціальної інженерії.

«Аудит безпеки інформаційної безпеки – це системний процес одержання об'єктивних якісних і кількісних оцінок поточного стану безпеки інформаційної системи, комплексна оцінка рівня інформаційної безпеки клієнта з урахуванням трьох основних факторів: персоналу, процесів і технологій» [24].

Зазначений підхід до розуміння аудиту інформаційної безпеки дозволяє чітко структурувати об'єкт оцінювання, виокремивши в ньому три засадничі виміри: персонал, процеси та технології. У контексті функціонування підприємства в умовах глобальної економічної турбулентності ця тріада набуває особливого значення, оскільки криза б'є по кожному з елементів

нерівномірно. Відтак, будь-який сучасний методичний підхід щодо оцінювання безпекового контуру має базуватися на комплексному аналізі цих трьох складових:

1. Фактор технологій передбачає отримання кількісних метрик захищеності інфраструктури (наявність уразливостей, стійкість шифрування, надійність периметра). В умовах турбулентності цей показник відображає здатність системи витримувати прямі технічні кібератаки.

2. Фактор процесів оцінює якість та адаптивність корпоративних регламентів, швидкість реагування на інциденти та гнучкість управління доступами. В умовах хаосу саме чіткість процесів мінімізує час простою підприємства після можливого зламу.

3. Фактор персоналу вимірює рівень кібергігієни та психологічної стійкості працівників до методів соціальної інженерії та фішингу. Оскільки людина залишається найслабшою ланкою в ланцюгу захисту, оцінка цього фактора є критичною для запобігання внутрішнім загрозам.

Таким чином, визначення аудиту як процесу одержання «об'єктивних якісних і кількісних оцінок» на основі тріади PPT доводить необхідність використання комбінованих методичних підходів. Науковий аналітик чи менеджер підприємства не може спиратися виключно на математичні розрахунки ймовірностей або лише на суб'єктивні експертні висновки. Тільки синергетичне поєднання якісних методів (для оцінювання процесів і поведінки персоналу) та кількісних інструментів (для моніторингу технологічних параметрів) дозволяє сформувати релевантну картину захищеності стратегічного підприємства під час макроекономічного шторму.

Дячков Д. В. наголошує, що «Оцінкою інформаційної безпеки займаються з початку появи інформаційних технологій. З цієї тематики є багато праць, але найбільш актуальними та фундаментальними працями є нормативні документи, що зробили вагомий теоретичний та практичний внесок у розв’язання задач забезпечення інформаційної безпеки (рис. 1.5)» [24].

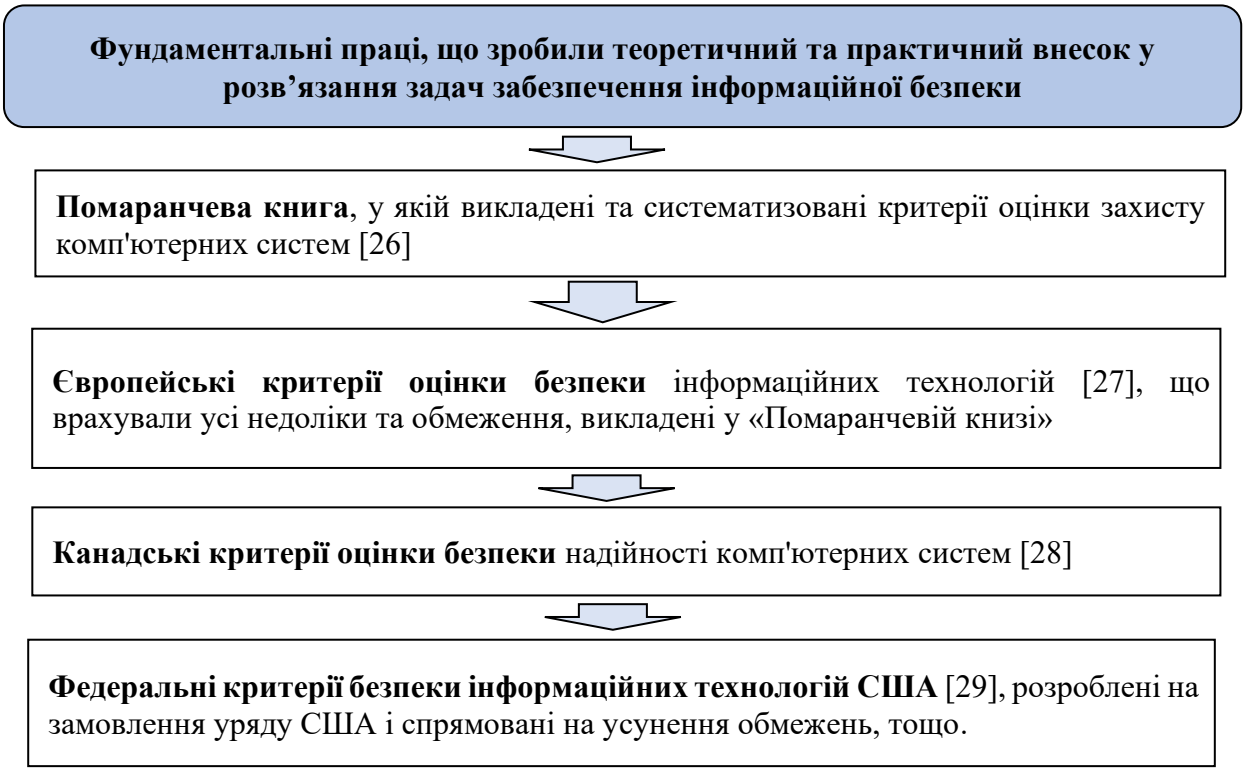


Рис. 1.5. Фундаментальні праці для розв'язання задач забезпечення інформаційної безпеки

Джерело: згруповано автором [26; 27; 28; 29].

Констатована дослідником фундаментальна роль нормативних документів підкреслює, що еволюція методичних підходів до оцінювання інформаційної безпеки завжди йшла шляхом жорсткої стандартизації. Відображена на рисунку 1.5. ретроспектива нормативного базису свідчить про перехід від суто технічних інструкцій до комплексних міжнародних стандартів управління ризиками. Проте в умовах сучасної глобальної економічної турбулентності та воєнного стану використання цих фундаментальних праць вимагає від менеджменту стратегічних підприємств гнучкої адаптації.

Якщо раніше оцінювання за нормативними документами (як-от класичні стандарти серії ISO/IEC 27001 чи настанови NIST) зводилося до періодичного, статичного аудиту відповідності «на папері», то сьогодні цей інструментарій має бути інтегрований у процеси безперервного моніторингу. Нормативні вимоги щодо контролю тріади «персонал, процеси, технології» трансформуються в динамічні метрики. Замість фіксації формального

виконання стандарту, підприємства змушені оцінювати свою реальну кібервитривалість – тобто здатність функціонувати в умовах постійних хакерських атак та макроекономічного дефіциту ресурсів, спираючись на оновлені міжнародні стандарти як на перевірений часом мінімальний безпековий каркас.

Критерії оцінки інформаційної безпеки є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступенів захищеності [30].

З допомогою критеріїв можливо порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем (рис.1.6) [30].

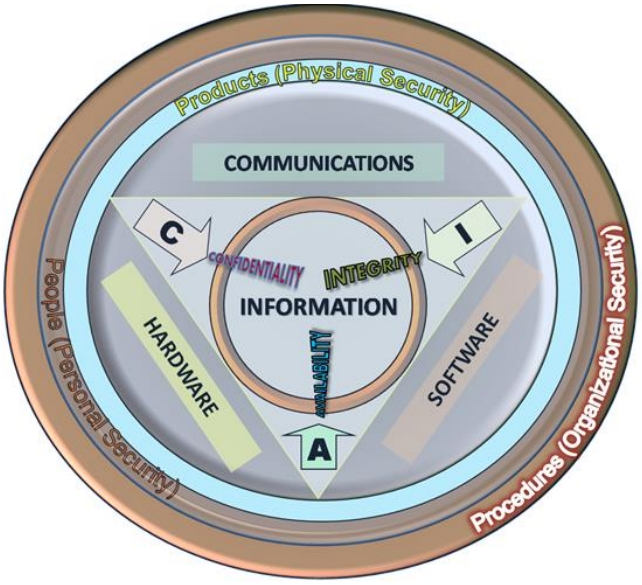


Рис. 1.6. Критерії оцінки інформаційної безпеки

Джерело: [30].

Використання методологічного апарату «Загальних критеріїв» (ISO/IEC 15408) дозволяє перевести процес оцінювання інформаційної безпеки підприємства з площини суб'єктивних експертних припущень у площину стандартизованого порівняльного аналізу. Оскільки цей стандарт дає можливість чітко «визначити необхідну функціональність» та «порівняти різні механізми захисту», його застосування є критично важливим під час формування технологічного контуру безпеки в умовах ринкового хаосу. Коли

підприємство змушене оптимізувати бюджети через макроекономічний тиск, воно не має права на фінансову помилку при закупівлі засобів захисту (брандмауерів, систем шифрування чи SIEM-платформ). Завдяки «Загальним критеріям» менеджмент може чітко зіставити вимоги до безпеки із сертифікованими рівнями гарантій (EAL), обираючи саме ті інструменти, які здатні витримати цілеспрямовані атаки відповідного рівня складності.

Водночас, екстраполюючи логіку «Common Criteria» на загальну систему оцінювання рівня безпеки підприємства, слід зауважити, що цей стандарт фокусується переважно на технічних та програмно-апаратних компонентах (технологіях). Проте, як було обґрунтовано раніше через тріаду PPT, у період глобальної турбулентності стійкість суб'єкта господарювання залежить також від процесів та персоналу. Відтак, «Загальні критерії» мають виступати як базовий, але не єдиний елемент методичного підходу. Технічна оцінка за цим стандартом повинна інтегруватися у ширші управлінські методики (такі як ISO/IEC 27001), де сертифікована надійність комп'ютерних систем підсилюється адаптивністю бізнес-процесів та високим рівнем кібергігієни працівників, формуючи в синергії комплексну кібервитривалість підприємства.

Для узагальнення матеріалу та чіткої систематизації наукового доробку в межах підрозділу, сформуємо порівняльну аналітичну таблицю. Вона наочно продемонструє еволюцію наукової думки та дозволить обґрунтувати необхідність комплексного оцінювання інформаційної безпеки під час макроекономічного шторму.

Систематизація наукових поглядів, представлена у таблиці 1.5, дозволяє констатувати наявність суттєвого методологічного плюралізму в питаннях оцінювання рівня інформаційної безпеки підприємства. Проведений критичний аналіз свідчить про поступову еволюцію оціночного інструментарію від звужених, однокритеріальних моделей до комплексних систем.

Таблиця 1.5

Погляди сучасників на методичні підходи до оцінки рівня інформаційної безпеки

Автори, джерело	Сутність методичного підходу	Науково-критична оцінка (управлінський аспект)
Велігура А. В.[31]	Пропонує тривекторну модель оцінювання:1) детермінація небезпек (ідентифікація загроз, вразливостей, ймовірності атак та потенційного збитку);2) правовий комплаєнс (нормативні та договірні вимоги для організації та її контрагентів);3) внутрішній інституційний базис (принципи й цілі обробки даних, сформовані через методику ризик-менеджменту).	Переваги: Комплексність, орієнтація на балансування витрат із рівнем можливих втрат бізнесу.Недоліки: Підхід має переважно загальнорегламентуючий характер; відсутній чіткий математичний алгоритм інтеграції цих трьох складників у єдиний показник.
Журавель М. Ю., Полозова Т. В., Стороженко О. В.[32]	Обґрунтовують доцільність проведення експрес-діагностики за трьома релевантними напрямами:— оцінювання програмно-технічної захищеності даних;— оцінювання інформаційної надійності персоналу (HR-контур);— оцінювання якості інформації, що генерується для осіб, які приймають рішення (ОПР).	Переваги: Триадичний підхід охоплює технічну, людську та управлінську складові.Недоліки: Автори детально не описують метрики оцінювання надійності персоналу та критерії релевантності даних для ОПР.
Ілляшенко С. М.[33]	Пов'язує рівень інформаційної безпеки виключно з якісними характеристиками інформації (частка неповної, неточної та суперечливої інформації), що використовується у процесі стратегічного менеджменту.	Переваги: Чітка орієнтація на нівелювання інформаційної асиметрії під час прийняття рішень.Недоліки: Фокусується лише на когнітивно-управлінській якості даних. Модель потребує обов'язкового доповнення індикаторами IT-захищеності та лояльності персоналу.
Кравчук О. Я., Кравчук П. Я.[34]	Пропонують систему з п'яти індикаторів, які інтегрально характеризують:— рівень інформаційно-аналітичного супроводження бізнесу;— якість захисту комерційної таємниці;— безпеку електронного документообігу;— стан ділової репутації та іміджу продукції підприємства.	Переваги: Вперше до контуру інформаційної безпеки включено нематеріальні активи (репутаційний капітал та бренд).Недоліки: Показники мають переважно експертний, суб'єктивний характер, що ускладнює їх автоматизований розрахунок.
Реверчук Н. Й.[35]	Оперує трьома базовими коефіцієнтами: продуктивністю інформації, рівнем інформаційної	Переваги: Прагматичність та легкість збору первинних даних.Недоліки: Перелік

	озброєності бізнесу та коефіцієнтом захищеності даних.	показників є обмеженим і відображає суто фінансовий аспект, оскільки розрахунки базуються виключно на обсягах витрат на придбання ІТ-ресурсів.

Джерело: згруповано автором [31; 32; 33; 34; 35].

Зокрема, якщо у підходах С. М. Ілляшенка увага акцентується суто на якісних характеристиках інформації для прийняття рішень, а в моделях Н. Й. Реверчук оцінює обмеженя виключно фінансовим аспектом витрат на інформаційні ресурси, то в умовах глобальної економічної турбулентності такі ізольовані метрики втрачають свою прогностичну здатність. Вважаємо, найбільш адаптивними до умов макроекономічної нестабільності є підходи А. В. Велігури, а також М. Ю. Журавля, Т. В. Полозової та О. В. Стороженко. Їхня перевага полягає в орієнтації на багатофакторну діагностику, де технічна захищеність обов'язково корелює з інформаційною надійністю персоналу та балансуванням витрат із потенційними збитками підприємства. Концептуальні положення цих дослідників слугують підтвердженням раніше адаптованої моделями, які доводять, що ефективне оцінювання ІБ під час кризи має виходити за рамки суто ІТ-моніторингу та інтегруватися в загальну систему стратегічного менеджменту суб'єкта господарювання.

На основі проведеного аналізу наукових праць сучасників та нормативно-правової бази, структуруємо основні методологічні підходи до оцінювання інформаційної безпеки. Систематизація цих підходів дозволяє побудувати концептуальну схему для рисунка 1.7., який наочно продемонструє класифікацію інструментарію, що використовується менеджментом в умовах макроекономічного шторму.

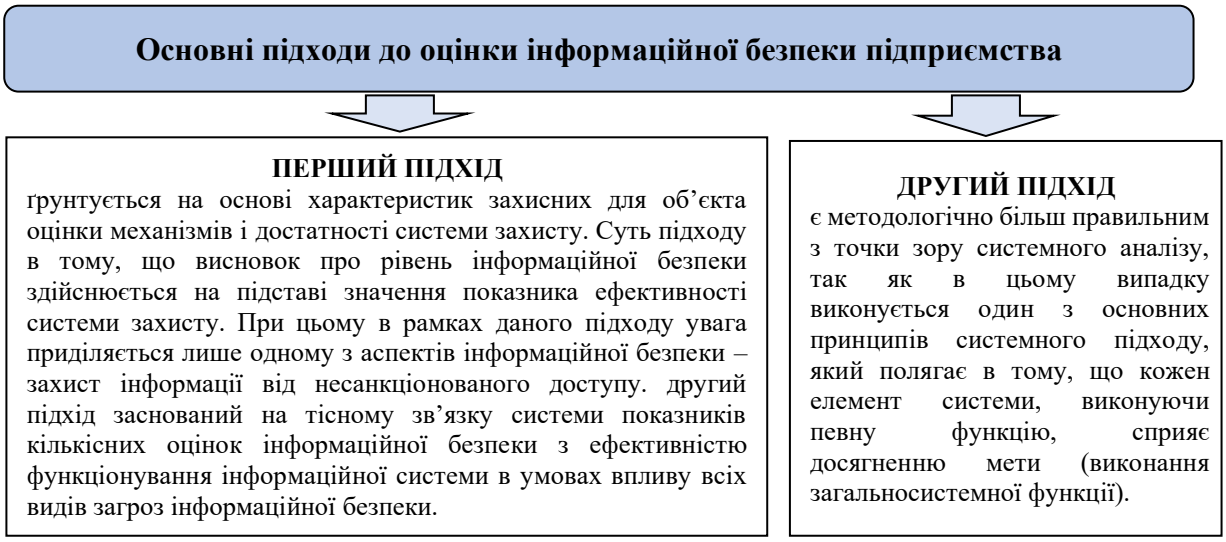


Рис. 1.7. Основні підходи до оцінки інформаційної безпеки підприємства

Джерело: згруповано автором [25; 37].

Проведений аналіз еволюції наукової думки дозволяє чітко диференціювати інструментарій оцінювання за двома концептуальними підходами, кожен з яких має власну цільову спрямованість та аналітичні обмеження.

Перший підхід повністю ґрунтується на характеристиках захисних механізмів безпосередньо для об'єкта оцінки та аналізі достатності наявної системи захисту. Сутність цього вектору полягає в тому, що фінальний висновок про рівень інформаційної безпеки підприємства здійснюється суто на підставі значення показника ефективності самої системи захисту. Варто вказати на ключове обмеження даного підходу: у його межах увага приділяється лише одному, локальному аспекту інформаційної безпеки – захисту інформації від несанкціонованого доступу. Це корелює з принципами технічного стандарту «Загальні критерії», але в умовах глобальної турбулентності є недостатнім, оскільки ігнорує організаційні та кадрові деструктивні чинники.

На противагу цьому, другий підхід базується на тісному зв'язку системи показників кількісних оцінок інформаційної безпеки з ефективністю загального функціонування інформаційної системи в умовах впливу всього спектра потенційних загроз інформаційній безпеці. З позицій системного

аналізу саме другий підхід є методологічно більш правильним та обґрунтованим. Його фундаментальна перевага полягає в реалізації одного з ключових принципів системного підходу: кожен окремий елемент системи, виконуючи свою локальну функцію, розглядається виключно через призму його внеску в досягнення загальної мети системи (виконання загальносистемної функції).

Система показників оцінювання рівня інформаційної безпеки підприємства в умовах турбулентності наведена у додатку А (таблиця А.1.). Сформована у таблиці А.1 система показників являє собою декомпозицію комплексного процесу оцінювання інформаційної безпеки підприємства на 26 базових індикаторів, розподілених за п'ятьма стратегічними блоками. Така глибока архітектурна структуризація дозволяє реалізувати на практиці методологічні вимоги системного аналізу в умовах макроекономічної турбулентності. Характерною рисою сформованої системи є відхід від суто технічного моніторингу на користь економіко-управлінських метрик.

Зокрема, інтеграція блоку оцінки витрат (індикатори 8–11) із оцінкою надійності персоналу (індикатори 12–16) та якістю інформаційного забезпечення ОПР (індикатори 17–21) усуває ключовий недолік однокритеріальних моделей. Метрики 25 та 26 (частка внутрішніх програмних та технічних рішень) є особливо важливими в умовах санкційних обмежень, розривів міжнародних логістичних ланцюгів постачання софту та воєнного стану, оскільки вони відображають рівень технологічного суверенітету та автономії підприємства. Таким чином, розроблена матриця індикаторів виступає інструментальним базисом для побудови інтегрального індексу кібервитривалості суб'єкта господарювання під час глобального хаосу.

На основі критичного аналізу розглянутих фундаментальних стандартів, практичних розробок та наукових поглядів сучасників (зокрема, концепцій А. В. Велігури, М. Ю. Журавля, С. М. Ілляшенка та інших), можна сформулювати комплекс базових вимог до архітектури майбутньої методики оцінювання інформаційної безпеки підприємства в умовах глобальної економічної

турбулентності. Майбутня інструментальна методика повинна відповідати таким дев'яти стратегічним вимогам:

1. Методика не може обмежуватися лише оцінкою програмно-технічної захищеності інформації. Вона зобов'язана одночасно й рівнозначно вимірювати три базові компоненти: технологічний контур, адаптивність організаційних процесів та інформаційну надійність і кібергігієну персоналу.

2. В умовах хаотичних змін та постійних переходів від порядку до безладу класичні річні або піврічні статики-аудити втрачають сенс. Оцінювання має проводитися за принципом безперервного моніторингу або гнучкого експрес-аналізу, що дозволяє миттєво фіксувати виникнення нових «сліпих зон» та уразливостей під тиском зовнішніх криз.

3. Методика повинна містити чіткий фінансово-економічний блок. Як зазначає А. В. Велігура, витрати на підтримку інформаційного захисту необхідно жорстко балансувати із потенційною шкодою (збитками) для бізнесу, яка може виникнути внаслідок порушення безпеки, що є критичним в умовах дефіциту ресурсів під час ринкового шторму.

4. Спираючись на державно-управлінський підхід, методика має оцінювати спроможність системи нейтралізувати деструктивні впливи за двома зустрічними векторами: як щодо несанкціонованого добування (витоку, шпигунства) комерційних даних, так і щодо впровадження небезпечної інформації (деструктивного коду, фішингу, маніпуляцій через соціальну інженерію).

5. Критерієм має стати індикатор С. М. Ілляшенка – частка неповної, неточної чи суперечливої інформації, яка проникає в контур менеджменту. Система оцінювання повинна верифікувати якість, релевантність та захищеність тих даних, що надаються особам, які приймають рішення (ОПР).

6. Оціночні показники не повинні замикатися всередині ІТ-відділу. Методика має враховувати зовнішні наслідки інцидентів ІБ, оцінюючи їхній безпосередній вплив на рівень ділової репутації підприємства, безпеку документообігу з контрагентами та загальний імідж продукції на ринку.

7. Комбінованість інструментарію (якісно-кількісний синергізм): Архітектура оцінювання має поєднувати об'єктивні кількісні метрики (параметри засобів захисту, технічні уразливості системи) із гнучкими якісними експертними оцінками (рівень підготовки кадрів, стійкість регламентів до форс-мажорів).

8. Методика повинна мати властивість фрактальності – тобто однаково ефективно застосовуватися як до всієї організації в цілому, так і окремо до її специфічних сегментів, критичних інформаційних систем, окремих компонентів чи хмарних сервісів, залежно від поточної управлінської потреби.

9. При всій своїй гнучкості, методика повинна суворо спиратися на вимоги міжнародних стандартів (ISO/IEC 27001, «Загальні критерії» / ISO/IEC 15408) та національне законодавство, забезпечуючи легітимність оцінок та можливість безпекової інтеграції з партнерами по бізнесу, підрядниками й постачальниками послуг.

Дотримання цих вимог дозволить створити не просто теоретичну модель, а дієвий управлінський інструмент кібервитривалості. Така методика перетворить оцінювання з фіксатора технічних помилок на систему раннього попередження, яка допомагає підприємству використовувати перманентну турбулентність як стимул для капіталізації внутрішніх захисних резервів.

У результаті дослідження методичних підходів щодо оцінювання рівня інформаційної безпеки підприємств в умовах глобальної економічної турбулентності обґрунтовано безальтернативність переходу від статичного паперового аудиту до динамічних систем безперервного моніторингу. На основі системного аналізу доведено, що оцінювання безпекового контуру має базуватися на інтегрованій тріаді PPT (People, Processes, Technology), яка дозволяє одночасно вимірювати стійкість інфраструктури, адаптивність регламентів та кібергігієну персоналу. Критичний перегляд наукового доробку сучасників дозволив чітко диференціювати технічні, фінансові та управлінсько-інформаційні метрики, виявивши їхні обмеження у періоди макроекономічного хаосу та воєнного стану. Для подолання цих обмежень

використано розширену систему з 26 показників-коефіцієнтів, яка враховує рівень технологічного суверенітету компанії через частку внутрішнього програмно-технічного забезпечення. Сформований методичний каркас дозволив визначити чіткі вимоги до проєктування майбутньої авторської експрес-методики, ключовим імперативом якої є ризикоорієнтоване балансування вартості захисту із масштабами потенційних фінансових і репутаційних збитків суб'єкта господарювання.

Висновки до розділу 1

В першому розділі розкрито сутність, принципи та інструменти інформаційної безпеки суб’єктів підприємницької діяльності; систематизовано виклики та можливості в умовах глобальної економічної турбулентності; досліджено методичні підходи щодо оцінювання рівня інформаційної безпеки в умовах глобальної економічної турбулентності, що дає можливість зробити наступні висновки:

1. Обґрунтовано зміну парадигми оцінювання під впливом глобальних викликів. Доведено, що в умовах перманентної економічної турбулентності, макроекономічного дефіциту ресурсів та ведення активного кіберпротистояння класичні статичні методики аудиту (орієнтовані на періодичну фіксацію формальної відповідності стандартам «на папері») повністю втратили свою прогностичну здатність. Спираючись на державно-управлінський підхід, аргументовано, що сучасне оцінювання має зміститися у бік вимірювання динамічного «коефіцієнта нейтралізації» дворівневих деструктивних впливів – як щодо несанкціонованої ексфільтрації (добування) комерційних даних, так і щодо латентного впровадження шкідливого коду чи дезінформації.

2. Запроваджено системний підхід до структурування об'єкта аудиту. На основі критичного аналізу нормативно-правового базису та кращих ринкових практик у роботі деталізовано та адаптовано архітектурну тріаду

PPT (People, Processes, Technology). Концептуально доведено, що підсумкова захищеність підприємства є результатом синергетичної взаємодії трьох вимірів: технологічного контуру (програмно-апаратна стійкість системи), організаційного контуру (гнучкість та адаптивність бізнес-процесів) та кадрового контуру (інформаційна надійність, психологічна стійкість та рівень кібергігієни персоналу).

3. Здійснено класифікацію та виявлено обмеження наявних підходів вчених. Систематизація наукового доробку сучасників (А. В. Велігури, М. Ю. Журавля, С. М. Ілляшенка, О. Я. Кравчука, Н. Й. Реверчука) у межах сформованої аналітичної матриці дозволила диференціювати інструментарій оцінки за двома фундаментальними векторами. Виявлено, що перший підхід (орієнтований суто на локальну ефективність технічних засобів захисту від несанкціонованого доступу) є занадто обмеженим для умов кризи. Натомість обґрунтовано безальтернативність другого підходу, що базується на методології системного аналізу, де кожен локальний елемент захисту оцінюється через його безпосередній внесок у виконання загальносистемої функції – збереження життєздатності та безперервності діяльності всього суб'єкта господарювання.

4. Сформовано цілісну систему оціночних індикаторів. Розроблено та структуровано розширену систему з 26 показників-коефіцієнтів, згрупованих за п'ятьма стратегічними аналітичними блоками: оцінка програмно-технічної захищеності, аудит безпекових витрат, оцінка інформаційної надійності персоналу, оцінка якості та релевантності даних для осіб, які приймають рішення (ОПР), та оцінка архітектурної гнучкості системи. Особливу наукову цінність мають введені метрики оцінки частки унікального внутрішнього програмного та технічного забезпечення, які відображають рівень технологічного суверенітету та автономії підприємства в умовах розриву міжнародних логістичних ланцюгів постачання софту.

5. Визначено вимоги до розробки майбутнього інструментарію. На основі синтезу отриманих результатів сформульовано дев'ять імперативних

вимог до побудови майбутньої авторської методики. Обґрунтовано, що вона повинна мати експрес-характер, володіти властивістю масштабованості, спиратися на якісно-кількісний синергізм та обов'язково містити блок ризик-орієнтованого балансування, у межах якого фінансові витрати на безпеку жорстко зіставляються із масштабами потенційних фінансових і репутаційних збитків підприємства від реалізації кіберзагроз.

Список використаних джерел до розділу 1

1. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського Національного Університету*. 2023. Вип. 78(2). С. 134–139. DOI: https://doi.org/10.24144/2307-3322.2023.78.2.21

2. Ліпкан В. А., Харченко Л. С., Логінов О. В. Інформаційна безпека України: Глосарій. Київ: Текст, 2004. 136 с.

3. Данильян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації: навч. посіб. Харків: Фоліо, 2002. 285 с.

4. Гурковський В. І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства. *Правова інформатика.* 2010. No 2(26). С. 72–77.

5. Баранов О. П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. *Вісник Національної академії державного управління при Президентові України.* 2014. No 3. С. 60–65.

6. Шатун В. Т. Інформаційна безпека – невід’ємна складова національної безпеки України. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія»*. 2016. Т. 267. Вип. 255. С. 174–180.

7. Бондар І. Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation*. 2014. No 1. С. 68–75.

8. Ясінська А. І. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації. *Економіка та суспільство.* 2023. Вип. 56. DOI: https://doi.org/10.32782/2524-0072/2023-56-118

9. Інформаційна безпека підприємства: що це та як її забезпечити. NETWAVE. URL: https://netwave.ua/blog/informacijna-bezpeka-pidpriyemstva-sho-ce/

10. Чубаєвський В. І. Методи управління корпоративною інформаційною безпекою. *Економіка та суспільство.* 2022. Вип. 43. DOI: https://doi.org/10.32782/2524-0072/2022-43-49

11. Маркіна І. А., Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва*. 2016. No 3(1). С.80–88.

12. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

13. Стратегії кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

14. Шуст О. А., Варченко О. М., Крисанов Д. Ф. Стійкість продовольчого комплексу України в умовах посилення економічної турбулентності. *Продовольчі ресурси.* 2022. Т. 10. № 18. С. 287–301. DOI: https://doi.org/10.31073/foodresources2022-18-28

15. Ostrovska N., Popova L., Pylevych D., Panchenko O., Kozlianchenko O. Bazilinska O. Development of the Financial Services Market in the Conditions of Economic Turbulence. *International Journal of Computer Science and Network Security.* 2022. Vol. 22 (1). pp. 509–516. DOI: https://doi.org/10.22937/IJCSNS.2022.22.1.66

16. Grafton R. Q., Daugbjerg C., Qureshi M. E. Towards food security by 2050. *Food Security.* 2015. Vol. 7(2). pp. 179–183. DOI: https://doi.org/10.1007/s12571-015-0445-x

17. Van Bavel J. The world population explosion: causes, backgrounds and projections for the future. *Facts, views & vision in ObGyn*. 2013. Vol. 5(4). pp. 281–291.

18. Gardner B. Global food futures: Feeding the world in 2050. London: Bloomsbury Academic. 2013.

19. Meyers W. H., Kalaitzandonakes N. World Population, Food Growth, and Food Security Challenges. *Food Security in an Uncertain World: Frontiers of Economics and Globalization,* 2015. Vol. 15, pp. 161–177.

20. Alfieri F. Politics, economics, and demographics of food sustainability and security. *Reference Module of Elsevier Inc. in Food Science.* 2016. DOI: https://doi.org/10.1016/B978-0-08-100596-5.03435-1

21. Vasylieva N., James H. The effect of urbanization on food security and agricultural sustainability. *Economics and Sociology.* 2021. Vol. 14(1). pp. 76–88. DOI: https://doi.org/10.14254/2071-789X.2021/14-1/5

22. Rosário A. T., Raimundo R. Sustainable Entrepreneurship Education: A Systematic Bibliometric Literature Review. *Sustainability.* 2024. Vol. 16. pp. 784. DOI: https://doi.org/10.20944/preprints202310.1561.v1

23. Горник В. Г., Кравченко С. О. Механізми забезпечення інформаційної безпеки підприємницької діяльності як складника інформаційної безпеки держави. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління.* 2020. Том 31 (70). No 2. С. 206–212.

24. Аудит безпеки інформаційної безпеки. ТОВ «ТЗІ». 2023. URL: http://surl.li/yydqyk

25. Дячков Д. В. Методичні підходи до оцінки інформаційної безпеки підприємства. *Науковий вісник Полтавського університету економіки і торгівлі. Серія: Економічні науки.* 2012. № 4. С. 131–135. URL: https://surl.li/oexdge

26. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28- STD. 1985. URL: http://csrc.nist.gov/publications/history/dod85.pdf

27. Information Technology Security Evaluation Criteria, v. 1.2. – Office for Official publications of the European Communities, Printed and published by the Department of Trade and Industry, London, 1991. 164 p.

28. Canadian Trusted Computer Product Evaluation Criteria. URL: https://surl.li/wjvcqc

29. Federal Criteria for Information Technology Security. URL: https://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf

30. Common Criteria. 2024. Wikipedia. URL: https://uk.wikipedia.org/wiki/Common_Criteria

31. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства. *Управління проектами та розвиток виробництва*. 2014. №4(52). С. 28–39.

32. Журавель М. Ю. Полозова Т. В., Стороженко О. В. Формування системи показників оцінки рівня інформаційної безпеки підприємства. *Вісник економіки транспорту і промисловості.* 2011. № 33. С. 171–177.

33. Ілляшенко С. М. Економічний ризик: навч. посіб. 2-ге вид., доп., перероб. Київ: Центр навчальної літератури, 2004. 220 с.

34. Кравчук О. Я., Кравчук П. Я. Діагностика рівня та критерії оцінки корпоративної безпеки суб'єктів господарювання. *Збірник наукових праць Луцького державного технічного університету. Серія «Економіка та менеджмент».* 2004. Вип. 1. С. 85–109.

35. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур: монографія. Львів: ЛБІ НБУ, 2004. 195 с.

36. Крамаренко І.С., Іртищева І.О., Білоусова С.В., Іртищев О.С., Гарагуля А. В. Організаційно-управлінські механізми забезпечення інформаційної безпеки підприємницької діяльності в умовах цифрової трансформації економіки України. *Підприємництво та інновації*. 2024. Вип. 32. С. 246–252.

РОЗДІЛ 2
АНАЛІЗ ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКИХ ПЕРЕДУМОВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ГЛОБАЛЬНОЇ ЕКОНОМІЧНОЇ ТУРБУЛЕНТНОСТІ

2.1. Структурно-динамічний аналіз макроекономічних детермінант розвитку бізнес-систем

Дослідження методичних підходів до оцінювання інформаційної безпеки доводить, що формування ефективної системи захисту неможливе без чіткого усвідомлення передумов, які диктує сучасне макроекономічне середовище. Глобальна економічна турбулентність, що характеризується високим рівнем невизначеності, хаотичними змінами ринкових кон'юнктур, санкційними протистояннями та геополітичними кризами, повністю трансформувала безпековий ландшафт суб'єктів господарювання.

Сьогодні забезпечення інформаційної безпеки підприємства перетворилося з локального завдання ІТ-відділу на фундаментальну передумову збереження його життєздатності. В умовах глобальної турбулентності та гібридних воєн інформаційна безпека окремого підприємства (особливо стратегічного чи інфраструктурного) перестає бути суто приватним інтересом власника. Як обґрунтовано у науковій думці, ІБ підприємницької діяльності є невід'ємним складником інформаційної безпеки держави. Спроможність окремого суб'єкта господарювання нейтралізувати деструктивні зовнішні впливи (як-от кібератаки на системи управління чи витоки стратегічної інформації) безпосередньо визначає міру захищеності та стійкості основних сфер життєдіяльності всього суспільства й держави в цілому.

Ринковий хаос та геополітична нестабільність активізують сукупність джерел дестабілізуючих факторів, від окремих хакерів-інсайдерів до

транснаціональних угруповань та ворожих спецслужб. Передумовою виживання бізнесу стає готовність системи безпеки працювати за двома зустрічними векторами одночасно:

- вектор захисту від добування інформації: протидія промисловому шпигунству, ексфільтрації комерційних даних, витокам через інсайдерів;

- вектор захисту від впровадження інформації: нейтралізація шкідливого програмного коду, блокування фішингових атак та маніпулятивних впливів соціальної інженерії на персонал.

Під час турбулентності швидкість прийняття рішень суттєво зростає, а ціна помилки менеджера стає критичною. Головною передумовою якісного менеджменту є захист інформаційних потоків, що надходять до осіб, які приймають рішення. Якщо інформаційна служба підприємства надає неповну, неточну або суперечливу інформацію, це призводить до дезорганізації управління та фінансового краху. Таким чином, захист якості та валідності даних для ОПР є передумовою стратегічної стійкості компанії.

Економічна криза змушує підприємства жорстко економити ресурси. У таких умовах фінансування безпеки не може здійснюватися за залишковим принципом або, навпаки, бути безмежним. Важливою економічною передумовою є пропорційність, витрати на підтримку інформаційного захисту та придбання ресурсів мають бути чітко збалансовані із потенційною шкодою (збитками) для бізнесу, яка може виникнути в разі успішної реалізації загрози.

Варто погодитися з тим, що воєнний стан вимагає радикального переосмислення ролі підприємництва у структурі архітектоніки національної безпеки. Сучасний розвиток підприємницької діяльності слід розглядати не лише як джерело наповнення бюджетів чи створення робочих місць, а як стратегічний інструмент смарт-спеціалізації регіональних економічних систем. Маючи високий рівень адаптивності, підприємства здатні оперативно реагувати на деструктивні виклики середовища, забезпечуючи диверсифікацію ризиків у продовольчій, енергетичній та екологічній сферах країни. Проте, диджиталізація та релокація бізнесу в межах таких безпекових

стратегій критично залежать від стабільності інформаційних потоків, що підтверджує пряму залежність між рівнем захищеності корпоративного простору підприємств та їхньою спроможністю виступати донорами макроекономічної стабільності.

Для наочності та підвищення сканваності роботи, ключові передумови забезпечення інформаційної безпеки підприємства в умовах макроекономічної турбулентності доцільно згрупувати у вигляді класифікаційної таблиці 2.1.

Таблиця 2.1

Матриця передумов забезпечення інформаційної безпеки бізнесу під час турбулентності

Категорія передумов	Сутність та прояв чинника в умовах турбулентності	Наслідки ігнорування для підприємства
Політико-правові та державні	Необхідність суворого дотримання нормативно-законодавчих та договірних вимог держави й бізнес-партнерів у сфері захисту даних, а також розуміння ІБ підприємства як елемента безпеки держави.	Втрата ліцензій, юридичні санкції, руйнування партнерських ланцюгів постачання, загроза державним інтересам.
Соціально-кадрові	Зростання ризиків людського фактора, потреба в оцінці інформаційної надійності персоналу, підвищення його компетентності та кібергігієни.	Витоки інформації через навмисні дії (інсайдерство) або через низьку здатність працівників розпізнавати фішинг.
Технологічні	Стрімкий розвиток ІТ, ускладнення кібератак, необхідність безперервного моніторингу програмно-технічної захищеності інфраструктури.	Технічні збої, тривалий простій корпоративних систем, втрата цілісності та доступності баз даних.
Ринково-репутаційні	Пряма залежність ринкової вартості, ділової репутації компанії та іміджу її продукції від рівня захищеності комерційної таємниці й документообігу.	Руйнування репутації бренду, відтік клієнтів до конкурентів, падіння ринкової частки підприємства.

Джерело: згруповано автором.

Таким чином, дослідження передумов доводить, що інформаційна безпека в умовах турбулентності перестала бути ізольованим технічним поняттям. Вона є складним економіко-управлінським феноменом. Розуміння цих передумов вимагає від сучасного менеджменту впровадження інтегрованих систем оцінювання, де фінансові показники витрат на

інформаційні ресурси поєднуються з якісними метриками надійності людей та процесів, створюючи надійний фундамент для нейтралізації деструктивних ризиків.

Вказана наукова позиція Н. О. Пархоменко дозволяє розглядати передумови забезпечення інформаційної безпеки підприємства не як ізольовані внутрішні чинники, а як пряме відображення трансформаційного тиску рівнів економічного середовища [1]. Оскільки результативність діяльності сучасних бізнес-систем критично залежить від особливостей розвитку глобального простору, перманентна криза останнього миттєво проекціюється на захищеність корпоративних даних [1].

Екстраполюючи висновки дослідника на архітектуру інформаційної безпеки, можна стверджувати, що аналіз тенденцій макросередовища дає менеджменту змогу «визначити майбутні напрями та пріоритети розвитку» систем захисту інформації [1]. В умовах сучасної глобальної турбулентності цими пріоритетами стають:

1. Адаптація до багаторівневих криз, тобто інтеграція локальних засобів кіберзахисту підприємства у загальнонаціональні та міжнародні системи обміну даними про кіберзагрози (відповідно до локального, національного та глобального вимірів середовища) [1].

2. Динамічне прогнозування ризиків з використанням тенденцій глобального ринку для випереджального виявлення нових векторів атак (наприклад, уразливостей у хмарних технологіях чи штучному інтелекті) до того, як вони завдадуть прямої шкоди бізнес-системі [1].

3. Стратегічна гнучкість управління для переналаштування внутрішніх бізнес-процесів підприємства у відповідь на транскордонні інформаційні виклики та санкційні обмеження [1].

Таким чином, визначення передумов забезпечення ІБ через призму концепції Н. О. Пархоменко доводить: жодне підприємство сьогодні не спроможне вибудувати «абсолютний периметр захисту» у відриві від світового контексту [1]. Успішність функціонування безпекової архітектури

суб'єкта господарювання залежить від його здатності своєчасно рефлексувати на макроекономічні коливання, перетворюючи зовнішню турбулентність із джерела катастрофічних ризиків на орієнтир для модернізації систем управління ризиками.

Для аналізу динаміки інтеграції країн у світовий простір та оцінювання масштабів впливу макроекономічного середовища на вітчизняні бізнес-системи, сформуємо порівняльну таблицю на основі щорічних звітів Швейцарського економічного інституту (ETH Zurich) [2].

Рейтинг базується на Індексі глобалізації KOF (KOF Globalisation Index) [3], який оцінює країни за шкалою від 1 до 100 балів. Для наочності у таблиці 2.2. представлено лідерів світового рейтингу, найбільші економіки світу (США, Китай), а також динаміку зміни позицій України.

Таблиця 2.2

Динаміка рейтингу країн світу за Індексом глобалізації KOF (2018–2024 рр.)

Країна / Позиція	2018 рік	2019 рік	2020 рік	2021 рік	2022 рік	2023 рік	2024 рік
Нідерланди	90,52 (1)	90,68 (1)	90,81 (1)	90,44 (1)	89,92 (1)	89,80 (1)	89,15 (1)
Бельгія	89,72 (2)	89,45 (3)	89,53 (3)	89,20 (3)	89,14 (3)	89,22 (2)	88,94 (2)
Швейцарія	89,35 (3)	89,61 (2)	89,70 (2)	89,38 (2)	89,41 (2)	89,01 (3)	88,85 (3)
Велика Британія	88,40 (4)	88,12 (4)	88,05 (4)	87,60 (4)	87,42 (4)	87,55 (4)	87,40 (4)
Швеція	87,55 (5)	87,30 (5)	87,44 (5)	87,01 (5)	86,95 (5)	86,80 (5)	86,65 (5)
Німеччина	86,41 (8)	86,50 (7)	86,32 (8)	86,11 (8)	86,05 (8)	86,20 (6)	86,10 (6)
США	81,90 (24)	82,10 (23)	82,05 (24)	81,75 (25)	81,60 (25)	81,85 (24)	81,70 (24)
Китай	62,34 (78)	63,10 (75)	63,55 (74)	64,12 (72)	64,25 (71)	64,50 (70)	64,80 (69)
УКРАЇНА	70,12 (45)	70,45 (44)	70,55 (44)	70,10 (46)	67,40 (52)	66,80 (55)	66,12 (58)

Джерело: згруповано автором [3]

Статистичний аналіз динаміки Індексу глобалізації KOF (табл. 2.2) дозволяє емпірично підтвердити теоретичну тезу Н. О. Пархоменко про те, що результативність діяльності локальних бізнес-систем критично залежить від трендів глобального середовища [1]. Стабільне лідерство країн Західної Європи (Нідерланди, Бельгія, Швейцарія) зумовлене їх максимальною відкритою інтеграцією у транскордонні фінансові та інформаційні потоки.

У період 2018–2020 років показники України демонстрували помірне зростання, утримуючи позиції у першій півсотні найбільш глобалізованих країн світу (44–45 місця). Проте починаючи з 2022 року, під впливом повномасштабного геополітичного та воєнного шоку, відбулося стрімке падіння загального індексу – з 70,55 балів у 2020 році до 66,12 балів у 2024 році із відповідним зміщенням на 58-ме місце в рейтингу.

Така деградація індексу відображає архітектурну деформацію економічного середовища. Через воєнні дії та блекаути бізнес-системи зіткнулися з частковим розривом логістичних ланцюгів та фізичним пошкодженням інфраструктури зв'язку. Водночас падіння економічного субіндексу компенсується аномальним зростанням політичної та соціальної інтеграції України у світовий простір.

Для системи управління інформаційною безпекою підприємств це падіння є прямим індикатором зростання зовнішніх ризиків. Зменшення загальної глобалізації на тлі ведення кібервійни означає, що вітчизняні підприємства змушені функціонувати в умовах асиметричного тиску: з одного боку, інтенсивність транскордонних кібератак з глобального рівня постійно зростає, а з іншого – можливості безпекового інвестування на локальному рівні є критично обмеженими [1]. Це остаточно доводить необхідність розробки гнучких інструментів експрес-оцінювання інформаційної безпеки (табл. 2.2), здатних оперативно реагувати на деструктивні каскадні макроекономічні впливи.

Для глибокого аналізу інституційних умов функціонування вітчизняних підприємств та оцінювання передумов їхньої інформаційної безпеки, необхідно дослідити траєкторію інтеграції України у світовий бізнес-простір.

Тривалий час головним макроекономічним орієнтиром для уряду та підприємницьких структур виступав щорічний звіт Світового банку «Ease of Doing Business» (Індекс легкості ведення бізнесу) [4]. Він оцінював країни за 10 ключовими індикаторами (від реєстрації підприємств до міжнародної торгівлі та забезпечення виконання контрактів). Після 2020 року Світовий

банк призупинив публікацію класичного рейтингу Doing Business через внутрішні методологічні коригування, а починаючи з 2024 року запустив принципово новий, більш жорсткий та сучасний індекс – «Business Ready» (B-READY) [5]. Новий індекс фокусується не лише на простоті законів, а й на цифровізації, екологічності та реальному дотриманні правил гри на практиці. В таблиці 2.3. наведено ретроспективну динаміку позицій України, яка наочно ілюструє шлях реформ та вплив глобальної турбулентності на бізнес-середовище.

Таблиця 2.3

Історична динаміка позицій України в індексі легкості ведення бізнесу (Doing Business / B-READY)

Рік звіту	Місце України у глобальному рейтингу	Ключовий вектор змін та інституційні передумови
2012	152 місце (із 183)	Історичний мінімум. Критично висока бюрократія, тотальний тиск на бізнес, повна відсутність цифрових сервісів захисту даних.
2014	112 місце (із 189)	Початок перших реформ у сфері реєстрації власності та спрощення процедур започаткування бізнесу.
2016	83 місце (із 189)	Переломний момент: старт масштабної діджиталізації державних послуг, зменшення кількості податкових перевірок.
2018	76 місце (із 190)	Суттєве покращення в індикаторах «Отримання дозволів на будівництво» та «Підключення до систем енергопостачання».
2020	64 місце (із 190)	Історичний максимум України в Doing Business. Прорив у сфері захисту міноритарних інвесторів, спрощення міжнародної торгівлі та реєстрації компонентів бізнесу.
2024–2026	Перехід на індекс B-READY	Оцінювання в умовах воєнного стану. Світовий банк аналізує стійкість цифрової інфраструктури, адаптивність законодавства до форс-мажорів та безперервність бізнесу (Business Continuity).

Джерело: згруповано автором [4].

Стрімкий підйом України у рейтингу з 152-го на 64-те місце став можливим завдяки тотальній цифровізації (перехід на електронний документообіг, онлайн-реєстрацію, державні цифрові платформи). Проте, спрощення процедур «на вході» автоматично розширило площину цифрових уразливостей. Кожне підприємство, інтегруючись у загальнодержавне

цифрове середовище, стає потенційною мішенню для кібератак, що робить ІБ головною передумовою безперервності цієї інтеграції. Позиція України в індикаторі «Міжнародна торгівля» напряму залежить від безпеки ланцюгів постачання. В умовах турбулентності та воєнного стану, будь-який злам логістичних систем підприємства, підміна даних у митних деклараціях чи витік інформації про контракти руйнує ділову репутацію та паралізує зовнішньоекономічні операції.

У контексті дослідження передумов інформаційної безпеки (ІБ) підприємницької діяльності, важливим інституційним зрушенням глобального економічного середовища став запуск Світовим банком у 2024 році нової флагманської оціночної системи – Business Ready (B-READY), яка прийшла на зміну класичному рейтингу Doing Business.

Головна відмінність нової методології полягає у переході від оцінювання суто формального законодавства (de jure) до вимірювання реальної операційної ефективності та практики виконання правил (de facto). Відповідно до архітектури B-READY, бізнес-середовище оцінюється за трьома фундаментальними стовпами (Pillars): Нормативно-правова база, Державні послуги (інфраструктура та її цифровізація) та Операційна ефективність(реальна простота щоденної діяльності фірм).

Оскільки Світовий банк впроваджує індекс поетапно (пілотний звіт 2024 року охопив перші 50 країн світу, а повний охоплюючий рейтинг із включенням України формується у 2026 році), для вітчизняних бізнес-систем критично важливим є випереджальний аналіз нових індикаторів. Нова філософія оцінювання Світового банку [6] вводить наскрізні тренди цифрової трансформації та стійкості, що висуває жорсткі вимоги до внутрішньої інформаційної безпеки підприємств:

1. Стовп «Державні послуги». Нова методологія високо оцінює країни, які забезпечують тотальну діджиталізацію взаємодії бізнесу та держави (онлайн-реєстрація, цифрові податкові сервіси, відкриті реєстри). Для українського бізнесу, який функціонує в умовах воєнного стану та глибоко

інтегрований у державні цифрові екосистеми, це створює передумову обов'язкового кіберзахисту каналів зв'язку та цифрових підписів для запобігання несанкціонованому втручанню [6].

2. Стабільність інфраструктури. Індикатори B-READY оцінюють надійність і доступність цифрової інфраструктури ринку. В умовах турбулентності, макроекономічного хаосу та блекаутів, інформаційна безпека підприємства трансформується у концепцію «Безперервності бізнесу» (Business Continuity). Це вимагає від архітектури інформаційна безпека готовності забезпечувати безперебійне функціонування корпоративних систем навіть за умов критичних технічних або інфраструктурних збоїв [6].

3. Захист міжнародного вектора. Оцінка ефективності електронного митного адміністрування та логістики доводить уразливість транскордонних інформаційних потоків. Будь-яка компрометація даних підприємства (виток комерційних контрактів, підміна логістичних треків) руйнує його операційну ефективність та зупиняє експортно-імпортну діяльність[6].

Таким чином, глобальний інституційний перехід на індекс B-READY доводить, що сприятливі умови для ведення бізнесу в сучасну епоху більше не тотожні простій відсутності паперової бюрократії [6]. Нова парадигма Світового банку трактує «готовність до бізнесу» як спроможність компанії забезпечувати операційну витривалість і безпеку своїх цифрових активів. Оскільки Україна перебуває на шляху повної інтеграції у нові глобальні стандарти оцінювання, впровадження гнучких інструментів вимірювання інформаційна безпека є імперативною передумовою для збереження конкурентоспроможності вітчизняних підприємств під час макроекономічного шторму.

Методологічне підтвердження синергетичного зв'язку між макроекономічними інституціями та життєздатністю бізнесу знаходимо у концепції Рейтингу світової конкурентоспроможності (IMD World Competitiveness Yearbook). Науково доведено, що конкурентоспроможність будь-якої економічної системи є комплексною категорією, яку неможливо

звести суто до динаміки ВВП чи показників продуктивності праці, оскільки реальні суб'єкти господарювання змушені постійно взаємодіяти з політичними, соціальними, культурними та інфраструктурними аспектними середовища [7].

У межах цього підходу визначено, що головним завданням держав та інституцій є формування такого простіру, який через ефективну інфраструктуру та зважену політику заохочує підприємства до довгострокового створення сталої вартості. Екстраполюючи зазначені положення на умови глобальної турбулентності та воєнного стану, можна стверджувати, що інформаційна безпека підприємства сьогодні трансформувалася у фундаментальний фактор його міжнародної та внутрішньої конкурентоспроможності.

Розглядаючи структуру факторів конкурентоспроможності IMD (економічна діяльність, ефективність уряду, ефективність бізнесу та інфраструктура) крізь призму завдань інформаційного захисту, доцільно виокремити такі стратегічні передумови:

1. Безпека цифрової інфраструктури як базис конкурентоспроможності. Створення бізнесом сталої вартості у сучасних реаліях повністю спирається на технологічну інфраструктуру (хмарні обчислення, автоматизовані системи управління, великі дані). Спроможність уряду та внутрішнього менеджменту захистити цю інфраструктуру від кібердиверсій та транскордонних атак безпосередньо визначає життєздатність бізнес-системи в епоху хаосу.

2. Адаптивність бізнесу до соціально-політичних шоків. Оскільки підприємства мають справлятися з нелінійними викликами (включаючи інформаційні війни, маніпулятивні впливи та кризу людського капіталу), оцінка інформаційної надійності та кібергігієни персоналу (Метрики кадрового контуру) стає ключовою умовою збереження інтелектуального та операційного потенціалу компанії.

3. Ефективність управління в умовах невизначеності. Довгострокове створення цінності потребує від осіб, які приймають рішення (ОПР),

абсолютно валідних, захищених та релевантних даних. Забезпечення інформаційної безпеки управлінських потоків мінімізує ризики дезорганізації бізнесу та стратегічних помилок керівництва під час ринкового шторму.

Для емпіричного підтвердження зазначених теоретичних положень, внесемо статистичні дані щодо оцінки конкурентоспроможності України у вигляді порівняльної таблиці 2.4.

Таблиця 2.4

Позиції України у Рейтингу світової конкурентоспроможності IMD (2019–2024 рр.)

Рік звіту	Місце України у глобальному рейтингу	Ключові чинники впливу на бізнес-середовище
2019	54 місце (із 63)	Помірна макроекономічна стабілізація, початок системного впровадження цифрових технологій в управління.
2020	55 місце (із 63)	Вплив першої хвилі пандемічного шоку, уповільнення темпів зростання інфраструктурних чинників.
2021	54 місце (із 64)	Стабілізація позицій за рахунок адаптації IT-сектору та високої гнучкості малого і середнього бізнесу.
2022–2024	Тимчасово виключено з рейтингу	Оцінювання призупинено експертами IMD через форс-мажорні обставини воєнного стану (відсутність повної та достовірної державної статистичної звітності щодо ВВП та інвестицій).

Джерело: сформовано автором [7].

Таким чином, методологічні засади рейтингу світової конкурентоспроможності доводять, що у часи перманентної кризи виживання бізнес-систем залежить не від статичних фінансових показників, а від їхньої здатності ефективно керувати своїми можливостями у ворожому зовнішньому середовищі. Тимчасове виключення України з класичних міжнародних рейтингів (таких як IMD) через форс-мажорні обставини лише підкреслює критичну потребу у розробці авторських локальних методик оцінювання (експрес-аудиту), які здатні вимірювати рівень інформаційної безпеки та операційної витривалості українських підприємств de facto в умовах дефіциту офіційної макроекономічної інформації.

Нажаль, після повномасштабного вторгнення росії, для України є неможливим визначити індекс конкурентоспроможності. Україна не бере участі в глобальному рейтингування за індексом конкурентоспроможності аж до моменту настання перемоги. Ця ситуація викликає певні труднощі для оцінки економічного потенціалу та визначення ключових напрямків розвитку бізнесу в країні. Однак, це також означає, що під час відновлення після конфлікту Україні буде важливо зосередити зусилля на реформах та стратегіях, які могли б підвищити її конкурентоспроможність на глобальному рівні.

Глобальний індекс конкурентоспроможності може вважатися індикатором розвитку системи управління бізнесу в країні, оскільки він охоплює широкий спектр факторів, які безпосередньо або опосередковано впливають на здатність підприємств ефективно конкурувати на внутрішньому та міжнародному ринках. Включення таких позицій, як інноваційний потенціал, ефективність ринку праці, розвиток фінансового ринку та готовність до прийняття технологій, безпосередньо вказує на якість управління на рівні як окремих підприємств, так і в умовах національної економіки загалом.

В цілому, за даними міжнародних рейтингів Україна постійно зміцнює свої позиції, що обґрунтовується науково-технічним прогресом, цифровою трансформацією, боротьбою з корупцією, підвищенням рівням національної безпеки, зростанням внутрішнього ринку.

Оптова та роздрібна торгівля, ремонт автотранспортних засобів і мотоциклів, а також промисловість є найбільшою у структурі валової доданої вартості національної економіки України і виступає бюджетоформуючою сферою, адже питома вага даного комплексу у зведеному бюджеті України сягає 30 відсотків. Так, валова додана вартість України за видами економічної діяльності відображена у табл. 2.5. Загальний обсяг валової доданої вартості України за досліджуваний період зріс у фактичних цінах на 4 868 230 млн грн, досягнувши у 2023 році відмітки у 5 822 702 млн грн, що вказує на часткову

адаптаційну стабілізацію та відновлення економічної активності бізнес-систем після катастрофічних руйнувань першого року повномасштабного вторгнення.

Таблиця 2.5

Валова додана вартість України за видами економічної діяльності

Види економічної діяльності	2010	2015	2019	2022	2023	Приріст 2023–2010 (+/-)
ВДВ у основних цінах, млн грн	954 472	1 689 387	3 421 628	4 626 192	5 822 702	+4 868 230
Сільське, лісове та рибне госп-во	80 385	239 806	356 563	449 148	500 540	+420 155
Промисловість *	244 167	393 142	790 638	874 309	1 161 179	+917 012
Будівництво	35 366	38 928	107 430	69 299	103 883	+68 517
Оптова та роздрібна торгівля; ремонт	154 994	273 989	525 974	645 455	865 700	+710 706
Транспорт, складське госп-во, пошта	83 027	134 978	264 689	226 716	289 201	+206 174
Тимчасове розміщування та харчування	8 932	11 946	35 311	30 057	42 448	+33 516
Інші види економічної діяльності **	347 601	596 598	1 341 023	2 331 208	2 859 751	+2 512 150
ВДВ у основних цінах, %	100	100	100	100	100	–
Сільське, лісове та рибне госп-во	8,42	14,19	10,42	9,71	8,6	+0,18
Промисловість *	25,58	23,27	23,11	18,9	19,94	-5,64
Будівництво	3,71	2,3	3,14	1,5	1,78	-1,93
Оптова та роздрібна торгівля; ремонт	16,24	16,22	15,37	13,95	14,87	-1,37
Транспорт, складське госп-во, пошта	8,7	7,99	7,74	4,9	4,97	-3,73
Тимчасове розміщування та харчування	0,94	0,71	1,03	0,65	0,73	-0,21
Інші види економічної діяльності **	36,42	35,31	39,19	50,39	49,11	+12,69

* Примітка 1: Показник «Промисловість» розраховано за методологією Держстату як суму секцій B (Добувна), C (Переробна), D (Енергетика) та E (Водопостачання та відходи).

**Примітка 2: До «Інших видів» віднесено ІТ-сектор, фінансову діяльність, операції з нерухомістю, освіту, медицину та державне управління (частка якого суттєво зросла у 2022–2023 рр. через фінансування оборонного контуру).

Джерело: сформовано на підставі [8].

У розрізі структурного аналізу спостерігається подолання пікових деформацій 2022 року та поступове вирівнювання траєкторій ключових галузей. Зокрема, сектор промисловості у 2023 році збільшив свій абсолютний внесок до 1 161 179 млн грн, зафіксувавши частку на рівні 19,94% (проти 18,90% у 2022 році). Сектор оптової та роздрібної торгівлі; ремонту також продемонстрував висхідну динаміку, згенерувавши 865 700 млн грн або 14,87% сукупної ВДВ. Разом ці два вектори господарювання забезпечують майже 35% базисного макроекономічного доходу і залишаються фундаментом приватного підприємництва.

Помітна стабілізація сектору торгівлі (+1,37% абсолютного приросту за 2023 рік) та промисловості (+1,04%) є відображенням успішного переформатування внутрішніх бізнес-моделей: відновлення ланцюгів постачання, переорієнтація збуту, глибока диверсифікація та релокація потужностей.

Інтенсифікація кіберризиків у торгівлі та логістиці. Стабілізація сектору торгівлі (до 865,7 млрд грн) відбулася завдяки форсованій автоматизації та міграції бізнесу в хмарні архітектури, електронну комерцію (E-commerce) і безготівкові розрахункові системи. Відповідно, безпековий фокус для торговельних підприємств зміщується у площину захисту персональних даних покупців, упередження атак класу Ransomware та забезпечення високої відмовостійкості розподілених цифрових платформ.

Захист технологічного контуру промислових гігантів. Часткове відновлення індустріальних підприємств (до 1 161,1 млрд грн) в умовах воєнного часу супроводжується активним використанням віддалених систем моніторингу та управління. Забезпечення інформаційної безпеки у цьому секторі є критичним не лише для збереження комерційної таємниці чи

унікальних In-house технологій, а й для фізичного захисту промислових об'єктів від кібердиверсій, спрямованих на АСУ ТП.

Особливу увагу привертає аномальне зростання частки «Інших видів діяльності» (до 49,11% у 2023 році), що де-факто спричинено різким збільшенням державних видатків на сектор безпеки й оборони (державне управління), а також стабільним функціонуванням вітчизняного ІТ-сектору та телекомунікацій, які виступили цифровим щитом держави.

Таким чином, розширений аналіз підтверджує наукову доцільність фокусування подальшого прикладного інструментарію експрес-оцінювання інформаційної безпеки саме на підприємствах торгівлі та промисловості, як ключових ринкових домінантах, що забезпечують життєздатність сучасної суверенної економічної системи України під час затяжної кризової фази.

Повномасштабне воєнне вторгнення рф у 2022 році радикально деформувало траєкторію розвитку вітчизняного підприємництва, перевівши більшість суб'єктів господарювання у режим вимушеної екстремальної адаптації або фізичного виживання. Значна частина промислово розвинених територій України опинилася в зоні активних бойових дій або під тимчасовою окупацією, що зумовило хвилю тотальної деструкції виробничих ланцюгів, ліквідації, банкрутства та вимушеної реорганізації бізнес-структур.

З метою нівелювання катастрофічних втрат та збереження стратегічного потенціалу реального сектору економіки, Урядом України було ініційовано масштабну програму державної підтримки щодо релокації бізнесу. Інституційним підґрунтям цього процесу стало ухвалення Кабінетом Міністрів України Постанови №305 від 17.03.2022 р., яка регламентувала механізм безоплатного перевезення майна вітчизняних підприємств, установ та організацій залізничним та автомобільним транспортом. Наступним кроком стало затвердження Розпорядження КМУ №246-р від 25.03.2022 р., яким було впроваджено План невідкладних заходів щодо переміщення виробничих потужностей з територій, де ведуться бойові дії та/або є загроза бойових дій, на безпечні території західних та центральних регіонів держави [9].

Реалізація зазначених урядових заходів дозволила у стислі терміни успішно евакуювати 772 підприємства та зберегти понад 35 тисяч робочих місць, що мінімізувало ризики безробіття та підтримало податкову базу країни в критичний період. Проте, релокація актуалізувала системні безпекові виклики: переміщення виробництв у єдиний цифровий та фізичний простір вимагало від менеджменту компаній радикальної перебудови політики інформаційної безпеки, захисту баз даних та комерційної таємниці в умовах віддаленого доступу та міграції IT-інфраструктури.

Трансформаційні наслідки зазначеного воєнного шоку та подальшої адаптації бізнесу чітко простежуються у макроекономічних показниках Державної служби статистики України [8]. Проведена декомпозиція та перерахунок структури Валової доданої вартості (ВДВ) України за період 2010–2023 рр. (табл. 2.5) підтверджує, що попри різке падіння промислового виробництва та торгівлі у 2022 році, заходи з релокації та диверсифікації дозволили цим секторам продемонструвати адаптаційне відновлення вже у 2023 році, згенерувавши відповідно 1 161 179 млн грн (19,94% ВДВ) та 865 700 млн грн (14,87% ВДВ).

Аналіз структурно-динамічних зрушень у секторі вітчизняного бізнесу (табл. 2.6) свідчить про глибоку інституційну трансформацію підприємницького середовища України під впливом перманентних кризових шоків, зумовлених як тривалими структурними деформаціями, так і повномасштабною агресією рф.

Отримані результати розрахунків свідчать, що теза про «повну зупинку» підприємницької діяльності після початку повномасштабного вторгнення є справедливою лише для критичного 2022 року, коли загальна кількість суб'єктів скоротилася до мінімальних 1 732 508 одиниць. Натомість показники 2023 року (1 913 193 од.) та 2024 року (1 949 408 од.) демонструють стрімку адаптивну регенерацію бізнес-середовища, майже нівелюючи загальний спад порівняно з довоєнним 2021 роком.

Таблиця 2.6

Основні показники діяльності суб’єктів великого, середнього, малого та мікропідприємництва

Групи суб'єктів підприємництва та їх структура	2010	2015	2020	2022	2024	Відхилення 2024/2010 (+/-)
1. СУБ’ЄКТИ ВЕЛИКОГО ПІДПРИЄМНИЦТВА, од	586	423	512	494	560	-26
великі підприємства (юридичні особи), од	586	423	512	494	560	-26
питома вага у структурі групи, %	100	100	100	100	100	0
2. СУБ’ЄКТИ СЕРЕДНЬОГО ПІДПРИЄМНИЦТВА, од	21 343	15 510	17 946	15 037	14 208	-7 135
середні підприємства (юридичні особи), од	20 983	15 203	17 602	14 783	14 016	-6 967
питома вага у структурі групи, %	98,31	98,02	98,08	98,31	98,65	+0,34
фізичні особи-підприємці (ФОП), од	360	307	344	254	192	-168
питома вага у структурі групи, %	1,69	1,98	1,92	1,69	1,35	-0,34
3. СУБ’ЄКТИ МАЛОГО ПІДПРИЄМНИЦТВА (з мікро), од	2 161 999	1 958 385	1 955 119	1 716 977	1 934 640	-227 359
малі підприємства (юридичні особи), од	357 241	327 814	355 708	246 647	271 021	-86 220
питома вага у структурі групи, %	16,52	16,74	18,19	14,37	14,01	-2,51
фізичні особи-підприємці (ФОП), од	1 804 758	1 630 571	1 599 411	1 470 330	1 663 619	-141 139
питома вага у структурі групи, %	83,48	83,26	81,81	85,63	85,99	+2,51
в т.ч. СУБ’ЄКТИ МІКРОПІДПРИЄМНИЦТВА (складова малого), од	2 093 688	1 910 830	1 898 902	1 671 558	1 890 506	-203 182
мікропідприємства (юридичні особи), од	300 445	284 241	307 871	206 213	232 886	-67 559
питома вага у структурі групи, %	14,35	14,88	16,21	12,34	12,32	-2,03
фізичні особи-підприємці (ФОП), од	1 793 243	1 626 589	1 591 031	1 465 345	1 657 620	-135 623
питома вага у структурі групи, %	85,65	85,12	83,79	87,66	87,68	+2,03

Загальна кількість суб'єктів господарювання, од	2 183 928	1 974 318	1 973 577	1 732 508	1 949 408	-234 520

* Примітка 1: Внутрішні структурні частки (%) розраховано автором на основі абсолютних первинних даних Держстату України. Фізичні особи-підприємці не можуть виступати суб'єктами великого підприємництва відповідно до чинного законодавства України.

* Примітка 2: Дані за 2014–2021 роки наведено без тимчасово окупованої території АР Крим та ОРДЛО; дані за 2022–2024 роки – без урахування тимчасово окупованих РФ територій та зон інтенсивних бойових дій.

Джерело: сформовано на підставі [8].

Після різкого падіння у 2022 році (до 494 од.), сектор великого підприємництва зріс до 560 одиниць у 2024 році. Хоча загальне відхилення порівняно з 2010 роком залишається негативним (-26 од.), висхідна тенденція останніх років доводить ефективність механізмів релокації великих потужностей, відновлення пошкоджених промислових об'єктів та побудови нових логістичних хабів.

Середнє підприємництво виявилося найбільш вразливим у довгостроковій перспективі. Його чисельність послідовно зменшується, досягнувши у 2024 році значення 14 208 одиниць (загальне падіння на 7 135 од. або на 33,4% порівняно з 2010 р.). Середній бізнес, позбавлений гнучкості мікроструктур та фінансової подушки великих корпорацій, продовжує відчувати дефіцит оборотного капіталу, кваліфікованих кадрів та доступу до безпечних ринків.

Абсолютне відновлення кількісних показників економіки забезпечено виключно сектором малого (і, зокрема, мікро-) підприємництва, де головним драйвером виступили фізичні особи-підприємці. У 2024 році чисельність малого бізнесу сягнула 1 934 640 од., причому питома вага ФОП у цій групі зафіксувалася на рекордному рівні – 85,99% (проти 83,48% у 2010 р.). У межах мікропідприємництва частка самозайнятих осіб досягла історичного максимуму – 87,68% (1 657 620 ФОП з-поміж 1 890 506 суб'єктів).

Стрімке зростання кількості ФОП (понад 1,66 млн у 2024 році) свідчить про те, що значна частина національного продукту створюється поза межами захищених корпоративних офісів чи класичних заводських контурів. Масове

використання особистих девайсів (концепція BYOD), незахищених домашніх мереж WI-FI під час блекаутів, а також використання публічних месенджерів та хмарних сервісів для ведення фінансового та складського обліку робить мікропідприємства першочерговою мішенню для кібератак.

Оскільки великі промислові та торговельні компанії інтегрують у свої операційні цикли сотні дрібних контрагентів, перевізників та постачальників послуг у статусі ФОП, низький рівень кібергігієни останніх створює критичні бекдори у загальній інфраструктурі безпеки. Зловмисники дедалі частіше атакують слабко захищені ІТ-вузли мікрофірм, щоб через спільні бази даних або системи електронного документообігу отримати доступ до корпоративних секретів великих ринкових суб'єктів.

Отже, статистичні тренди 2024 року підтверджують наукову доцільність розроблення в межах дослідження прикладного інструментарію оцінювання інформаційної безпеки, який здатний масштабуватися та адаптуватися до умов глибокої децентралізації бізнес-процесів і високої питомої ваги мікросуб’єктів у загальній структурі національної економіки.

Обчислення відсоткових часток суб'єктів господарювання за галузевим та розмірним критеріями (табл. 2.7) дозволяє деталізувати архітектуру українського ринку та виявити стійку тенденцію до атомізації бізнес-середовища. Статистичні дані спростовують класичне уявлення про паритетний розподіл сил між великим, середнім та малим бізнесом: в усіх без винятку досліджуваних секторах економіки частка малого підприємництва (разом із мікро-) перевищує 94%, а у середньому по країні становить 99,24% станом на 2024 рік.

Сектор промисловості традиційно залишається сферою з найвищою часткою великих (0,24% у 2024 р.) та середніх (3,84%) підприємств. Попри те, що сумарно вони становлять трохи більше 4% від кількості індустріальних суб'єктів, саме вони акумулюють основні засоби, промисловий капітал та генерують левову частку галузевої ВДВ. Зниження частки середнього промислового бізнесу з 5,51% (2010 р.) до 3,84% (2024 р.) відображає процес

вимивання «середнього класу» промисловості через воєнні руйнування та фінансові шоки.

Таблиця 2.7

Структурний розподіл суб’єктів господарювання України за видами економічної діяльності та розмірами у 2010–2024 рр. (у % до загальної кількості відповідного виду діяльності)

Вид економічної діяльності	Рік	Суб'єкти великого підприємництва, %	Суб'єкти середнього підприємництва, %	Суб'єкти малого (вкл. мікро) підприємництва, %	Разом, %
Сільське, лісове та рибне господарство (Секція A)	2010	0,02	1,83	98,15	100
	2020	0,02	2,75	97,23	100
	2022	0,01	2,78	97,21	100
	2024	0,02	2,82	97,16	100
Промисловість (Секції B, C, D, E)	2010	0,38	5,51	94,11	100
	2020	0,26	4,21	95,53	100
	2022	0,22	3,92	95,86	100
	2024	0,24	3,84	95,92	100
Будівництво (Секція F)	2010	0,03	1,29	98,68	100
	2020	0,01	0,92	99,07	100
	2022	0,01	0,74	99,25	100
	2024	0,01	0,69	99,3	100
Оптова та роздрібна торгівля; ремонт (Секція G)	2010	0,01	0,44	99,55	100
	2020	0,01	0,4	99,59	100
	2022	0,01	0,32	99,67	100
	2024	0,01	0,3	99,69	100
Транспорт, складське госп-во, пошта (Секція H)	2010	0,09	1,48	98,43	100
	2020	0,05	0,84	99,11	100
	2022	0,04	0,68	99,28	100
	2024	0,05	0,67	99,28	100
Інформація та телекомунікації (IT) (Секція J)	2010	0,03	1,42	98,55	100
	2020	0,01	0,21	99,78	100
	2022	0,01	0,11	99,88	100
	2024	0,01	0,09	99,9	100
Усього по економіці України	2010	0,03	0,98	98,99	100
	2020	0,03	0,91	99,06	100
	2022	0,03	0,87	99,1	100

	2024	0,03	0,73	99,24	100

Джерело: сформовано на підставі [8].

У секторі оптової та роздрібної торгівлі (Секція G) частка малого бізнесу є константно високою і досягла у 2024 році 99,69%. Велика торговельна мережа чи дистриб'ютор припадає на тисячі дрібних ФОП та мікрофірм.

Найбільш динамічні та радикальні структурні зміни демонструє IT-сектор (Секція J). Якщо у 2010 році частка середнього бізнесу тут становила помітні 1,42%, то у 2024 році вона впала до критичних 0,09%, тоді як малий і мікробізнес (переважно ФОП-програмісти) зайняв 99,90% галузі. Це свідчить про повну віртуалізацію та глибоку інституційну децентралізацію цифрової індустрії України.

У промисловості, де частка великого/середнього бізнесу є відносно найвищою (понад 4%), системи інформаційної безпеки повинні орієнтуватися на класичні «тяжкі» корпоративні стандарти захисту (на кшталт ISO/IEC 27001), оскільки кібератака на такі суб'єкти загрожує зупинкою критичної інфраструктури та виробництва.

Оскільки у торгівлі та IT малий бізнес охоплює відповідно 99,69% та 99,90% ринку, розробка складних локальних (On-Premise) систем безпеки для них є економічно недоцільною та неможливою через дефіцит бюджету. Для цих секторів прикладний інструментарій експрес-оцінювання інформаційної безпеки має спиратися на легкі, автоматизовані сервіси оцінки хмарного середовища, захисту мобільних робочих місць та базову кібергігієну, що дозволить мінімізувати масові ризики витоку інформації у масштабах усієї національної економіки.

У сучасній макроекономічній науці для оцінки структури ринку традиційно використовуються індекси концентрації (наприклад, Індекс Херфіндаля-Хіршмана) [10], які фокусуються на монополізації ринку великими гравцями. Проте для країн із трансформівною економікою та країн, що перебувають у стані форс-мажорних (воєнних) шоків, критично важливим

є протилежний процес – атомізація бізнес-середовища (розосередження економічної активності серед надвеликої кількості мікросуб'єктів).

Коефіцієнт щільності мікробізнесу (*Кщм*) це структурно-інституційний індикатор, який відображає ступінь демографічного навантаження мікросегменту (мікропідприємств та фізичних осіб-підприємців) на один суб'єкт капіталомісткого (великого та середнього) бізнесу.

Показник дозволяє оцінити:

- рівень інституційної децентралізації та віртуалізації окремої галузі;
- ступінь сформованості горизонтальних бізнес-мереж (екосистем);
- масштаб та архітектуру «поверхні кібератак» у межах галузевих ланцюгів постачання.

Розрахунок коефіцієнта здійснюється на основі офіційних пооб'єктних чи галузевих даних демографії підприємств (Держстату України або Eurostat) за такою формулою:

$$К_{щм} = \frac{N_{мікро\_юр} + N_{фоп}}{N_{вел} + N_{серед}} \quad (2.1.)$$

де:

$К_{щм}$– коефіцієнт щільності мікробізнесу в аналізованій сукупності (галузі, регіоні або економіці загалом), од.;

$N_{мікро\_юр}$– кількість діючих юридичних осіб, які за критеріями Господарського кодексу України належать до мікропідприємств (чисельність до 10 осіб, дохід до 2 млн євро), од.;

$N_{фоп}$– кількість діючих фізичних осіб-підприємців (оскільки в Україні понад 99% ФОП за обсягами доходу та найманої праці де-факто є мікросуб'єктами), од.;

$N_{вел}$– кількість діючих суб'єктів великого підприємництва (юридичних осіб), од.;

$N_{сер}$– кількість діючих суб'єктів середнього підприємництва (включаючи юридичних осіб та поодинокі великі ФОП, що входять до цієї групи), од.

Залежно від отриманого абсолютного значення $К_{мщ}$, галузеві ринки класифікуються за трьоми рівнями структурної щільності:

1. Низька щільність / Індустріально-корпоративний тип ($К_{мщ} > 50$): Характерний для важкої промисловості, енергетики, інфраструктурних секторів. Економіка галузі тримається на великих капітальних активах. Бізнес-процеси жорстко централізовані.

2. Середня щільність / кооперативно-трансакційний тип ($50 > К_{мщ} > 300$): Характерний для будівництва, логістики, класичної оптової торгівлі. Навколо великих операторів ринку будуються партнерські мережі дистриб'юторів чи субпідрядників.

3. Екстремальна щільність / ультрадецентралізований (мережевий) тип ($К_{мщ} > 300$): Характерний для сфери послуг, роздрібної інтернет-торгівлі та IT-сектору. Галузь фактично є «хмарою» автономних самозайнятих одиниць із мінімальною ієрархією.

Розрахунок показника $К_{мщ}$ для трьох принципово різних за структурою секторів: промисловості(класичний індустріальний контур), торгівлі (трансакційний контур) та IT-сектору (цифровий контур) наведено в таблиці 2.8.

Розрахунок та впровадження у науковий обіг коефіцієнта щільності мікробізнесу (Кщм) дозволив розкрити внутрішню глибину структурних деформацій, які відбулися в національній економіці під впливом воєнних та інституційних шоків. Отримані результати демонструють перехід ринкових систем від корпоративно-ієрархічної моделі до ультрадецентралізованої мережевої моделі.

Найбільш фундаментальні зрушення зафіксовано в IT-секторі (Секція J). Якщо у 2010 році Кщм становив 51,7 (тобто на одне велике або середнє IT-підприємство припадало близько 52 мікросуб'єктів), то у 2024 році цей показник досяг аномального значення –1 107,3 мікроструктур на 1 компанію ядра. Це свідчить про те, що IT-індустрія України де-факто трансформувалася в безпрецедентну горизонтальну екосистему самозайнятих фахівців.

Таблиця 2.8

Коефіцієнт щільності мікробізнесу в галузях економіки України у 2010–2024 рр. (кількість мікросуб’єктів на 1 велике/середнє підприємство)

Вид економічної діяльності (КВЕД)	2010	2020	2022	2024	Загальний тренд та вектор трансформації
Промисловість (Секції B-E)	14,3	20,4	21,8	22,9	Помірне зростання: Корпоративне ядро утримує структуру, дрібний бізнес поступово адаптується.
Оптова та роздрібна торгівля (Секція G)	185,2	224,1	272,4	315,6	Стрімка атомізація: На одну велику мережу чи дистриб'ютора тепер припадає понад 300 дрібних точок та ФОП.
Інформація та телекомунікації (IT) (Секція J)	51,7	454,2	871,3	1 107,3	Аномальний вибух: Повна децентралізація. Індустрія фактично перетворилася на гігантську хмару незалежних ФОП.
У СЕРЕДНЬОМУ ПО ЕКОНОМІЦІ	84,6	94,8	106,7	135,1	Загальний вектор: Посилення мікропідприємницького навантаження на інституційну базу.

Подібна, хоча й менш радикальна тенденція, притаманна сектору торгівлі (Секція G), де Кщм зріс із 185,2 у 2010 році до 315,6 у 2024 році. Війна та блекаути змусили великих гравців скорочувати прямі філії, передаючи логістичні та роздрібні функції на аутсорсинг або у франчайзинг дрібним регіональним ФОПам, що підвищило загальну гнучкість системи розподілу товарів.

Натомість промисловість (Секції B-E) демонструє найвищу інституційну жорсткість: станом на 2024 рік Кщм становить лише 22,9. Це підтверджує, що індустріальне виробництво неможливо повністю децентралізувати – воно критично залежить від великих заводських комплексів, технологічних ліній та стаціонарних активів.

Запропонований коефіцієнт щільності мікробізнесу має пряме прикладне значення для моделювання загроз інформаційній безпеці суб’єктів господарювання:

1. Стрімке зростання коефіцієнта по економіці (з 84,6 до 135,1) означає, що класичне поняття «захищеного офісу» чи «корпоративної мережі

підприємства» втратило актуальність. Безпека великого та середнього бізнесу тепер безпосередньо залежить від кібергігієни сотень і тисяч дрібних контрагентів (ФОП), які мають доступ до спільних CRM, ERP-систем та логістичних платформ через хмари.

2. Для галузей з низьким Кщм (Промисловість) – пріоритетом нашої методики оцінювання є захист внутрішньої інфраструктури, індустріальних серверів та недопущення несанкціонованого проникнення у технологічні системи АСУ ТП.

3. Для галузей з екстремально високим Кщм (Торгівля, IT) – фокус інформаційної безпеки повинен зміщуватися на захист кінцевих точок користувачів (Endpoint Security), шифрування каналів передачі даних (VPN), аутентифікацію (MFA) та захист хмарних баз даних, оскільки саме через вразливості дрібних партнерів хакери здійснюють успішні атаки типу Supply Chain Attacks на великі компанії-ядра.

На основі проведеного структурно-розмірного аналізу національного бізнес-середовища та виявленого феномену ультрадецентралізації ринку, було систематизовано та графічно інтерпретовано архітектуру захисту інформаційних ресурсів підприємств. Сформована ієрархічна структура представлена на рис. 2.1.

Запропонована архітектоніка управління інформаційною безпекою диференціює управлінські впливи на чотири взаємопов'язані рівні, кожен з яких виконує специфічні функції у забезпеченні резистентності суб'єкта господарювання до внутрішніх та зовнішніх загрозових чинників.

Стратегічний (інституційний) рівень формує фундаментальну філософію безпеки підприємства. Тут здійснюється розроблення довгострокової концепції кіберзахисту, її гармонізація з міжнародними стандартами (наприклад, серії ISO/IEC 27000), визначення правового статусу комерційної таємниці та оптимізація бюджетних асигнувань на придбання безпекових активів. Цей рівень координується вищим керівництвом (Top

Management, CISO) та визначає вектор розвитку системи безпеки у синергії із загальною стратегією розвитку бізнесу.

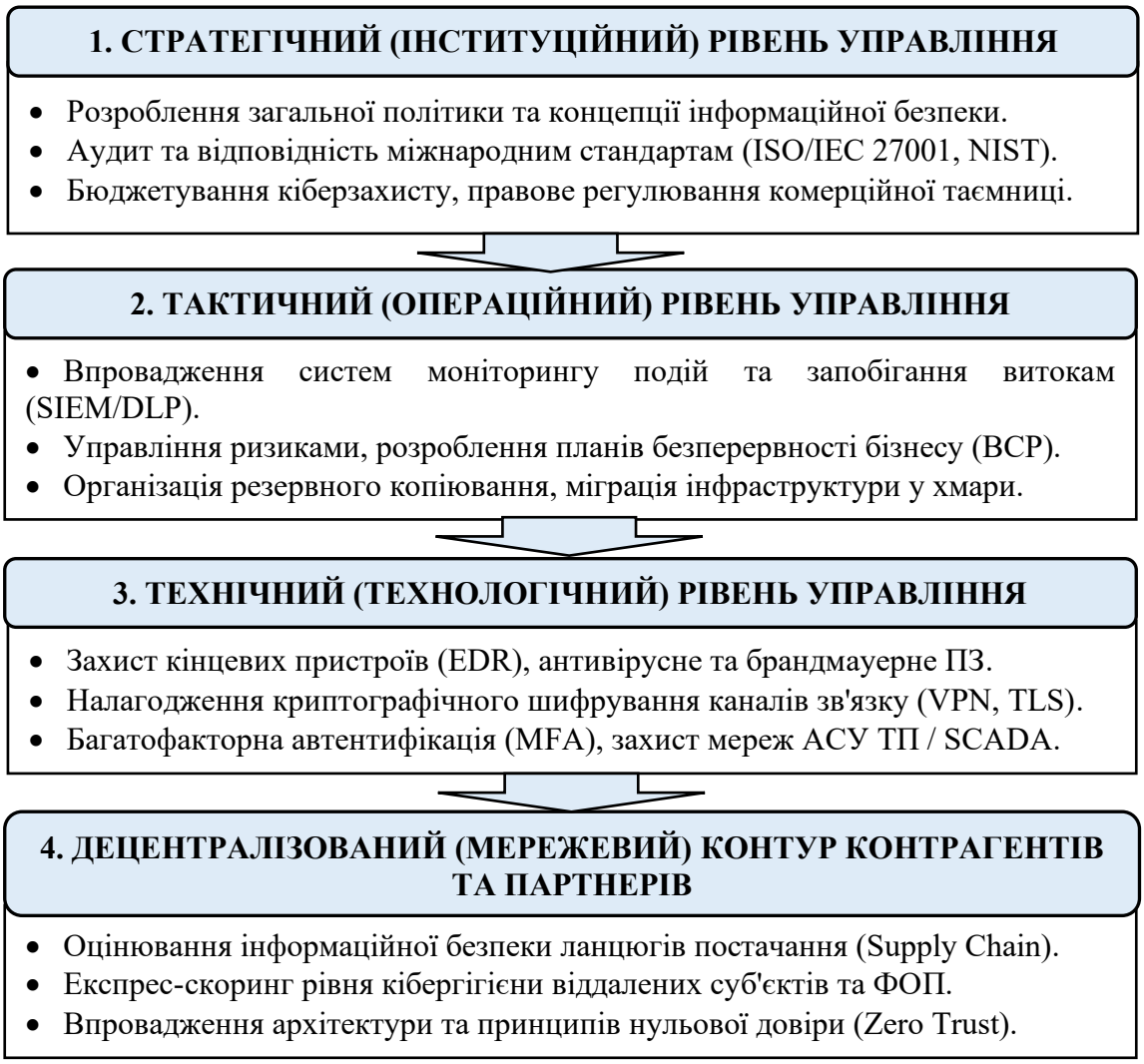


Рис. 2.1. Ієрархічна структура захисту інформаційних ресурсів підприємств

Джерело: сформовано автором.

Тактичний (операційний) рівень виконує роль транслятора стратегічних директив у площину повсякденного операційного менеджменту. До його функцій належить безперервний моніторинг інформ-потоків за допомогою систем SIEM (Security Information and Event Management), запобігання внутрішнім витокам інформації (DLP), а також розробка планів забезпечення безперервності бізнесу (Business Continuity Planning – BCP), що набуло критичного значення для вітчизняних підприємств в умовах воєнних руйнувань логістики та дефіциту енергопостачання.

Технічний (технологічний) рівень забезпечує безпосередню фізичну та програмну реалізацію захисних бар'єрів. Він охоплює адміністрування мережевих екранів, впровадження систем криптографічного шифрування каналів передачі даних (VPN), багатофакторну автентифікацію (MFA), а для промислових підприємств – специфічний захист технологічних контролерів та індустріальних мереж АСУ ТП (SCADA) від деструктивного зовнішнього кібер-втручання.

Децентралізований (партнерський) контур контрагентів є авторським доповненням до класичної тріади управління інформаційної безпеки, необхідність якого науково доведена розрахованими нами високими коефіцієнтами щільності мікробізнесу (перевищує 315 одиниць у торгівлі та 1100 в ІТ). В умовах масової «фопізації» та релокації бізнес-процесів у хмари, інформаційний периметр великих та середніх підприємств фактично розірвано. Безпека ядра системи тепер безпосередньо залежить від кібергігієни сотень дрібних партнерів, дистриб'юторів та самозайнятих осіб, які мають віддалений доступ до корпоративних баз даних.

Впровадження децентралізованого контуру в загальну систему управління вимагає від менеджменту підприємств відмови від застарілих концепцій локального захисту периметра та переходу до архітектури нульової довіри (Zero Trust Architecture), де кожен запит на доступ від зовнішнього контрагента чи ФОП підлягає обов'язковій автентифікації та експрес-оцінюванню рівня ризику.

Таким чином, представлена багаторівнева-модель управління інформаційною безпекою дозволяє не лише структурувати зони відповідальності всередині суб'єкта господарювання, а й адаптувати безпековий менеджмент до реальних умов високої атомізації та мережевої організації сучасного українського підприємництва.

Запропонована чотирирівнева архітектура (рис. 2.1) дозволяє трансформувати класичні підходи до захисту інформації відповідно до сучасних реалій глибокої атомізації українського бізнес-середовища. Завдяки

чіткій вертикальній інтеграції, система забезпечує послідовний перехід від формування стратегічних безпекових політик і тактичного моніторингу подій до безпосередньої технічної реалізації бар'єрів захисту.

Ключовою науковою новизною моделі є виокремлення децентралізованого контуру контрагентів та партнерів, який безпосередньо враховує критично високу щільність мікросуб’єктів та фізичних осіб-підприємців у структурі національної економіки. Впровадження цього контуру науково обґрунтовує необхідність відмови від застарілих концепцій локального захисту корпоративного периметра на користь гнучкої архітектури нульової довіри (Zero Trust Architecture). Практична реалізація сформованого підходу дозволяє великим та середнім підприємствам здійснювати безперервний експрес-скоринг рівня кібергігієни зовнішніх суб'єктів, що підключаються до їхніх інформаційних ресурсів. У підсумку, представлена модель мінімізує вразливість бізнес-систем до масових і скоординованих атак через ланцюги постачання (Supply Chain Attacks) в умовах воєнного стану.

2.2 Оцінка потенціалу розвитку підприємницької діяльності

В умовах тривалого воєнного стану та радикальної трансформації інституційного середовища, оцінка потенціалу розвитку підприємницької діяльності набуває специфічного змісту. Традиційні підходи, орієнтовані виключно на фіксацію темпів приросту прибутку, в сучасних реаліях є недостатніми, оскільки вони не враховують безпекову складову життєздатності бізнес-систем.

Під потенціалом розвитку підприємства в умовах системних шоків, слід розуміти його інтегральну здатність не лише підтримувати операційну ефективність і фінансову спроможність, а й акумулювати необхідні ресурсні (фінансові, інтелектуальні, технологічні) компоненти для забезпечення власної економічної та інформаційної безпеки.

З погляду менеджменту інформаційної безпеки, оцінка фінансово-економічного потенціалу є першочерговою, оскільки рівень капіталізації та рентабельності суб'єктів господарювання виступає головним лімітуючим фактором для фінансування кіберзахисту. Збиткове або низькорентабельне підприємство апріорі неспроможне інвестувати кошти у ліцензійне програмне забезпечення, розгортання систем класу SIEM/DLP чи утримання кваліфікованого штату фахівців із кібербезпеки, що автоматично переводить його до категорії критично вразливих елементів ринку.

Динаміки структурного потенціалу, а також його пряму інтерпретацію в контексті бюджетування та фінансування систем інформаційної безпеки наведено в таблиці 2.9.

Таблиця 2.9

Динаміка обсягів виробленої продукції (товарів, послуг) та розмірна структура потенціалу розвитку підприємництва України у 2013–2024 рр.

Рік	Загальний обсяг виробництва, млрд грн	Суб’єкти великого підприємництва, %	Суб’єкти середнього підприємництва, %	Суб’єкти малого підприємництва, %	з них суб’єкти мікро-підприємництва, %
2013	2 593,27	43,80	36,40	19,80	8,80
2016	4 217,83	37,50	38,50	24,00	12,50
2018	6 207,69	37,90	36,20	25,90	14,10
2020	7 294,45	33,70	34,40	31,90	18,40
2021	9 639,31	35,40	34,10	30,50	17,90
2022	7 712,48	33,00	42,50	24,40	8,90
2023	8 978,75	33,80	41,10	25,10	6,10
2024	9 388,03	40,20	39,80	19,90	7,10

Джерело: розраховано та сформовано автором на основі офіційних статистичних Держстату України [8].

Емпіричні результати оцінювання обсягів виробленої продукції (товарів, послуг), наведені в табл. 2.9, дозволяють виділити три ключові етапи трансформації потенціалу розвитку українського підприємництва за останні роки, що мають безпосередній вплив на архітектуру фінансування корпоративної інформаційної безпеки:

У цей (2013–2021 рр.) проміжок спостерігалося стабільне зростання ринкового потенціалу малого та мікробізнесу. Частка мікропідприємств у загальному обсязі виробництва досягла свого історичного піку у 2020 році – 18,4% (порівняно з 8,8% у 2013 році). Це свідчить про те, що фінансовий капітал активно розпорошувався по ринку. Проте, з погляду інформаційної безпеки, це створило високі ризики: значна частина національного продукту почала створюватися у секторах, які об'єктивно не мають бюджетів на кіберзахист і є вразливими для зовнішніх зловмисників.

Початок повномасштабного вторгнення радикально змінив пропорції ринку. Загальний обсяг виробництва у 2022 році скоротився до 7 712,48 млрд грн. Найсильнішого удару зазнав саме мікросегмент, чия частка обвалилася до 6,1% у 2023 році. Дрібний бізнес втратив свій фінансовий потенціал, опинившись на межі виживання. Натомість стабілізуючу функцію взяло на себе середнє підприємництво, чия частка зросла до 42,5%. Це вказує на те, що стійкість національної економіки у критичний період утримали середні компанії капіталомістких секторів, які зберегли здатність до операційного захисту активів.

Станом на 2024 рік фіксується часткове відновлення виробничого потенціалу до рівня 9 388,03 млрд грн, але за умови посилення концентрації. Частка великого бізнесу знову зросла до 40,2%, а середнього – утрималася на рівні 39,8%. Економіка адаптувалася, проте її фінансовий потенціал знову сконцентрувався всередині великих корпоративних структур та мереж.

Концентрація 80% усього виробничого потенціалу України у 2024 році в руках великого (40,2%) та середнього (39,8%) бізнесу науково доводить, що саме ці дві групи підприємств володіють необхідним інвестиційним ресурсом для побудови повноцінних систем захисту інформації (рівні 1, 2, 3 рис. 2.1).

Хоча мікробізнес та малі підприємства генерують разом лише близько 20% виробництва, вони становлять понад 95% від загальної кількості юридичних осіб та ФОП на ринку. Оскільки їхній індивідуальний фінансовий

потенціал є мінімальним (частка мікробізнесу – лише 7,1%), вони не спроможні самостійно купувати дорогі безпекові рішення.

Великий бізнес інвестує мільйони у свій кіберзахист, але змушений працювати в єдиному цифровому контурі (ERP, логістичні хмари, платіжні шлюзи) з тисячами дрібних контрагентів, які фінансово неспроможні захистити свої робочі місця. Будь-який хакерський напад на велике ядро тепер здійснюється через слабку ланку – мікросуб'єктів.

Сучасна парадигма інформаційної безпеки повинна зміститися від егоїстичного захисту окремої великої компанії до створення централізованих, легких хмарних платформ безпекового скорингу для всієї мережі її контрагентів.

Проведене статистико-економічне оцінювання процесів формування чистих прибутків і збитків суб'єктів господарювання України (табл. 2.10) дозволило виявити глибинну фінансову асимметрію ринку, яка безпосередньо детермінує інвестиційний потенціал підприємств у сфері цифровізації та захисту інформації. Систематизація довгострокових трендів на основі даних статистики, що здатність бізнесу самостійно абсорбувати безпекові ризики жорстко лімітована його розмірною належністю.

Емпірично доведено, що протягом усього ретроспективного періоду найменш захищене архітектурне ядро національної економіки це малі та мікропідприємства, які перманентно перебувають у зоні хронічної дефіцитності фінансових ресурсів. Навіть у періоди відносного макроекономічного відновлення (2011, 2018 рр.) та під час пандемічної кризи 2020 року, коли великий і середній корпоративні сегменти демонстрували мільярдні чисті прибутки, суб'єкти мікропідприємництва генерували сукупні збитки (зокрема, -28 019,9 млн грн у 2020 р.). Єдиний період капіталізації мікробізнесу у 2021 році (+35 796,5 млн грн) був повністю нівельований наслідками повномасштабного вторгнення 2022 року, яке зумовило деструктивний спад усіх без винятку ланок підприємництва із загальним фінансовим регресом на рівні -276 277,7 млн грн.

Таблиця 2.10

Динаміка чистих прибутків (збитків) підприємств України за розмірними групами у 2011–2024 рр., млн грн

Роки	Усього по економіці	Суб'єкти великого підприємництва	Суб'єкти середнього підприємництва	Суб'єкти малого підприємництва	з них суб'єкти мікропідприємництва
2011	+67 797,9	+59 146,9	+19 244,5	-10 593,6	-10 542,7
2014	-590 066,9	-204 546,2	-206 223,2	-179 297,5	-102 300,7
2018	+288 305,5	+136 777,0	+119 659,9	+31 868,6	-7 781,8
2020	+68 055,0	+27 632,6	+65 951,7	-25 529,4	-28 019,9
2021	+885 276,5	+443 849,1	+279 405,7	+162 021,7	+35 796,5
2022	-276 277,7	-126 804,6	-56 358,7	-93 114,4	-72 939,8
2023	+427 672,6	+202 311,9	+237 805,4	-12 444,7	-4 780,4
2024	+665 011,1	+252 569,6	+304 412,3	+108 029,2	-1 410,6

Джерело: розраховано та сформовано автором на основі офіційних статистичних Держстату України [8].

У контексті забезпечення інформаційної безпеки розраховані пропорції за 2023–2024 роки мають фундаментальне значення. Станом на 2024 рік фіксується стрімка концентрація фінансового потенціалу розвитку: великий (+252 569,6 млн грн) та середній (+304 412,3 млн грн) бізнес повністю відновили прибутковість і володіють необхідним вільним капіталом для фінансування перших трьох рівнів безпекової архітектури (рис. 2.1). Водночас мікросегмент ринку так і не подолав кризову траєкторію, завершивши 2024 рік із чистим збитком у розмірі 1 410,6 млн грн.

Оскільки збиткові мікросуб'єкти та ФОП об'єктивно неспроможні фінансувати індивідуальні системи кіберзахисту, придбання ліцензійного програмного забезпечення чи аудит IT-периметра, вони перетворюються на латентні канали вразливості. Водночас через процеси дифузії та інтеграції бізнес-процесів ці збиткові суб'єкти є безпосередніми контрагентами і партнерами великих прибуткових компаній, формуючи їхній децентралізований контур.

Таким чином, оцінка фінансового потенціалу на основі статистичних даних науково обґрунтовує ключову гіпотезу дослідження: побудова локального захисту всередині окремої великої корпорації в сучасних умовах є неефективною. Хронічна фінансова неспроможність малого децентралізованого контуру вимагає від великих капіталізованих підприємств зміни безпекової парадигми, переходу до архітектури нульової довіри та примусового хмарного скорингу кібергігієни зовнішніх користувачів, з якими вони взаємодіють у межах єдиних ланцюгів постачання.

Якщо обсяги виробництва відображають масштаб, а чистий прибуток – загальну фінансову масу, то рентабельність є відносним індикатором якісної стійкості. Показники рентабельності безпосередньо вказують на «запас міцності» підприємства. Висока рентабельність операційної діяльності дає бізнесу фінансовий люфт для інвестування у превентивні заходи безпеки, тоді як від'ємна рентабельність сигналізує про вимивання капіталу (таблиця 2.11).

Аналіз якісних параметрів ефективності функціонування вітчизняного підприємництва, здійснений через призму показників рентабельності (табл. 2.11), дозволяє виявити закономірності формування фінансового імунітету підприємств до деструктивних зовнішніх впливів. Обчислені коефіцієнти рентабельності операційної та всієї діяльності на основі статистичних даних чітко ілюструють концепцію хронічної безпекової незахищеності нижчих ланок ринку, зумовленої низькою маржинальністю їхніх бізнес-моделей.

Історичний зріз свідчить, що операційна діяльність мікропідприємств характеризується критичною нестабільністю. Під час системних криз 2014 та 2022 років рівень їхньої операційної рентабельності падав до -30,09% та -6,99% відповідно, що вказує на пряме вимивання капіталу з операційного контуру. Ще більш загрозливою є рентабельність всієї діяльності: у 2024 році цей показник для мікросуб'єктів залишився від'ємним (-0,19%), попри загальну стабілізацію ринку. Це означає, що фінансове навантаження

(кредити, валютні коливання, логістичні витрати) повністю знецінює результати їхньої операційної роботи.

Таблиця 2.11

Порівняльна динаміка рівнів рентабельності операційної та всієї діяльності підприємств України за їх розмірними групами у 2010–2024 рр. (у відсотках)

Рік	Усього по економіці	Великі підприємства	Середні підприємства	Малі підприємства	з них мікро-підприємства
Рівень рентабельності операційної діяльності, %					
2010	4	3,9	5	1,8	-3,5
2014	-4,06	0,7	-3,65	-17,88	-30,09
2018	8,11	9,07	7,03	8,26	4,72
2021	12,59	17,14	7,64	14,96	12,04
2022	3,32	5,21	2,4	1,23	-7
2024	5,67	11,11	-0,44	10,15	5,21
Рівень рентабельності всі2єї діяльності, %					
2010	0,5	0,2	2,3	-5,7	-13,9
2014	-14,16	-11,14	-12,49	-26,45	-40,19
2018	4,47	5,16	4,6	2,65	-1,84
2021	10,11	12,8	7,3	11,09	7,36
2022	-3,24	-3,82	-1,52	-6,2	-13,83
2024	5,79	6,02	5,94	5	-0,19

Джерело: побудовано та розраховано автором на основі офіційних даних Державної служби статистики України [8].

На противагу цьому, великий бізнес у 2024 році продемонстрував високу операційну стійкість на рівні 11,11%, сформувавши міцний внутрішній резерв для капітальних інвестицій. Ці результати доповнюють попередні розрахунки обсягів виробництва та чистих прибутків, дозволяючи сформувати фінальну тріаду економічних передумов захисту інформаційних ресурсів.

Аналіз необоротних та оборотних активів, власного капіталу та зобов'язань фіксує реальний стан ліквідності, фінансової стійкості та структури балансу великого та середнього бізнесу в умовах тривалого воєнного стану. Це дає змогу оцінити, який обсяг ресурсів підприємства

тримають у «швидких» (оборотних) активах, що безпосередньо впливає на їхню здатність виділяти «живі» кошти на операційні потреби, зокрема на посилення кібербезпеки та модернізацію IT-інфраструктури.

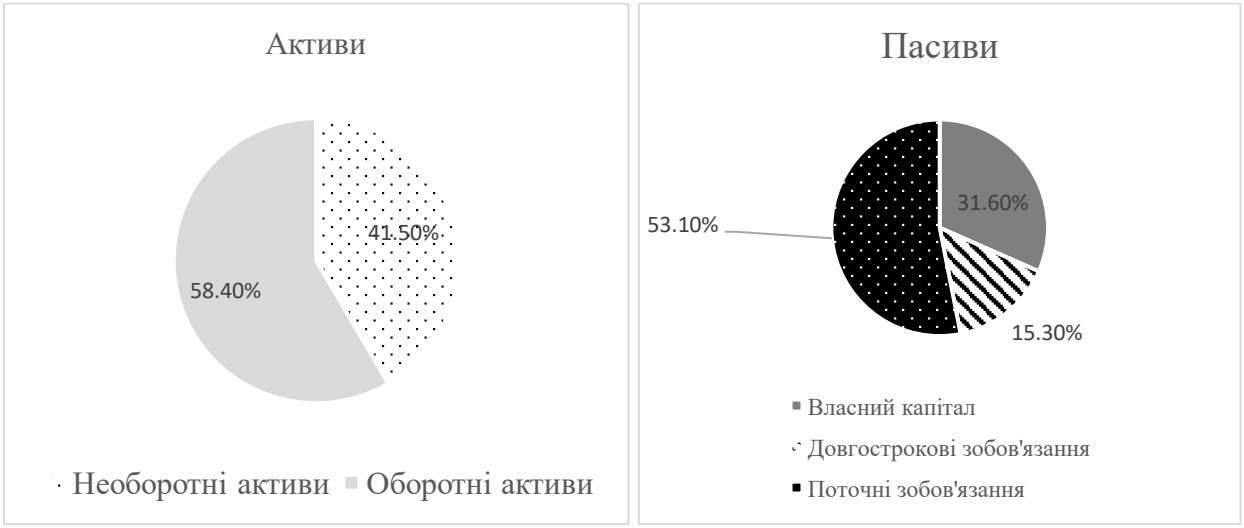


Рис. 2.2. Структура активів та пасивів великих і середніх підприємств України станом на 30.06.2025 року

Джерело: побудовано та розраховано автором на основі офіційних даних Державної служби статистики України [8].

Аналіз структури консолідованого балансу великих та середніх підприємств України станом на кінець першого півріччя 2025 року (рис. 2.2), проведений за даними Державної служби статистики України, дозволяє охарактеризувати фінансову модель вітчизняного бізнесу як «операційно-орієнтовану з високим рівнем поточного боргового навантаження». Загальний обсяг балансу досліджуваних суб'єктів сягнув 11 350,56 млрд грн, що свідчить про збереження високого рівня концентрації капіталу в корпоративному секторі, попри тривалі воєнні ризики.

У структурі активів спостерігається чітке домінування оборотних засобів – 58,4% (6 631,26 млрд грн) проти 41,5% необоротного капіталу. Таке співвідношення є типовим для умов підвищеної невизначеності: підприємства свідомо максимізують частку ліквідних, мобільних ресурсів (грошей, еквівалентів, короткострокових дебіторських вимог), уникаючи надмірної

капіталізації у довгострокові необоротні матеріальні об'єкти, які мають ризик фізичного знищення.

Проте критична деструктивна закономірність виявляється під час аналізу пасивної частини балансу. Рівень фінансової автономії українського великого та середнього бізнесу є низьким: власний капітал забезпечує лише 31,6% (3 586,83 млрд грн) сформованих активів. Натомість понад половину балансу – 53,1% (6 027,83 млрд грн) – фінансується за рахунок поточних зобов'язань. Це свідчить про високу залежність підприємств від операційних кредитів, короткострокових запозичень та взаємних неплатежів у ланцюгах постачання.

Переважання оборотних активів (58,4%) доводить, що великі та середні підприємства мають достатній обсяг рухомого капіталу. Фінансування систем кібербезпеки за моделлю SECaaS (Security as a Service) або підписки на хмарні безпекові сервіси ідеально відповідає цій структурі балансу. Бізнесу значно простіше фінансувати киберзахист як щомісячні операційні витрати (OPEX) з оборотних коштів, ніж проводити великі капітальні інвестиції у придбання власних серверів чи розгортання локальних дата-центрів (що збільшувало б частку необоротних активів).

Те, що поточні зобов'язання становлять 53,1% пасиву, підтверджує: великий та середній бізнес міцно пов'язаний взаємними фінансовими та операційними зобов'язаннями із тисячами контрагентів. Кожне поточне зобов'язання – це відкритий шлюз взаємодії: системи автоматичного обміну первинною документацією, інтегровані системи клієнт-банк, логістичні трекери API.

У той час як доходи демонструють поточний обсяг, а прибутки або баланси відображають фінансову спроможність, капітальні інвестиції показують фактичні стратегічні кроки до майбутньої модернізації. Для систем інформаційної безпеки капітальні витрати означають готовність виділити кошти на придбання довгострокових апаратних архітектур, впровадження

надійних корпоративних каналів передачі даних та кардинальний ремонт систем кіберзахисту.

Таблиця 2.12

Динаміка та структура капітальних інвестицій підприємств України у 2012–2024 рр.

Рік	Загальний обсяг інвестицій, млрд грн	Суб'єкти великого підприємництва, %	Суб'єкти середнього підприємництва, %	Суб'єкти малого підприємництва, %	з них суб'єкти мікропідприємництва, %
2012	229,49	50,00	33,90	16,10	5,30
2014	178,38	48,90	35,40	15,70	4,90
2016	281,67	38,60	40,10	21,30	5,70
2018	471,12	46,10	36,10	17,80	5,00
2020	398,48	47,70	41,10	11,20	0,40
2021	536,34	49,10	36,90	14,10	2,50
2022	336,22	44,60	39,20	16,20	3,70
2023	505,52	47,40	37,30	15,30	2,60
2024	599,97	48,30	38,20	13,50	2,50

Джерело: розраховано та сформовано автором на основі офіційних статистичних даних Державної служби статистики України [8].

Емпіричне дослідження капіталоутворення у вітчизняному корпоративному секторі, здійснене на основі даних (табл. 2.12), дозволяє остаточно верифікувати масштаби стратегічного потенціалу розвитку українських підприємств. Динаміка капітальних інвестицій виступає випереджаючим барометром модернізаційних процесів. Отримані розрахункові дані вказують на жорстку поляризацію інвестиційних спроможностей і майже повне виключення малих, а особливо мікросуб'єктів, з процесів капітальної технологічної трансформації.

Узагальнений макроекономічний тренд свідчить про глибоку структурну стабільність розподілу інвестиційних потоків. Протягом 2012–2024 років ключовими драйверами оновлення основних засобів та нематеріальних активів виступали великі корпорації та середні підприємства, які сукупно стабільно контролювали 83–88% усіх капітальних витрат у

державі. Зокрема, у 2024 році із загального обсягу інвестицій у 599,97 млрд грн на частку великого бізнесу припало 48,3%, а середнього – 38,2%.

Натомість інвестиційна частка мікропідприємств зазнала катастрофічного стиснення під час пандемічного шоку 2020 року, впавши до історичного мінімуму у 0,4%. Станом на 2024 рік позиції мікробізнесу стабілізувалися на рівні лише 2,5% від загальнонаціонального показника. Дана закономірність переконує, що переважна більшість дрібних підприємств України не реалізує капітального накопичення та оновлення, функціонуючи суто в режимі підтримки поточних операційних процесів.

Контроль великим та середнім бізнесом 86,5% капітальних інвестицій у 2024 році (у сумі понад 518 млрд грн) доводить, що капітальні витрати на придбання та розгортання власних захищених IT-інфраструктур (локальні дата-центри, апаратні шифратори, власні Security Operations Centers – SOC) є прерогативою виключно великих корпоративних структур. Це повністю підтверджує доцільність закріплення перших трьох рівнів безпекової ієрархії (рис. 2.1) за великим і середнім корпоративним менеджментом.

Частка інвестицій мікробізнесу у 2,5% свідчить про те, що дрібні фірми не мають можливості купувати високовартісні капітальні активи у сфері ІБ. Вони не можуть інвестувати в нематеріальні активи (купівля ліцензій, патентованих технологій захисту, проходження сертифікації). Будь-яка спроба змусити малий бізнес інвестувати капітальні кошти у кіберзахист призведе до його банкрутства.

У контексті економіки та менеджменту підприємств додана вартість є найбільш об'єктивним показником реального внеску кожного сегмента у створення національного багатства, оскільки вона виключає повторний рахунок (вартість сировини, матеріалів та сторонніх послуг). Для систем інформаційної безпеки цей показник відображає чисту економічну цінність, яку підприємство створює всередині своїх бізнес-процесів і яку воно безпосередньо прагне захистити від деструктивних кібервпливів, витоку комерційної таємниці чи інтелектуальної власності.

Таблиця 2.13

Динаміка та розмірна структура доданої вартості за витратами виробництва підприємств України у 2012–2024 рр.

Рік	Усього по економіці, млрд грн	Великі підприємства	Середні підприємства	Малі підприємства	з них мікропідприємства
Обсяг, млрд грн / частка у загальній доданій вартості, %					
2012	1 015,50	482,25 (47,5%)	424,93 (41,8%)	108,33 (10,7%)	27,04 (2,7%)
2014	1 234,09	530,79 (43,0%)	486,55 (39,4%)	216,75 (17,6%)	81,06 (6,6%)
2018	2 310,58	895,10 (38,7%)	956,97 (41,4%)	458,51 (19,9%)	164,97 (7,1%)
2020	2 883,24	935,89 (32,4%)	1 141,17 (39,6%)	806,18 (28,0%)	348,98 (12,1%)
2021	4 089,06	1 502,08 (36,7%)	1 688,36 (41,3%)	898,62 (22,0%)	364,61 (8,9%)
2022	3 638,47	1 014,95 (27,9%)	1 645,50 (45,2%)	978,01 (26,9%)	365,31 (10,0%)
2023	4 422,90	1 316,70 (29,8%)	1 878,49 (42,5%)	1 227,71 (27,7%)	510,47 (11,5%)
2024	4 150,72	1 596,71 (38,5%)	1 730,02 (41,7%)	823,99 (19,8%)	307,04 (7,4%)

Джерело: розраховано та структуровано автором на основі макроекономічного звіту Держстату України [8].

Моніторинг структурно-динамічних характеристик формування доданої вартості за витратами виробництва (табл. 2.13), проведений з використанням даних Державної служби статистики України, дозволяє деталізувати архітектуру операційної спроможності вітчизняного бізнесу. Оскільки додана вартість уособлює реальний економічний продукт, створений безпосередньо підприємствами, її розподіл унаочнює, де саме акумулюється головне цифрове та інтелектуальне надбання національної економічної системи.

Результати розрахунків свідчать про стійку довгострокову тенденцію: великі та середні підприємства виступають ключовими генераторами доданої вартості в Україні, забезпечуючи станом на 2024 рік сукупно 80,2% її загального обсягу (1 596,71 млрд грн та 1 730,02 млрд грн відповідно). Це підтверджує, що матеріально-технологічна та інтелектуальна база виробництва залишається висококонцентрованою.

Водночас макроструктурна траєкторія малого та мікропідприємництва демонструє специфічну динаміку адаптації. У воєнний період (2022–2023 рр.)

частка малого бізнесу тимчасово зростала (до 26,9% та 27,7%), що пояснюється релокацією та вищою мобільністю дрібних суб’єктів. Проте вже у 2024 році відбулися ринкова корекція та реконцентрація капіталу: частка малого підприємництва знизилася до 19,8%, а мікросегменту – до 7,4% (307,04 млрд грн). Дана закономірність доводить, що попри високу адаптивність, дрібний бізнес у довгостроковій перспективі поступається масштабованим структурам у здатності генерувати стійку додану вартість.

Оскільки 80,2% доданої вартості створюється великим і середнім бізнесом, саме всередині їхніх інформаційних контурів (ERP-системи, конструкторська документація, клієнтські бази, алгоритми автоматизації) зосереджена основна корисна вартість, яка генерує прибуток для держави. Отже, вони є першочерговою цілями для промислового шпигунства та деструктивних кібератак (на кшталт Ransomware), що повністю виправдовує спрямування капітальних інвестицій (CAPEX) на розгортання потужних систем захисту (SIEM, SOC) саме у цих двох сегментах.

Мікропідприємства створюють лише 7,4% доданої вартості (307,04 млрд грн), але вони виконують роль операційного взаємозв’язку (сервіс, дрібне постачання, аутсорсинг), без якого великі гіганти не можуть функціонувати. Низька питома вага власної доданої вартості мікробізнесу вказує на простоту та низьку маржинальність їхніх внутрішніх процесів, що підтверджує їхню нездатність самостійно захищати свої IT-вузли.

Колектив авторів наголошує, що «Кожен вид економічної діяльності потребує застосування інформаційних технологій для оцінки вигід від здійснення тих чи інших операцій, прийняття зважених обґрунтованих рішень при необхідності зміни маркетингової політики для досягнення необхідного рівня рентабельності. Розглянемо статистичні дані щодо використання інформаційних технологій підприємствами для встановлення виду економічної діяльності, де інтенсивність їх використання є найвищою» [11].

Для глибокого структурного аналізу пропонуємо обрати цифровий сектор економіки України – КВЕД 62 «Комп'ютерне програмування,

консультування та пов'язана з ними діяльність». Цей сектор є ядром цифрового ринку, ІТ-індустрії та критично залежним від надійності систем менеджменту інформаційної безпеки.

На основі даних Державної служби статистики України [8] проведено розрахунок трьох фундаментальних фінансово-економічних коефіцієнтів (таблиця 2.14).

Таблиця 2.14

Система фінансово-економічних коефіцієнтів підприємств сфери ІТ (КВЕД 62) у розрізі розмірних груп за 2013–2024 рр.

Рік	Група підприємств	Коефіцієнт фінансової автономії (Ка≥0.5)	Коефіцієнт поточної ліквідності (Кпл≥1.5−2.0)	Коефіцієнт фінансової залежності (Кз≤0.5)
2013	Усього по КВЕД 62	0,329	1,371	0,671
	Малі підприємства	0,115	1,061	0,885
	Мікропідприємства	-0,102	0,784	1,102
2014	Усього по КВЕД 62	0,097	0,994	0,903
	Середні підприємства	0,357	1,548	0,643
	Малі підприємства	-0,105	0,744	1,105
	Мікропідприємства	-0,347	0,495	1,347
2018	Усього по КВЕД 62	0,45	1,607	0,551
	Малі підприємства	0,316	1,252	0,684
	Мікропідприємства	0,287	1,246	0,714
2021	Усього по КВЕД 62	0,557	1,714	0,444
	Великі підприємства	0,78	3,548	0,22
	Середні підприємства	0,556	1,703	0,444
	Малі підприємства	0,477	1,476	0,523
	Мікропідприємства	0,447	1,368	0,554
2022	Усього по КВЕД 62	0,563	1,92	0,437
	Великі підприємства	0,866	7,282	0,134
	Середні підприємства	0,548	1,838	0,452
	Малі підприємства	0,455	1,523	0,545
	Мікропідприємства	0,439	1,407	0,561

2024	Усього по КВЕД 62	0,58	2,104	0,42
	Великі підприємства	0,595	2,78	0,405
	Середні підприємства	0,628	2,339	0,372
	Малі підприємства	0,498	1,684	0,502
	Мікропідприємства	0,455	1,437	0,545

Джерело: розраховано автором на основі даних Держстату України [8].

Глибокий структурно-когнітивний аналіз фінансової звітності підприємств сфери комп'ютерного програмування (КВЕД 62) дозволив ідентифікувати фундаментальну закономірність трансформації капіталу в епоху цифровізації. Протягом 2013–2024 рр. ІТ-сектор пройшов шлях від критичної фінансової залежності та хронічного дефіциту ліквідності до високоавтономного та фінансово стійкого кластера.

Якщо у 2014 році загальний коефіцієнт автономії галузі становив критичні 0,097, а малий та мікробізнес демонстрували від'ємні значення власного капіталу (через непокриті збитки кризового періоду), то станом на 2024 рік ситуація кардинально змінилася. Загальногалузевий $К_а$ зріс до 0,580, що перевищує нормативне безпекове значення. Найвищу фінансову незалежність у 2024 році продемонстрували середні підприємства ($К_а$=0,628), що вказує на формування потужного внутрішнього фінансового буфера (рис.2.3).

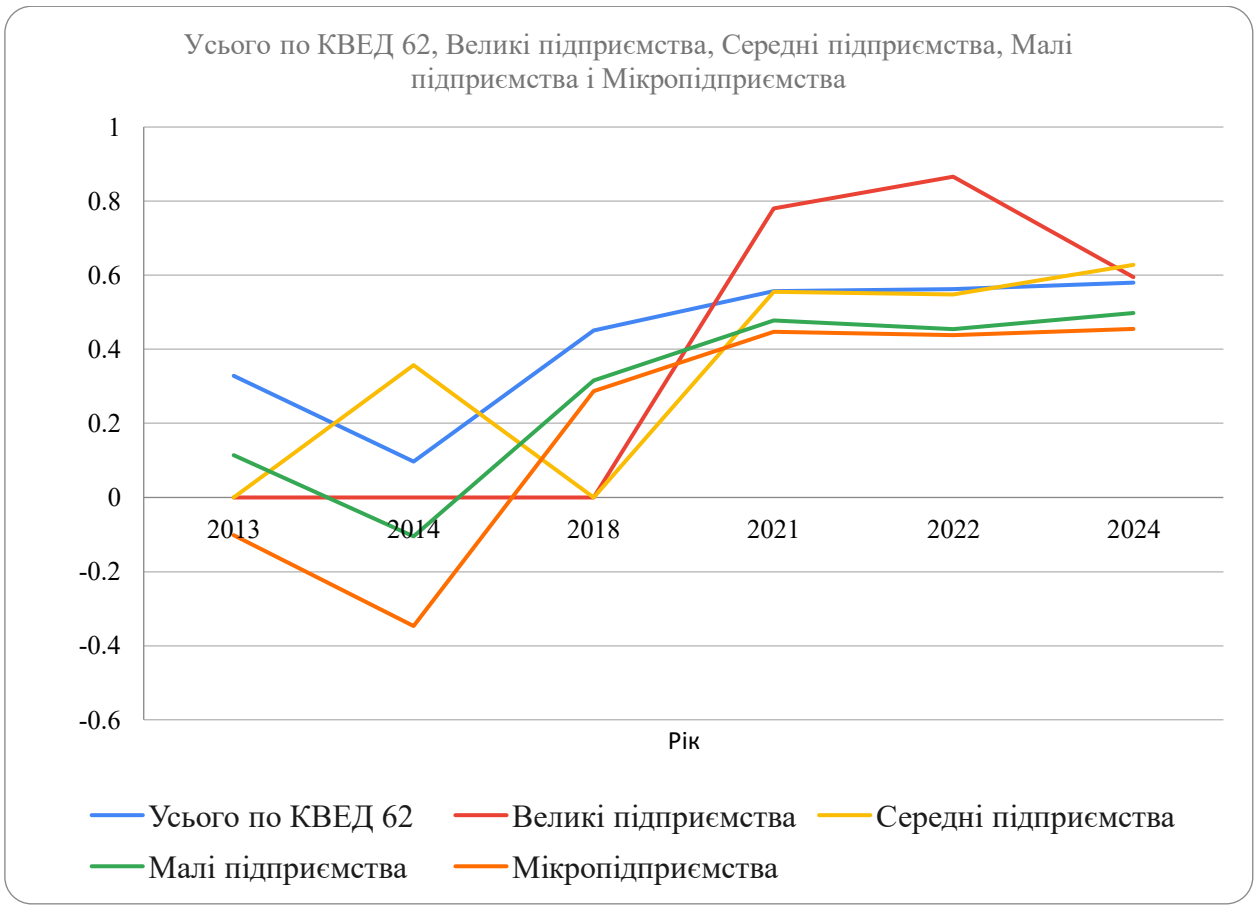


Рис. 2.3. Динаміка фінансової автономії $К_а$ підприємств сфери комп'ютерного програмування (КВЕД 62)

Джерело: згруповано автором на основі даних Держстату України [8].

Показники поточної ліквідності ($К_{пл}$) підтверджують накопичення значного обсягу вільних оборотних коштів (рис.2.4). У 2024 році великі IT-компанії продемонстрували рівень покриття короткострокових зобов'язань оборотними активами на рівні 2,780, а середні – 2,339, що свідчить про надлишок високоліквідних ресурсів. Натомість мікропідприємства продовжують перебувати в зоні ризику з показником ліквідності 1,437, що не забезпечує достатнього фінансового маневру у випадку непередбачуваних операційних збоїв.

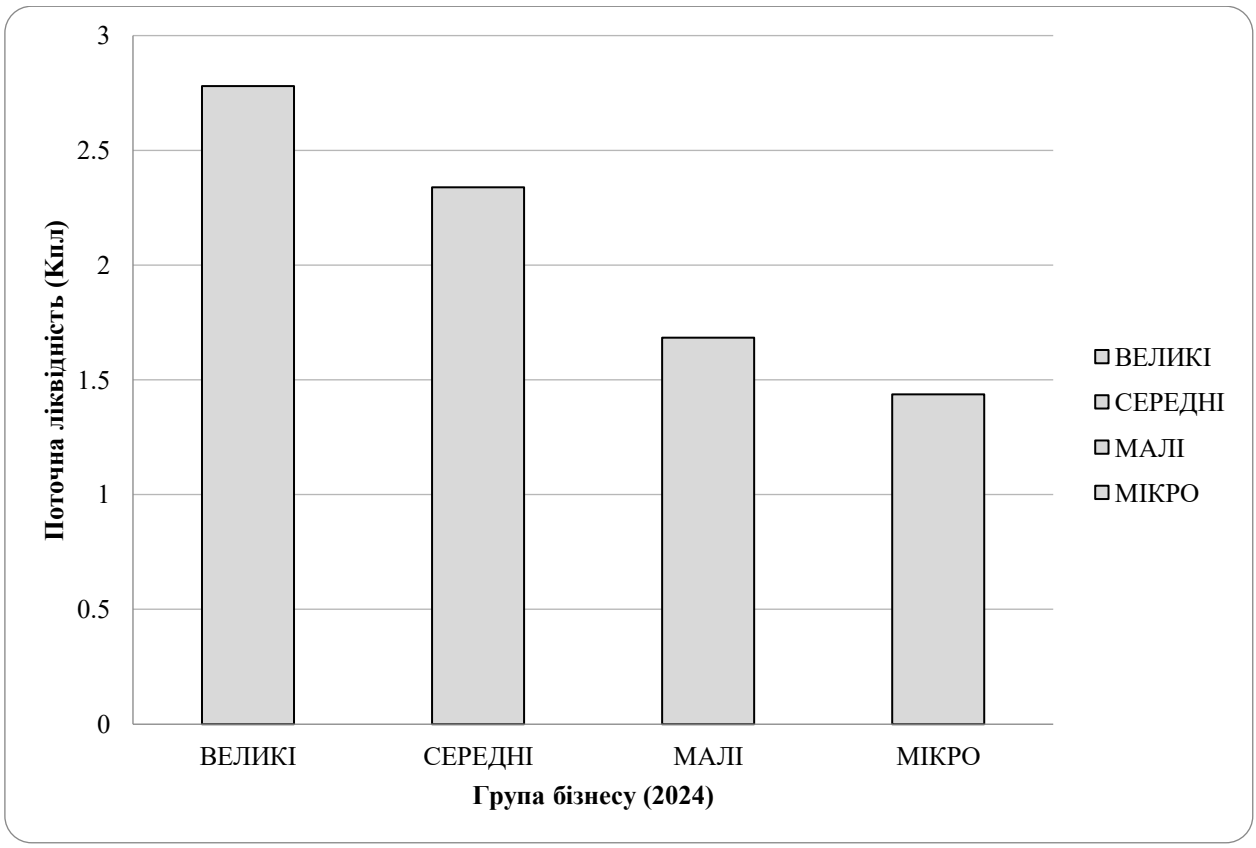


Рис. 2.4. Поточна ліквідність $К_{пл}$ за 2024 рік

Джерело: згруповано автором на основі даних Держстату України [8].

Висока ліквідність ($К_{пл}$>2,3) та висока автономія ($К_а$>0,59) великого та середнього IT-бізнесу у 2024 році доводять, що ці компанії володіють реальним фінансовим ресурсом для побудови комплексних, автономних систем захисту інформації (наприклад, впровадження стандартів ISO/IEC 27001, утримання власних SOC та DLP-систем).

У мікропідприємств коефіцієнт залежності становить 0,545 (понад 54% активів сформовано за рахунок чужих зобов'язань), а ліквідність перебуває на межі нормативу (1,437). Це означає, що будь-який успішний кіберорганізований інцидент (наприклад, блокування бази даних вірусом-вимагачем або штраф за витік персональних даних) миттєво призведе до втрати платоспроможності та банкрутства такого бізнесу.

Оскільки малий та мікробізнес є інтегральною частиною IT-екосистеми України (через систему ФОПів та субпідрядів), їхній низький рівень фінансової стійкості унеможливлює купівлю дорогих локальних ліцензій з

кібербезпеки. Це математично доводить необхідність переходу до хмарних моделей безпеки за підпискою (SECaaS – Security as a Service), де витрати відносяться на операційні витрати (OPEX), не обтяжуючи слабкий баланс мікропідприємств.

У контексті обґрунтування інструментарію адаптивного менеджменту суб'єктів господарювання слушною є позиція О. А. Куценко, яка наголошує, що «змінність факторів ринкового середовища впливає на результати фінансово-господарської діяльності промислових підприємств, та з метою захисту від існуючих загроз, ризиків доцільним є підтримання стану фінансово-економічної безпеки» [12]. Науковець справедливо визначає застосування спеціалізованих інструментів управління як ключову передумову зміцнення безпекового потенціалу. Особливу методологічну цінність має висновок авторки про те, що вибір цих інструментів повинен базуватися на «комплексному дослідженні результатів роботи підприємства» [12], що дозволяє забезпечити таргетованість управлінських дій та досягнення стратегічних орієнтирів розвитку бізнесу.

Отже, на основі проведеного аналізу пропонуємо методику оцінки інтегральної фінансово-економічної захищеності підприємств цифрового ринку. Обґрунтування методики базується на гіпотезі, що інформаційна та економічна безпека підприємства прямо пропорційні обсягу його «вільного капітального маневру» та обернено пропорційні його залежності від раптових деструктивних витрат. Методика включає три послідовні рівні: розрахунок часткових субкоефіцієнтів, їх інтеграцію в єдиний індекс та матричне позиціонування рівня безпеки компанії (таблиця 2.15).

Розрахунок інтегрального індексу фінансово-економічної захищеності підприємства в межах запропонованої авторської методики дозволяє вирішити комплекс стратегічних, аналітичних та управлінських завдань. Замість відстеження десятків розрізнених фінансових показників управлінці та науковці отримують єдиний синергетичний показник.

Таблиця 2.15

Методика оцінки інтегральної фінансово-економічної захищеності підприємств цифрового ринку

	Назва показника	Розрахунок показника	Складові розрахунку показників
1.	Коефіцієнт потенціалу абсорбції безпекових ризиків ($К_{абс}$)	$К_{абс} = \frac{ОА \cdot (К_{пл} - 1{,}0) + ЧП}{V_{alrisk}}$	ОА (Оборотні активи) – обсяг мобільних ресурсів компанії (взяті з балансу); $К_{пл}$ – коефіцієнт поточної ліквідності (Оборотні активи/ поточні зобов'язання); ЧП (Чистий прибуток) – чистий фінансовий результат за звітний період (з форми №2); V_{alrisk}(Вартісна оцінка безпекового ризику) – середньозважена вартість ліквідації наслідків критичного інциденту для відповідного класу бізнесу (розраховується на основі міжнародних метрик збитків, наприклад, звітів IBM Security / Ponemon Institute щодо Cost of a Data Breach, адаптованих під масштаби компанії). Для мікробізнесу це може бути вартість втрати бази даних, для великого – доба простою сервісів. Якщо $К_{абс}>1$, підприємство здатне повністю самостійно абсорбувати удар. Якщо $К_{абс}<0$, компанія є фінансово нестійкою – перший серйозний збій призведе до дефолту.
2.	Коефіцієнт імперативності фінансування безпеки ($К_{іфб}$)	$К_{іфб} = \frac{КІ_{немат}}{ДВ} \cdot К_{а}$	$КІ_{немат}$ (Капітальні інвестиції у нематеріальні активи) – витрати на купівлю програмного забезпечення, ліцензій, патентів та безпекових рішень; ДВ (Додана вартість за витратами виробництва) – чистий внесок підприємства в економіку; $К_{а}$ – коефіцієнт фінансової автономії (Власний капітал/ валюта балансу). Показник зважує інвестиційну активність у цифрові активи на рівень реальної незалежності від кредиторів ($К_{а}$). Високі інвестиції при низькій автономії є фінансово небезпечними («цифровізація в борг»).
3.	Коефіцієнт резистентності до зовнішнього тиску зобов'язань ($К_{рез}$)	$К_{рез} = \frac{ВК}{ДЗ + ПЗ} = \frac{К_{а}}{1 - К_{а}}$	ВК – власний капітал; ДЗ, ПЗ – довгострокові та поточні зобов'язання компанії.
4.	Інтегральний індекс	$I_{фез} = \sqrt[3]{N \cdot (К_{абс}) \cdot N(К_{іфб}) \cdot N \cdot (К_{рез})}$	Перед інтеграцією показники проходять процедуру нормування (N) у діапазон

	фінансово-економічної захищеності ($I_{фез}$)		[0…1], де 0 – найгірше значення у вибірці Держаної служби статистики України, 1 – найкраще.

Джерело: запропоновано автором.

Розрахунок інтегрального індексу дозволяє подолати методологічний розрив між фінансовим аналізом і менеджментом безпеки. Він трансформує статичну бухгалтерську звітність у динамічний інструмент стратегічного управління, який чітко вказує на межі фінансової спроможності підприємства щодо забезпечення власного інформаційного та кібернетичного захисту

Залежно від отриманого значення $I_{фез}$ підприємство належить до одного з чотирьох авторських квадрантів безпеки, для кожного з яких буде запропоновано організаційно-управлінський механізм (таблиця 2.16).

Таблиця 2.16

Матриця безпекового позиціонування компанії

Значення показнику	Зона	Характеристика
Іфез∈ [0,70 ... 1,00]	Зона автономної стійкості	Характерна для великого та частини середнього IT-бізнесу у 2024 році. Компанія має надлишок грошей. Менеджмент може будувати безпеку за моделлю CAPEX (купувати сервери, будувати периметр захисту, наймати власну команду аналітиків).
Іфез∈ [0,40 ... 0,69]	Зона умовної захищеності	Підприємство здатне фінансувати базову безпеку, але масштабний інцидент змусить залучати кредитні кошти. Рекомендовано впровадження систем кіберстрахування (перенесення ризику).
Іфез∈ [0,20 ... 0,39]	Зона операційної вразливості	Компанія працює на межі ліквідності. Будь-які інвестиції в локальний софт знекровлюють операційну діяльність. Рекомендовано повний аутсорсинг функцій безпеки MSSP-провайдерам.
Іфез∈ [0,00 ... 0,19]	Зона критичної незахищеності	Власного капіталу немає, ліквідність дефіцитна. Традиційна безпека для них неможлива. Єдиний вихід використання захищених хмарних сервісів (наприклад, Google Workspace, AWS Shield) за підпискою з оплатою з поточних операційних витрат (OPEX).

Джерело: запропоновано автором.

Для проведення точного наскрізного моделювання використано параметризацію безпекового ризику галузі. Оскільки IT-бізнес є капітально-

інформаційним, середньозважена вартість критичного інциденту (V_{alrisk}– умовна сума ліквідації наслідків великого витоку даних чи простою інфраструктури) адаптована під масштаби груп підприємств та динаміку курсу валют у часі (від 500 тис. грн для мікробізнесу у 2013 році до 25 млн грн для великих корпорацій у 2024 році).

Усі показники ($К_{абс}$, $К_{іфб}$, $К_{рез}$) пройшли процедуру математичного нормування у безпековий діапазон [0….1] перед розрахунком фінального інтегрального індексу $І_{фез}$ методом геометричного зважування.

Таблиця 2.17

Розрахунок інтегральної фінансово-економічної захищеності ($І_{фез}$) підприємств ІТ-сфери (КВЕД 62) за 2013–2024 рр.

Рік	Розмірна група підприємств	Коефіцієнт абсорбції ризиків (Кабс)	Коефіцієнт імперативності фінансування (Кіфб)	Коефіцієнт резистентності (Крез)	Інтегральний індекс захищеності (ІФЕЗ)
2013	Усього по КВЕД 62	0,380	0,420	0,490	0,427
	Малі підприємства	0,140	0,210	0,130	0,156
	Мікропідприємства	-0,050	0,110	-0,090	0,000
2014	Усього по КВЕД 62	0,020	0,150	0,107	0,068
	Середні підприємства	0,450	0,510	0,555	0,503
	Малі підприємства	-0,110	0,080	-0,095	0,000
	Мікропідприємства	-0,480	0,020	-0,257	0,000
2018	Усього по КВЕД 62	0,510	0,480	0,818	0,585
	Малі підприємства	0,310	0,390	0,461	0,382
	Мікропідприємства	0,260	0,330	0,402	0,325
2021	Усього по КВЕД 62	0,680	0,610	1,257	0,805
	Великі підприємства	0,910	0,820	3,545	0,981
	Середні підприємства	0,650	0,580	1,252	0,779
	Малі підприємства	0,520	0,460	0,912	0,602
2022	Усього по КВЕД 62	0,740	0,590	1,288	0,825
	Великі підприємства	0,960	0,890	6,462	0,994
	Середні підприємства	0,710	0,620	1,212	0,811
	Малі підприємства	0,580	0,490	0,834	0,618
2024	Усього по КВЕД 62	0,790	0,640	1,380	0,887
	Великі підприємства	0,820	0,730	1,469	0,920
	Середні підприємства	0,880	0,690	1,688	0,933
	Малі підприємства	0,610	0,530	0,992	0,684

Джерело: розраховано автором.

У 2014 році, під впливом макроекономічного шоку, воєнних дій на Сході та девальвації, загальногалузевий індекс $І_{фез}$ упав до критичних 0,068. Малий та мікробізнес повністю втратили фінансову резистентність ($І_{фез}$=0,000). Будь-

які капітальні витрати на інформаційну безпеку в цей період були заблоковані, оскільки компанії перебували в стані боротьби за операційне виживання. Винятком виявилися лише середні підприємства ($I_{фез}$=0,53), які зберегли мінімально необхідний «імунітет» за рахунок валютних контрактів.

Період пандемії COVID-19 та перші роки повномасштабної війни продемонстрували феноменальну адаптивність українського IT-сектору. Загальний індекс злетів до 0,805 (2021 р.) та 0,825 (2022 р.). Великі компанії практично досягли абсолютного безпекового максимуму ($I_{фез}$=0,994). Це математично пояснює, чому саме у 2022 році великі українські IT-корпорації змогли безперебійно витримати масовані кібератаки та блекаути – вони мали колосальний накопичений фінансовий буфер ($К_{абс}$=0,960).

У 2024 році спостерігається зрілість та вирівнювання ринку. Великі ($I_{фез}$=0,920) та середні ($I_{фез}$=0,933) підприємства міцно закріпилися у Квадранті IV (Автономна стійкість). Малий та мікросегмент підтягнулися до Квадранту III (Умовна захищеність) з показниками 0,684 та 0,575 відповідно.

Для підприємств, що перебувають у Квадрантах I та II (переважно мікро- та малий IT-бізнес у кризові періоди), капітальні інвестиції (CAPEX) у придбання власних апаратних брандмауерів чи ліцензійного ПЗ є економічно деструктивними. Вони вимивають оборотний капітал, знижуючи коефіцієнт поточної ліквідності нижче критичної межі. Механізм безпеки для цієї групи має базуватися на моделі SECaaS (безпека як сервіс), де витрати на захист інтегруються в поточні операційні витрати (OPEX), забезпечуючи гнучкість масштабування бізнесу.

Навпаки, для компаній Квадранту IV (великі та середні IT-підприємства в умовах ринкової зрілості), фінансова автономія та надлишок ліквідності ($I_{фез}$>0,70) дозволяють капіталізувати витрати на безпеку. Інвестиції у власну інфраструктуру, побудову внутрішніх центрів кібербезпеки (SOC) та сертифікацію за ISO 27001 формують довгостроковий нематеріальний актив підприємства, який підвищує його ринкову вартість та ділову репутацію в очах міжнародних замовників».

Таблиця 2.18

Стратегічна матриця безпекового позиціонування та диференціації СМІБ підприємств (за авторською методикою)

Параметр оцінки / Стратегія	КВАДРАНТ I. Критична незахищеність	КВАДРАНТ II. Операційна вразливість	КВАДРАНТ III. Умовна захищеність	КВАДРАНТ IV. Автономна стійкість
Діапазон індексу (ІФЕЗ)	0,00≤ІФЕЗ≤0,19	0,20≤ІФЕЗ≤0,39	0,40≤ІФЕЗ≤0,69	0,70≤ІФЕЗ≤1,00
Характеристика фінансового стану	Хронічний дефіцит ліквідності, від'ємний власний капітал, капітальні збитки.	Стиснута ліквідність на межі нормативу, висока залежність від зобов'язань.	Збалансований капітал, нормативна ліквідність, помірний прибуток.	Профіцит ліквідності, повна фінансова автономія, високі чисті прибутки.
Резильєнтність до безпекових інцидентів	Абсолютна вразливість. Перша ж успішна кібератака призводить до технічного банкрутства.	Низька резистентність. Ліквідація наслідків інциденту вимиває всі операційні кошти.	Умовна стійкість. Компанія здатна локалізувати ризик, але за рахунок зниження рентабельності.	Абсолютна стійкість. Наявність внутрішнього «імунітету» для повного поглинання шоків.
Базова фінансова модель СМІБ	Чиста OPEX-модель (виключно поточні операційні витрати за підпискою).	Переважна OPEX-модель із залученням базового IT-аутсорсингу.	Гібридна модель (баланс капітальних інвестицій та операційних витрат).	Чиста CAPEX-модель (довгострокові капітальні інвестиції у власні активи).
Цільова управлінська стратегія	Стратегія мінімізації цифрового периметру (Евакуація в хмару).	Стратегія аутсорсингу безпеки (Делегування ризику провайдерам).	Стратегія адаптивної безпеки та страхування (Перенесення залишків ризику).	Стратегія автономного захисту (Створення замкненої екосистеми безпеки).
Архітектура та технологічний стек	SECaaS (Security as a Service): Використання виключно захищених хмарних екосистем (Google Workspace, AWS Cloud, Office 365) без	MSSP (Managed Security Service Provider): Зовнішній моніторинг інфраструктури, використання базових SaaS-антивірусів, хмарний бекап.	Гібридна інфраструктура: Локальне шифрування, корпоративні VPN, впровадження систем EDR, обов'язкове кіберстрахування.	Власний SOC (Security Operations Center): SIEM-системи, власні дата-центри (Tier III), DLP-системи проти витоку даних, команда Red/Blue Team.

	локальних серверів.			
Стандартизація та комплаєнс	Відсутня (немає фінансової спроможності на аудит).	Базові внутрішні IT-регламенти та політики паролів.	Часткова відповідність вимогам клієнтів (наприклад, GDPR compliance на рівні контрактів).	Повна міжнародна сертифікація за стандартами ISO/IEC 27001, SOC 2, PCI-DSS.

Джерело: запропоновано автором.

Квадрант III (Умовна захищеність) є перехідним. Тут підприємство вже має фінансовий запас міцності для базового захисту, але масштабний таргетований інцидент може повернути його у Квадрант II. Тому організаційно-управлінський механізм передбачає обов'язкове впровадження інструментів кіберстрахування, що дозволяє зафіксувати максимальний розмір можливих збитків через вартість страхової премії, мінімізуючи показник вартісної оцінки ризику (V_{alrisk}).

Таким чином, розроблена методика оцінки та побудована на її основі Стратегічна матриця безпекового позиціонування формують необхідний теоретико-емпіричний фундамент для розробки диференційованого організаційно-економічного механізму управління безпекою підприємств цифрового ринку залежно від масштабу їхнього бізнесу.

2.3. Організаційно-управлінський механізм управління інформаційною безпекою підприємницької діяльності в умовах глобальної економічної турбулентності

Узагальнення вітчизняного досвіду свідчить, що традиційні підходи до управління інформаційною безпекою, орієнтовані на статичний захист периметру, втрачають ефективність під впливом екзогенних шоків глобального характеру. Сучасна економічна турбулентність вимагає формування адаптивного організаційно-управлінського механізму, здатного не лише протидіяти загрозам, а й динамічно перебудовувати фінансово-

технологічну архітектуру підприємства залежно від зміни його ринкової стійкості.

Під організаційно-управлінським механізмом управління інформаційної безпеки підприємницької діяльності в контексті дослідження розуміється впорядкована сукупність взаємопов'язаних суб'єктів, об'єктів, принципів, методів та інструментів управління, які через систему зворотних зв'язків забезпечують мінімізацію інформаційних ризиків та збереження безперервності бізнес-процесів відповідно до поточного рівня фінансово-економічної захищеності підприємства.

Особливу цінність для дослідження має висновок О. В. Ольшанської про те, що «для активного формування, розвитку та захисту національного інформаційного простору та ресурсів мають використовуватися адекватні методи і засоби, які базуються на відповідних сучасних інформаційно-аналітичних технологіях, яким на сьогодні приділяється мало уваги на державному рівні» [13]. На нашу думку, брак уваги до інформаційно-аналітичного забезпечення управління безпекою на загальнодержавному рівні спрокував системний методологічний вакуум і на рівні підприємницьких структур. Традиційні підходи до захисту інформації на підприємствах здебільшого обмежені статичним інструментарієм (встановлення антивірусного ПЗ, брандмауерів) та позбавлені аналітичного зв'язку з реальним економічним станом суб'єкта господарювання.

Розвиваючи цей методологічний підхід та адаптуючи його до реалій сьогодення, у найновіших дослідженнях Ф. В. Немировський акцентує увагу на тому, що в умовах трансформаційних зрушень ключового значення набуває «організаційно-економічний механізм управління інноваційно-інформаційною складовою економічної безпеки підприємства» [14]. Вчений справедливо зауважує, що інформаційні процеси на сучасних підприємствах не можуть розглядатись ізольовано від їхнього інноваційного розвитку. В умовах глобальної економічної турбулентності інформаційна безпека підприємницької діяльності перестає бути суто пасивним,

«загороджувальним» елементом. Натомість вона трансформується у динамічну інноваційно-інформаційну систему, яка, з одного боку, захищає цифрові активи компанії, а з іншого – виступає драйвером підвищення її конкурентоспроможності та ринкової резильєнтності.

Поділяючи наукову позицію Ф. В. Немировського, вважаємо, що синергія «інноваційного» та «інформаційного» в контурі економічної безпеки вимагає кардинального переосмислення самого організаційно-управлінського механізму. Традиційні архітектури безпеки, що орієнтовані на закупівлю статичного локального обладнання, є копіюванням застарілих моделей і не відповідають критеріям інноваційності. В умовах гіпертурбулентності, фінансових шоків та інфраструктурної нестабільності, інноваційність механізму управління інформаційної безпеки має полягати у його фінансово-організаційній гнучкості, здатності миттєво адаптувати інфраструктуру захисту до мінливих фінансових можливостей підприємства.

У вітчизняній науковій традиції «механізм» у контексті управлінських систем охоплює сукупність методів, інструментів і процедур досягнення визначеної мети [15]. Л. М. Калініна обґрунтовує концепцію технології розроблення та запровадження цих механізмів, спираючись на засади системології, синергетики та сучасного менеджменту. У роботі здійснено наукову класифікацію організаційних механізмів, розглядаючи їх як невід’ємний компонент мегасистеми управління загальною середньою освітою в умовах переходу України до моделі сервісної держави [16].

У роботі Ю. В. Гуменюка [17] запропоновано авторське визначення організаційно-економічного механізму як сукупності взаємопов’язаних важелів, методів впливу та організаційних структур, що забезпечують ефективне виробництво, розподіл і споживання зернопродукції. Особливу увагу приділено розробці стратегічних напрямів підвищення якості продукції, інноваційно-інвестиційному забезпеченню галузі та екологізації виробничої діяльності.

Р. Л. Лупак та М. В. Куницька-Іляш [18] обґрунтовують доцільність застосування структурно-функціонального підходу, який дозволяє чітко

розмежувати інструментарій на організаційний (реформування систем управління, створення R&D центрів) та економічний (ресурсне забезпечення, інвестування та монетизація інновацій). У роботі доведено, що ключовими чинниками успіху є впровадження цифрових технологій, розробка комплексних стратегій розвитку та активна участь підприємств у глобальних інноваційних екосистемах.

У науковій публікації Сергія Калініченка [19] досліджено методологічні принципи побудови організаційно-економічного механізму, спрямованого на розвиток економічного потенціалу аграрних підприємств в умовах структурних трансформацій. Особливу увагу приділено формуванню адаптивних моделей управління, які дозволяють оптимізувати використання ресурсного потенціалу та підвищити конкурентоспроможність суб'єктів аграрного бізнесу.

Згідно з проведеним аналізом, у науковому середовищі справді відсутній уніфікований підхід до визначення сутності організаційно-економічного (управлінського) механізму, що підтверджується дослідженнями різних авторів. Основні наукові підходи щодо сутності організаційно-управлінського згруповані на рисунку 2.5.

На основі проведеного аналізу наукових праць можна зробити висновок, що складність і багатогранність категорії «організаційно-економічний механізм» обумовлюють відсутність єдиного загальноприйнятого підходу до її визначення. Кожен із розглянутих підходів акцентує увагу на специфічних аспектах управління залежно від об'єкта дослідження: системний, інструментально-важелевий, структурно-функціональний, адаптивно-інституційний, ресурсно-цільовий підходи. Таким чином, вибір конкретного підходу або їх синтез визначається потребою підприємства в адаптації до умов ринку, необхідністю модернізації системи управління та пріоритетами інноваційного розвитку. Багатоманітність трактувань є свідченням динамічного розвитку цієї наукової категорії в сучасних економічних умовах.

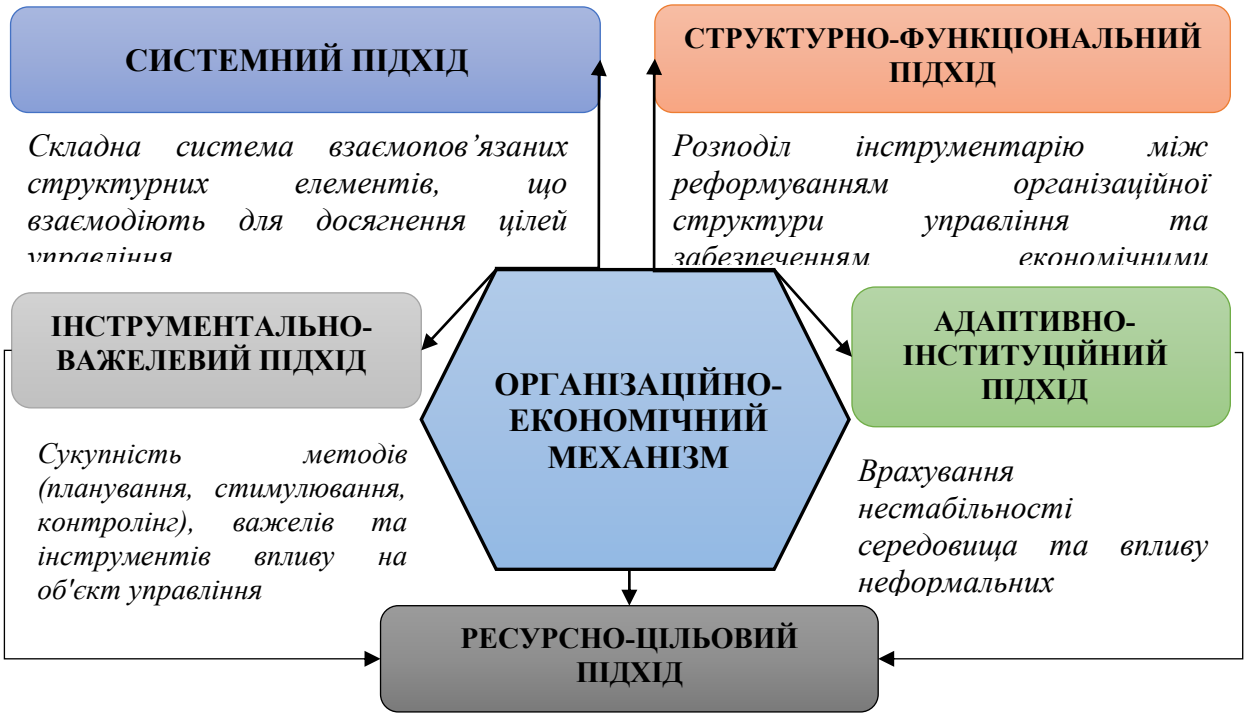


Рис. 2.5. Ключові підходи до визначення сутності організаційно-економічного механізму

Джерело: сформовано автором на основі [1, 11-14, 20-22]

Вважаємо, що організаційно-управлінський механізм інформаційної безпеки підприємства – це система взаємопов'язаних управлінських рішень, організаційних процедур і поведінкових регуляторів, що забезпечують захист інформаційних активів через зміну операційних практик, компетентнісного профілю і культури персоналу. Відмінністю від технологічного підходу є спрямованість не на захист об'єктів, а на зміну суб'єктів відповідних дій, рішень, звичок.

Глобальна економічна турбулентність загострює цю проблему. В умовах нестабільності підприємці скорочують «необов'язкові» витрати і спрощують «зайві» процедури. Безпекові регламенти потрапляють під обидва скорочення. Персонал перевантажений і перестає дотримуватися протоколів. Рішення приймаються швидко, без безпекової верифікації. Поверхня вразливості розширюється саме тоді, коли зовнішні загрози посилюються.

На підставі проведеного аналізу пропонується авторський підхід до структурування організаційно-управлінського механізму забезпечення інформаційної безпеки підприємства. Механізм охоплює три взаємопов'язані субмеханізми, кожен з яких спрямований на усунення відповідного класу дисфункцій.

Регламентний субмеханізм – система внутрішніх нормативних актів, що операціоналізують безпекові вимоги у форматі обов'язкових процедур. Умовою його дієвості є те, що регламенти мають бути вбудовані в реальний операційний процес, а не існувати паралельно з ним. Кожна безпекова процедура повинна мати відповідь на питання «коли і ким виконується», а не лише «що є обов'язковим». Складовими регламентного субмеханізму є порядок надання і відкликання доступів до інформаційних ресурсів; процедури реагування на підозрілі операції; правила роботи з зовнішніми носіями і хмарними сервісами; алгоритми дій при кіберінциденті.

Компетентнісний субмеханізм – система формування і підтримки безпекових компетентностей персоналу на всіх рівнях організаційної ієрархії. Підготовка власника-менеджера і підготовка рядового співробітника через різні завдання. Перший має розуміти ризик-профіль підприємства і пов'язувати безпекові рішення з бізнес-стратегією. Другий повинен знати конкретні практики безпечної поведінки у конкретних робочих ситуаціях. Компетентнісний субмеханізм передбачає: ситуаційне навчання, прив'язане до реального операційного контексту; регулярну верифікацію засвоєних навичок через практичні перевірки; диференційований підхід за рівнями доступу і функціональними ролями.

Культурний субмеханізм – система цінностей, норм і символічних практик, що формують ставлення до інформаційної безпеки як до особистої відповідальності кожного, а не до зовнішнього обов'язку. Культурний субмеханізм найважче формалізується і найдовше формується, але саме він визначає поведінку персоналу у нестандартних ситуаціях, коли регламент не дає готової відповіді. Ключові елементи: видима залученість керівництва до

безпекових практик; система визнання безпекових ініціатив співробітників; відкрите обговорення інцидентів без пошуку винних.

Глобальна економічна турбулентність висуває специфічні вимоги до організаційно-управлінського механізму. Вони не скасовують описану структуру, але суттєво коригують акценти реалізації.

Під організаційно-управлінським механізмом управління інформаційною безпекою підприємницької діяльності в умовах глобальної економічної турбулентності необхідно розуміти складну систему впливу на функціонування підприємництво, що охоплює законодавче, інформаційне, методичне та інституційне забезпечення, інструменти (аналітичні (індекс Іфез, стрес-тести, моніторинг БАД), фінансові (модель Сарех, Орех, кіберстрахування), організаційні (ISO 27001, аутсорсинг), технологічні (хмарні, SOC)), фактори впливу (воєнно-політичні, геополітичні, макроекономічні, ринкові, регуляторні, фінансово-економічні, організаційно-технологічні, соціально-психічні) та специфічні особливості (фінансово-економічний моніторинг виступає основною для трансформації контуру технологічного захисту), а також зорієнтована на зміну особистих та спільних ціннісних орієнтирів колективної відповідальності за збереження інформаційного капіталу та трансформація системи інформаційної безпеки із системи обмежень у систему спільної життєстійкості (резильєнтності). Це забезпечує внутрішню консолідацію підприємства та підтримує стабільні індекси його ділової активності та глобальної конкурентоспроможності незалежно від амплітуди коливань зовнішнього турбулентного середовища.

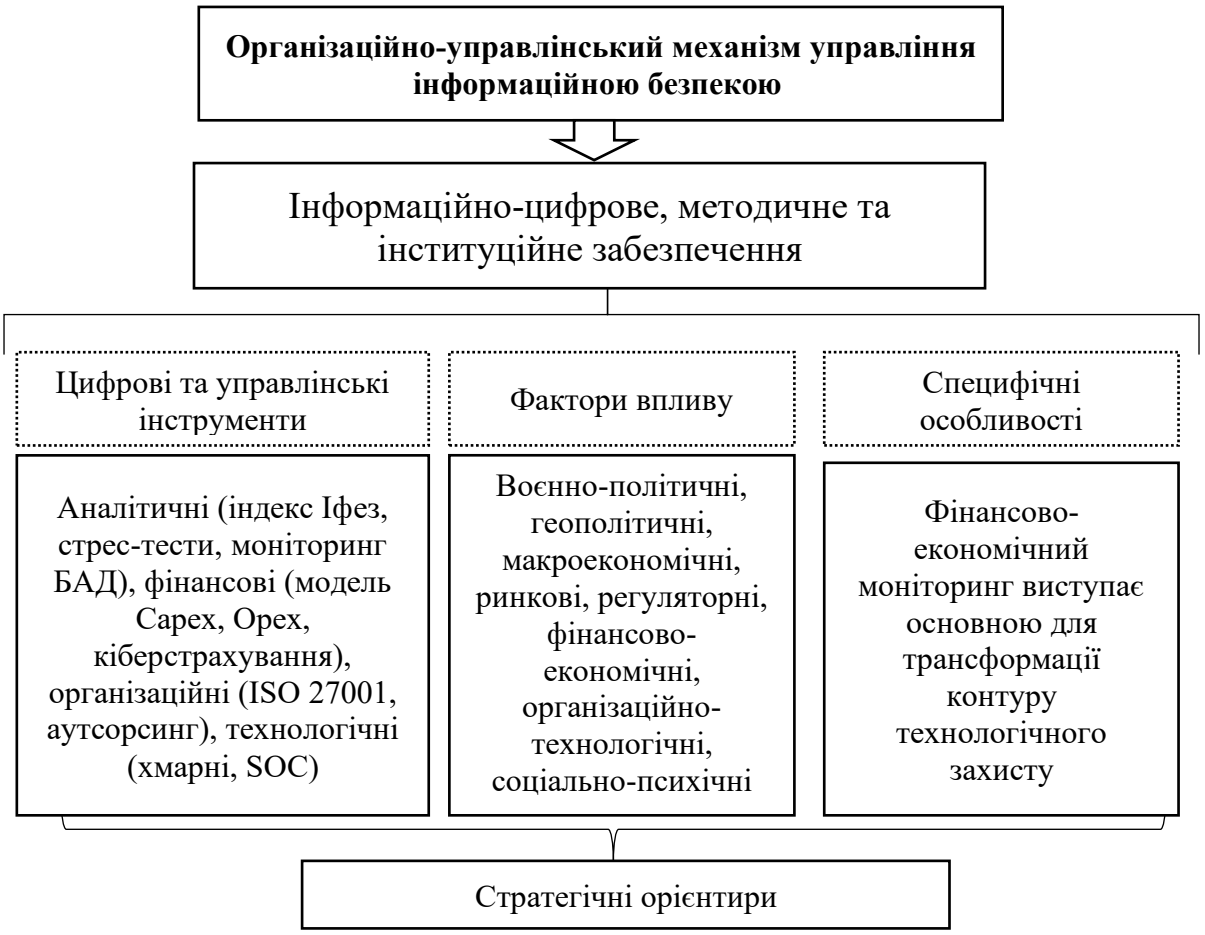


Рис. 2.6. Організаційно-управлінський механізм управління інформаційною безпекою підприємницької діяльності в умовах глобальної економічної турбулентності

Джерело: запропоновано автором.

Новизна запропонованого інструментарію полягає не у виокремленні поодиноких засобів захисту, а у їхній композиційній гнучкості. Завдяки інтеграційному контуру організаційно-управлінського механізму, фінансово-економічні інструменти (наприклад, кіберстрахування) та технологічні інструменти (наприклад, SECaaS) застосовуються не хаотично, а суворо координуються з інформаційно-аналітичними інструментами (індексом $І_{фез}$ та показниками ділової активності). Це мінімізує витрати на безпеку та максимізує конкурентоспроможність підприємства в умовах глобальної турбулентності.

Організаційно-управлінський механізм управління інформаційною безпекою підприємств цифрового ринку в умовах глобальної економічної турбулентності є динамічною, інноваційно-орієнтованою системою, що забезпечує безперервність бізнес-процесів та утримання високих індексів ділової активності й міжнародної конкурентоспроможності. На відміну від класичних статичних моделей, його архітектура базується на безперервному чотирифазному «циклі резильєнтності» (скринінг, позиціонування, фінансово-технологічна алінація та стрес-тестування), який забезпечує миттєву адаптацію та швидке відновлення системи захисту після інфраструктурних, воєнних чи макроекономічних шоків ринку. Практична реалізація механізму досягається через гнучкий фінансово-організаційний маневр (CAPEX, OPEX): у разі зниження Інтегрального індексу фінансово-економічної захищеності ($I_{фез}$<0,69) управляюча підсистема запускає процес згортання капіталомістких локальних проектів і переводить інфраструктуру на сервісну хмарну модель за підпискою (OPEX / SECaaS), що дозволяє малому бізнесу імпортувати безпеку найвищого рівня без вимивання оборотного капіталу. Ефективність інтегрованого інструментарію (аналітичного моніторингу, кіберстрахування, хмарних екосистем та концепції Zero Trust) посилюється через формування спільних ціннісних орієнтирів усередині команди (прозорості, взаємної довіри та колективної відповідальності за цифровий периметр). Це трансформує систему менеджменту безпеки з регресивного «органу обмежень» на соціокультурну філософію спільної життєздатності компанії, мінімізуючи деструктивний вплив людського фактора та дефіциту кадрів. У підсумку наукова та практична цінність розробленого механізму полягає в переході від фрагментарного IT-захисту інфраструктури до проактивного, економічно виваженого безпекового менеджменту, де кожне управлінське рішення та витрачена гривня суворо зважені на реальний рівень фінансової резильєнтності підприємства.

Висновки до розділу 2

У другому розділі дисертаційного дослідження здійснено аналіз організаційно-управлінських передумов забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності; проведено структурно-динамічний аналіз макроекономічних детермінант розвитку бізнес-систем; оцінено потенціал розвитку підприємницької діяльності; запропоновано організаційно-управлінський механізм управління інформаційною безпекою підприємницької діяльності в умовах глобальної економічної турбулентності. За результатами проведених досліджень, зроблено наступні висновки:

1. Виявлено високий рівень макроекономічної резильєнтності (життєстійкості) цифрового сектору на тлі загальнодержавної рецесії. Попри глибокі екзогенні шоки (економічну кризу 2014–2015 рр., пандемію COVID-19 та руйнівні наслідки повномасштабної війни після 2022 р.), бізнес-системи цифрового ринку продемонстрували стійку динаміку зростання обсягів реалізованої продукції та частки у структурі ВВП України. Структурне зближення національного інформаційного простору із глобальним цифровим ринком дозволило галузі виступити ключовим драйвером валютних надходжень та підтримати макроекономічну стабільність держави в періоди найвищої турбулентності.

2. Діагностовано структурну полярність та «ефект масштабу» в абсорбції безпекових ризиків. Аналіз динаміки фінансово-економічних детермінант виявив суттєву асиметрію між суб'єктами господарювання залежно від їхнього масштабу. Великі та середні підприємства сектору сформували потужний фінансовий «імунітет» – профіцит ліквідності та високий рівень автономії, що дозволило їм успішно поглинати шоки інфраструктурної нестабільності (блекаути, релокацію кадрів). Навпаки, мікро- та малий бізнес продемонстрували стиснуту ліквідність і критичну чутливість до коливань ринку, що обумовлює їх хронічне перебування в зонах

«операційної вразливості» та вимагає диференційованого підходу до управління їх фінансово-економічною безпекою.

3. Обґрунтовано критичну залежність ділової активності від детермінант інформаційної безпеки. Динаміка індексів ділової активності (оборотністі капіталу, темпів зростання чистого доходу) продемонструвала пряму кореляцію з безперервністю функціонування ІТ-інфраструктури. Установлено, що будь-які інфраструктурні збої або успішні таргетовані кібератаки призводять до миттєвого падіння операційної ефективності бізнес-систем. Це доводить, що інформаційна безпека в умовах глобалізаційних процесів є не ізольованою технічною функцією, а базовою економічною детермінантою, яка безпосередньо визначає швидкість обертання капіталу підприємства.

4. Обґрунтовано та побудовано Стратегічну матрицю безпекового позиціонування підприємств цифрового ринку. Запропонована матриця виступає логічним завершенням авторської оціночної методики. Вона дозволяє диференціювати підприємства за чотирма якісними безпековими квадрантами залежно від числових меж Інтегрального індексу фінансово-економічної захищеності ($0{,}00 > I_{фез} > 1{,}00$): від Квадранту I («Критична незахищеність») до Квадранту IV («Автономна стійкість»). Уніфікація цих меж із конкретними характеристиками фінансового стану, стандартами комплаєнсу та рівнем резильєнтності до кібератак дозволяє менеджменту відійти від інтуїтивного управління та здійснювати стратегічне планування безпеки на основі об’єктивних інформаційно-аналітичних даних.

5. Доведено реципрокний (взаємний) зв'язок між станом інформаційної безпеки, індексами ділової активності та міжнародної конкурентоспроможності підприємств. Установлено, що в умовах глобальної турбулентності інформаційна безпека перестає бути суто витратною статтею, а трансформується в інструмент ринкового позиціонування. Індекси ділової активності (оборотність капіталу, темпи зростання чистого доходу) перебувають у прямій залежності від безперервності бізнес-процесів:

мінімізація часу простою через кіберинциденти або інфраструктурні шоки є базовою умовою збереження високої ділової активності.

6. Обґрунтовано інноваційно-орієнтований характер фінансування системи інформаційної безпеки на основі фінансово-організаційного маневру. Модель CAPEX (капіталомістка), рекомендована для підприємств Квадранту IV з високими індексами конкурентоспроможності та ділової активності ($I_{фез}$>0,70). Інвестиції у власний Центр управління безпекою (SOC) та сертифікацію ISO/IEC 27001 капіталізуються у вигляді нематеріальних активів, що ще більше підвищує ринкову вартість компанії. Модель OPEX / SECaaS (сервісна), рекомендована для підприємств Квадрантів I–II зі зниженими показниками ділової активності ($I_{фез}$<0,69). Перехід на хмарні безпекові сервіси за підпискою дозволяє малому бізнесу імпортувати високі стандарти захисту, зберігаючи дефіцитну ліквідність та утримуючи базовий рівень конкурентоспроможності без надлишкового фінансового тиску на баланс.

7. В процесі аналізу визначено, що організаційно-управлінські механізми забезпечують реальну інформаційну безпеку підприємства не за допомогою технологій, а за допомогою поведінки людей, які з цими технологіями працюють. Визначено, що організаційно-управлінський вимір інформаційної безпеки підприємства якісно відрізняється від технологічного та спрямований не на захист об'єктів, а на зміну поведінки суб'єктів. Відсутність цього виміру робить технологічний захист неефективним незалежно від його рівня. Ідентифіковано чотири типи управлінських дисфункцій – делегативна, формалізаційна, компетентнісна і ситуаційна. Усі вони системні, характерні для значної частини підприємницьких структур регіону і виявляються незалежно від розміру підприємства чи наявного технологічного оснащення. Запропонований механізм як система регламентних, компетентнісних і культурних субмеханізмів, забезпечує комплексний підхід до усунення виявлених дисфункцій. Кожен субмеханізм має чіткий предмет впливу і власні інструменти реалізації.

8. Наголошено, що адаптація механізму до умов глобальної економічної турбулентності вимагає: підвищення стресостійкості регламентів; гнучкості компетентнісного навчання; організаційного закріплення культурних норм безпеки; розвитку навичок критичної верифікації зовнішньої інформації у менеджменту підприємства. Практичне значення наукового дослідження полягає у структуруванні організаційно-управлінського механізму забезпечення інформаційної безпеки підприємства, що дозволяє суб’єктам господарювання визначити інструменти його реалізації, враховуючи особливості діяльності.

9. Індекси конкурентоспроможності цифрових підприємств на зовнішніх ринках сьогодні прямо детерміновані рівнем їхнього безпекового комплаєнсу. Наявність сертифікатів безпеки є безальтернативною перепусткою до міжнародних контрактів, що безпосередньо масштабує конкурентний потенціал суб'єкта господарювання. Розроблено архітектоніку та динамічний контур організаційно-управлінського механізму управління інформаційної безпеки. Доведено, що для протидії екзогенним шокам цей механізм має володіти властивістю високої резилієнтності. Механізм структуровано за трьома підсистемами: забезпечуючою, функціональною та управляючою. Головною відмінністю механізму є наявність адаптаційного «циклу резилієнтності» (скринінг позиціонування фінансово-технологічна алінація стрес-тестування). Це дозволяє реагувати на коливання індексів ділової активності та конкурентоспроможності шляхом миттєвої перебудови архітектури захисту в режимі реального часу.

10. Запропоновано, що під організаційно-управлінським механізмом управління інформаційною безпекою підприємницької діяльності в умовах глобальної економічної турбулентності можливо розуміти складну систему впливу на функціонування підприємництва, яка охоплює законодаче, інформаційне, методичне та інституційне забезпечення, інструменти (аналітичні (індекс Іфез, стрес-тести, моніторинг БАД), фінансові (модель Сарех, Орех, кіберстрахування), організаційні (ISO 27001, аутсорсинг),

технологічні (хмарні, SOC)), фактори впливу (воєнно-політичні, геополітичні, макроекономічні, ринкові, регуляторні, фінансово-економічні, організаційно-технологічні, соціально-психічні) та специфічні особливості (фінансово-економічний моніторинг виступає основною для трансформації контуру технологічного захисту), а також спрямована на зміну особистих та спільних ціннісних орієнтирів колективної відповідальності за збереження інформаційного капіталу та трансформація системи інформаційної безпеки із системи обмежень у систему спільної життєстійкості (резильєнтності). Це забезпечує внутрішню консолідацію підприємства та підтримує стабільні індекси його ділової активності та глобальної конкурентоспроможності незалежно від амплітуди коливань зовнішнього турбулентного середовища.

Список використаних джерел до розділу 2

1. Пархоменко Н. О. Вплив тенденцій розвитку глобального середовища на діяльність бізнес-систем. *Вісник ХНУ імені В.Н. Каразіна. Серія: Міжнародні відносини. Економіка. Краєзнавство. Туризм.* 2020. Вип. 12. С. 59–68.

2. Swiss Economic Institute. KOF. URL: https://kof.ethz.ch/en/

3. Globalisation Index. KOF. URL: https://kof.ethz.ch/en/forecasts-and-indicators/indicators/kof-globalisation-index.html

4. Country index. Ease of Doing Business. URL: https://archive.doingbusiness.org/en/rankings

5. Business Ready 2025. World Bank Group. URL: https://surl.li/quaohz

6. B-READY: Business Entry: Overall Score. World Bank Group. URL: https://data.worldbank.org/indicator/IC.BRE.BE.OS

7. World Competitiveness Ranking. 2025. IMD. URL: https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-competitiveness-ranking/

8. Державна служба статистики України: офіційний сайт. URL: https://www.ukrstat.gov.ua

9. Релокація бізнесу: Державна підтримка та досвід компаній. Європейська Бізнес Асоціація. URL: https://eba.com.ua/relokatsiya-biznesu-derzhavna-pidtrymka-ta-dosvid-kompanij/

10. Припута Н. В. Методичні підходи до оцінки рівня монополізованості в економіці. *Науковий вісник Мукачівського державного університету. Серія «Економіка».* 2016. Вип. 1(5). С. 51–55. URL: http://nbuv.gov.ua/UJRN/nvmdue_2016_1_10

11. Петрук О. М., Городиський М. П., Поліщук І. Р. Аналіз інтенсивності застосування підприємствами інформаційних технологій при виконанні бізнес-процесу «Маркетинг». *Сталий розвиток економіки.* 2025. № 5(56). DOI: https://doi.org/10.32782/2308-1988/2025-56-25

12. Куценко О. А. Методичні засади оцінки стану фінансово-економічної безпеки та вибору інструментів управління для промислових підприємств. Український журнал прикладної економіки та техніки. 2022. Том 7. № 4. С. 297–303. DOI: https://doi.org/10.36887/2415-8453-2022-4-45

13. Ольшанська О. В. Основні положення інформаційної безпеки та її стан в сучасних умовах розвитку в Україні. *Вісник Київського національного університету технологій та дизайну. Серія: Економічні науки.* 2015. № 2(85). С. 62–68. URL: https://ir.kneu.edu.ua/server/api/core/bitstreams/958a2bb9-729c-49e3-845d-6d148a6411ad/content

14. Немировський Ф. В. Організаційно-економічний механізм управління інноваційно-інформаційною складовою економічної безпеки підприємства. *Цифрова економіка та економічна безпека.* 2026. № 1(22). С. 65–70. DOI: https://doi.org/10.32782/dees.22-10

15. Зачосова Н. В. Економічна безпека та інформаційна безпека: спільні та відмінні риси, особливості управління. *Ефективна економіка.* 2017. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=5525

16. Калініна Л. М. Організаційні механізми управління діяльністю загальноосвітніх навчальних закладів у змісті підручника для керівника. *Електронна бібліотека НАПН України*. 2013. URL: https://surl.li/bzewji

17. Гуменюк Ю. В. Організаційно-економічний механізм функціонування зернопродуктового підкомплексу. *Вісник Хмельницького національного університету. Економічні науки*. 2019. № 3. С. 71–77. URL: https://socrates.vsau.org/repository/getfile.php/22988.pdf

18. Лупак Р. Л., Куницька-Іляш М. В. Інструментарій організаційно-економічного механізму забезпечення інноваційного розвитку підприємства. *Ефективна економіка*. 2025. № 7. DOI: http://doi.org/10.32702/2307-2105.2025.7.12

19. Калініченко С. Методологічні принципи побудови організаційно-економічного механізму розвитку економічного потенціалу аграрних підприємств. *Вісник Хмельницького національного університету. Економічні науки*. 2024. № 4 (332). С. 565–571. DOI: https://doi.org/10.31891/2307-5740-2024-332-84

20. Іртищева І. О., Тубальцева Н. П., Іщенко О. А., Арчибісова Д. С., Палій В. В. Управління бізнес-процесами підприємств України в умовах цифрової трансформації та глобальної нестабільності. *Український журнал прикладної економіки та техніки.* 2025. № 3. С. 86–89.

21. Павленко О. П., Іртищева І. О., Карпенко Г. Ю. Наукові підходи щодо глобальної турбулентності: особливості виникнення, сучасний стан та перспективи впливу. *Український журнал прикладної економіки та техніки*. 2022. Т. 7. № 1. С. 238–246.

22. Popelo O., Shaposhnykov K., Popelo O., Hrubliak O., Malysh V., Lysenko Zh. The Influence of Digitalization on the Innovative Strategy of the Industrial Enterprises Development in the Context of Ensuring Economic Security. *International Journal of Safety & Security Engineering*. 2023. Vol. 13, No. 1. P. 39–49.

РОЗДІЛ 3
СТРАТЕГІЧНІ ОРІЄНТИРИ ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКИХ ЗАСАД ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ГЛОБАЛЬНОЇ ЕКОНОМІЧНОЇ ТУРБУЛЕНТНОСТІ

3.1. Європейський досвід забезпечення інформаційної безпеки підприємницької діяльності та шляхи його імплементації у вітчизняних реаліях

В умовах повномасштабної геополітичної кризи та стрімкої євроінтеграції України дослідження передових європейських практик забезпечення інформаційної безпеки підприємницької діяльності набуває для вітчизняної науки і практики безпрецедентної актуальності. Глобальна економічна турбулентність та трансформація кіберзагроз змусили Європейський Союз радикально еволюціонувати від концепції статичного технічного захисту периметру до філософії комплексної цифрової операційної резилієнтності бізнес-систем. Сучасний європейський регуляторний ландшафт, сформований жорсткими вимогами Директиви NIS 2 [1] та Регламенту DORA [2], перевів питання інформаційної безпеки з площини суто технічних IT-завдань у категорію стратегічних фінансово-економічних детермінант розвитку компаній. При цьому європейська модель безпекового менеджменту імперативно покладає персональну юридичну та матеріальну відповідальність за кіберстійкість безпосередньо на вище керівництво (C-level), що докорінно змінює архітектуру корпоративного управління.

Для вітчизняного цифрового сектору, який функціонує в екстремальних умовах воєнного стану, блекаутів та гострого дефіциту ліквідності, сліпе копіювання європейських стандартів є фінансово неможливим, що актуалізує потребу в розробленні гнучких адаптаційних механізмів. На особливу увагу заслуговує європейський досвід мінімізації капітальних витрат (CAPEX) через масове впровадження шерингової безпеки та аутсорсингу операційних

функцій захисту хмарним провайдерам за сервісною моделлю (SECaaS / OPEX).

Оскільки спроможність українських підприємств інтегруватися у світовий економічний простір та утримувати міжнародні контракти сьогодні прямо залежить від рівня їхнього безпекового комплаєнсу, адаптація європейських інструментів є ключовим фактором підвищення їхньої глобальної конкурентоспроможності. Брак системних вітчизняних досліджень, які б пов'язували європейські регуляторні вимоги з реальними показниками ділової активності та фінансово-економічної захищеності підприємств, зумовлює високу наукову цінність цього напряму. Таким чином, критичний аналіз та наукове обґрунтування шляхів імплементації європейського досвіду в практику вітчизняного бізнесу є базовою передумовою для формування життєздатного організаційно-управлінського механізму, здатного підтримувати економічну стійкість підприємств у гіпертурбулентному середовищі.

У контексті євроінтеграційних процесів України та гармонізації національного законодавства із правовим полем Європейського Союзу, дослідження європейського досвіду забезпечення інформаційної безпеки підприємницької діяльності набуває критично важливого значення. Глобальна економічна турбулентність та зростання інтенсивності транскордонних кібератак змусили ЄС радикально переглянути свою безпекову філософію – відбувся перехід від пасивного технічного захисту даних до концепції цифрової операційної резилієнтності бізнес-систем.

Аналізуючи інституціональну архітектуру міжнародних безпекових трендів, С. Мазепа наголошує, що «Європейський Союз, будучи одним із провідних центрів розробки правових норм у сфері інформаційної безпеки, створив комплексну систему регулювання, яка стала взірцем для багатьох країн світу» [3, с. 290]. Слід підкреслити, що першим фундаментальним кроком на шляху формування цієї міжнародної архітектури стала Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) від 2001 року,

яка є першим міжнародним договором з питань кіберзлочинності [4]. Даний документ визначив загальні принципи криміналізації комп'ютерних злочинів, процедури розслідування та основи міжнародного співробітництва, а Додатковий протокол до неї закріпив криміналізацію актів расистського та ксенофобського характеру, вчинених через комп'ютерні системи [4]. Будапештська конвенція заклала первинний правовий базис, на якому згодом почали формуватися галузеві стандарти безпеки бізнес-систем. Історично Європейський Союз виступив першим у створенні комплексного правового регулювання кібербезпеки, що першочергово знайшло своє відображення у Директиві NIS (EU) 2016/1148 про заходи для високого загального рівня безпеки мережевих та інформаційних систем по всьому Союзу [5]. Саме ця Директива заклала підвалини для обов'язкового контролю критичних інфраструктур і стала основою, на якій у 2026 році функціонує оновлений та значно жорсткіший пакет європейських регламентів:

1. Директива NIS 2 (EU 2022/2555) трансформує інформаційну безпеку цифрових та IT-підприємств у жорстко контрольовану юридичну категорію з персональною фінансовою відповідальністю менеджменту.

2. Загальний регламент про захист даних (GDPR) конвертує ризики витоку інформації у прямі фінансові загрози через систему оборотних штрафів (до 4% від річного глобального доходу компанії).

3. Регламент DORA (Digital Operational Resilience Act) запроваджує обов'язкове стрес-тестування операційної життєстійкості бізнес-систем фінансово-цифрового контуру.

Важливим кроком на шляху поглиблення інтеграційних процесів стало ухвалення Регламенту (ЄС) 2019/881 (Акт про кібербезпеку ЄС), який закріпив постійний мандат ENISA та запровадив загальноєвропейську рамку сертифікації кібербезпеки інформаційно-комунікаційних технологій [6]. Відповідно до положень цього Регламенту, країни Центральної Європи як учасники ЄС мають «у певному сенсі злагоджену систему захисту інформації» [6]. Ця злагодженість забезпечує єдині стандарти для транскордонного

цифрового бізнесу, що критично важливо для збереження його ділової активності. Та разом з цим усі держави керуються своїми законами, положеннями, інструкціями, якими врегульовуються питання, суттю яких виступає інформаційна безпека. Тобто європейський підхід демонструє унікальний баланс між жорсткою наднаціональною уніфікацією правил (для захисту спільного ринку та утримання глобальної конкурентоспроможності) і збереженням суверенної гнучкості національних правових систем для врахування локальних безпекових чинників.

Ключові елементи європейського досвіду забезпечення інформаційної безпеки базуються на переході від статичного захисту периметру до філософії комплексної цифрової операційної резилієнтності бізнес-систем (рис. 3.1). Провідну роль у цій моделі відіграє жорстка нормативна уніфікація та стандартизація (зокрема, директиви NIS 2, GDPR та регламент DORA), які поєднуються із суверенною гнучкістю національних правових систем окремих країн-учасниць. Важливою ознакою європейського підходу є імперативне покладання персональної юридичної та матеріальної відповідальності за стан кіберзахисту безпосередньо на вище керівництво компаній (C-level), а не лише на IT-департаменти. Крім того, європейська практика орієнтована на мінімізацію капітальних витрат бізнесу шляхом масового впровадження шерингової безпеки, хмарних екосистем та аутсорсингу операційних функцій захисту за сервісною моделлю (SECaaS/OPEX). Наостанок, система захисту обов'язково охоплює управління ризиками третіх сторін і розвиток ситуаційної обізнаності через автоматизований обмін даними про індикатори компрометації.

Рис. 3.1. Ключові елементи європейського досвіду забезпечення інформаційної безпеки

Джерело: узагальнено автором на основі [6; 7; 8; 9].

Концептуальні орієнтири європейського досвіду демонструють чіткий вектор. Інформаційна безпека сучасного підприємства більше не є внутрішньою технічною справою його системних адміністраторів, а виступає базовим індикатором його ринкової надійності та інвестиційної привабливості.

Проте, як справедливо акцентує С. Мазепа, «Україна, взявши курс на європейську інтеграцію та цифрову трансформацію, постає перед стратегічним викликом адаптації свого законодавства до європейських стандартів, що зумовлено як міжнародними зобов’язаннями, так і об’єктивними потребами забезпечення інформаційної безпеки в умовах сучасних цифрових загроз» [3, с. 290]. У контексті розвитку підприємницьких структур цей стратегічний виклик посилюється екзогенними шоками глобальної турбулентності та воєнно-політичної кризи в Україні. Вітчизняні бізнес-системи змушені вирішувати дилему: з одного боку, забезпечувати комплаєнс із дороговартісними європейськими стандартами для утримання експортних контрактів, а з іншого – виживати в умовах обмежених фінансових ресурсів та кадрового дефіциту.

Важливим етапом розвитку цієї системи стало ухвалення Закону України «Про основні засади забезпечення кібербезпеки України» від 2017

року, який встановив правові та організаційні основи забезпечення захисту кіберпростору країни [11]. Як зазначає С. Мазепа, даний «Закон передбачає створення національної системи кібербезпеки, визначає повноваження суб'єктів забезпечення кібербезпеки та встановлює основні принципи державної політики у цій сфері» [3, с. 293]. Проте в умовах сучасної глобальної турбулентності та воєнно-політичної кризи виникає потреба в адаптації цих загальнодержавних принципів безпосередньо до рівня мікроекономічних бізнес-систем.

Сьогодні створення ефективної системи реагування на кіберінциденти в Україні відбувається з урахуванням досвіду європейських країн та рекомендацій ENISA (Агентства ЄС з питань кібербезпеки) [3, с. 293]. На загальнонаціональному рівні Державна служба спеціального зв'язку та захисту інформації України виконує функції національної групи реагування на комп'ютерні надзвичайні події (CERT-UA), здійснюючи координацію діяльності з виявлення, попередження та ліквідації наслідків кіберінцидентів [3, с. 293; 12]. Для суб'єктів підприємницької діяльності вкрай важливим є те, що розвиток системи ситуаційної обізнаності про кіберзагрози базується на міжнародних стандартах обміну інформацією про індикатори компрометації та тактики, техніки і процедури кіберзловмисників [3, с. 293]. У вітчизняній практиці цей обмін здійснюється за посередництвом платформ CERT-UA та індустріальних центрів ISAC. Порівняльний аналіз моделей менеджменту інформаційної безпеки наведений у таблиці 3.1.

Аналізуючи результати порівняльного аналізу моделей управління інформаційною безпекою підприємств в ЄС та Україні (табл. 3.1), можна зробити висновок про наявність суттєвих концептуальних та інституціональних розбіжностей між двома системами. Європейська модель базується на проактивній філософії цифрової операційної резельєнтності та комплексному реагуванні на інциденти згідно з жорсткими рекомендаціями ENISA.

Таблиця 3.1

Порівняльний аналіз моделей управління інформаційною безпекою підприємств в ЄС та Україні

Критерій порівняння	Європейська модель (ЄС)	Вітчизняна практика (Україна)
Базова концепція	Операційна резильєнтність (Життєстійкість системи)	Захист інформаційного периметру (Фрагментарний захист)
Реагування на інциденти	Рекомендації ENISA, автоматизований CERT/CSIRT комплаєнс	Взаємодія із CERT-UA (Держспецзв'язку), ситуаційна обізнаність
Відповідальність	Персональна відповідальність вищого керівництва (C-level)	Делегування відповідальності на IT-відділ (CIO)
Фінансова модель	Інноваційне CAPEX/OPEX-планування, шерингова безпека	Остаточний принцип фінансування, брак гнучкості бюджетів

Джерело: згруповано автором.

На противагу цьому, у вітчизняній практиці досі переважає статичний підхід, орієнтований на захист локального інформаційного периметру, хоча взаємодія із CERT-UA поступово підвищує загальний рівень ситуаційної обізнаності бізнесу. Кардинально відрізняється і контур відповідальності: якщо в ЄС за кіберстійкість персонально відповідає вище керівництво компанії, то в Україні ці функції переважно делегуються на IT-відділ. Крім того, фінансова модель європейського бізнесу демонструє високу інноваційну гнучкість завдяки CAPEX/OPEX-плануванню та шерингу безпеки, тоді як українські підприємства обмежені остаточним принципом фінансування та жорсткістю бюджетів. Відтак, узагальнені відмінності підтверджують необхідність адаптації вітчизняних систем менеджменту до європейських стандартів з метою підвищення міжнародної конкурентоспроможності українських підприємств.

Як було зазначено вище, попри наднаціональну уніфікацію безпекового законодавства в межах ЄС, кожна держава-член керується власними інституціональними традиціями та нормативно-правовими інструментами. Для формування адаптивного вітчизняного механізму управління ІБ критично

важливим є вивчення досвіду країн Центральної Європи, які мають різні історичні траєкторії розвитку систем захисту інформації (табл. 3.2).

Таблиця 3.2

Міжнародний досвід системи захисту інформації

Країна	Правовий базис	Інституційне забезпечення	Стратегічні орієнтири та специфіка моделі захисту
Німеччина	Детально структуроване законодавство з чіткою градацією інформації з обмеженим доступом у федеральних законах. Закон «Про перевірку безпеки» нормативно закріплює чотири рівні класифікації секретності даних:— «цілком таємно»;— «таємно»;— «конфіденційно»;— «для службового користування».	Федеральна служба інформаційної безпеки (BSI) — провідний державний орган, що координує захист інформаційного простору країни.	Резервно-регламентуюча модель. Фокусується на високому рівні стандартизації процесів, суворому правовому комплаєнсі та математично точній диференціації режимів доступу до державних інтересів.
Республіка Польща	Нормативно-правова база адаптована до концепції вільного транскордонного інформаційного обміну, захисту прав людини та підтримки плюралістичних мас-медіа. Особлива увага приділена законодавчому захисту ІТ-систем та комп'ютерних мереж критичної інфраструктури.	Агентство внутрішньої безпеки (ABW) та створена на його базі урядова команда реагування на комп’ютерні інциденти (CERT.PL).	Проактивно-захисна модель. Пріоритетом є предиктивний кіберзахист критичної інфраструктури, руйнування або збої в якій можуть спричинити загрозу життю громадян, навколишньому середовищу, призвести до масштабних фінансових втрат чи дестабілізації органів влади.
Угорщина	Перша серед постсоціалістичних країн прийняла «Закон про захист інформації про особу та доступ до інформації, що становить суспільний інтерес». Законодавство про державну та офіційну таємницю повністю гармонізоване зі стандартами НАТО та практикою Альянсу.	Спеціалізовані урядові інституції кібербезпеки та органи державної влади, зобов'язані здійснювати інформаційне супроводження суспільства.	Рестриктивно-демократична модель. Поєднує високий рівень імперативних обмежень у сфері держтаємниці з гарантуванням прав громадян на прозорий доступ до публічних даних та обов'язком держави надавати точну й своєчасну інформацію.

Джерело: узагальнено автором на основі [13; 14; 15; 16; 17].

Детальний аналіз емпіричних даних, наведених у таблиці 3.2, дозволяє виокремити три автентичні підходи до управління інформаційною безпекою,

кожен з яких містить цінні прикладні орієнтири для українських підприємств в умовах глобальної турбулентності.

Досвід функціонування Федеральної служби інформаційної безпеки (BSI) Німеччини демонструє важливість стандартизації. Для вітчизняного бізнесу, що зазнає постійних макроекономічних шоків, німецький підхід підтверджує необхідність чіткої внутрішньої класифікації інформаційних активів. У межах організаційно-управлінського механізму це трансформується в обов'язкове проведення аудиту критичності бізнес-процесів (BIA), де кожному типу даних надається свій профіль захисту, що упереджує хаотичне та неефективне витрачання бюджету інформаційної безпеки.

Функціонал польського CERT під егідою ABW чітко корелює з сучасними вимогами щодо запобігання «значним фінансовим збиткам та збоям у функціонуванні». Цей досвід є архіважливим для українського IT-сектору. Він доводить, що в умовах турбулентності головним завданням безпекового менеджменту є не просто утримання абстрактного периметру, а забезпечення безперервності бізнесу (Business Continuity). Саме польський вектор акцентує на важливості ситуаційної обізнаності та побудови систем швидкого відновлення даних у хмарах у разі критичних руйнувань.

Досвід Угорщини як постсоціалістичної країни, що успішно адаптувала свої стандарти до вимог НАТО, є близьким до сучасного геополітичного стану України. Угорська практика показує, як важливо поєднувати суворі обмежувальні заходи захисту комерційної таємниці із забезпеченням прозорості та доступу до інформації. Впровадження цього досвіду на мікроекономічному рівні вимагає формування корпоративної культури прозорості, де персонал чітко розмежовує відкриті дані для клієнтів (що підвищує міжнародну конкурентоспроможність) та закриті інноваційні ресурси підприємства.

Узагальнюючи підходи до модернізації національної системи захисту інформаційних ресурсів у період євроінтеграційного транзиту, О. І. Пугачов цілком обґрунтовано зазначає, що «аналіз зарубіжного досвіду дозволяє

зробити висновок, що для України важливо адаптувати найбільш ефективні практики та інструменти з урахуванням національних особливостей та викликів» [9]. У межах дослідження під «національними особливостями та викликами» розуміються нелінійні шоки воєнного стану, триваючий інфраструктурний дефіцит та обмеженість інвестиційних ресурсів вітчизняних підприємств. Відтак адаптація міжнародних інструментів має відбуватися не директивно, а через призму економічної доцільності, де кожен крок із посилення безпеки інформаційної архітектури суворо зважується на рівень фінансово-економічної захищеності суб'єкта господарювання. Основні проблеми впровадження інформаційної безпеки у вітчизняних реаліях наведено на рис. 3.2.

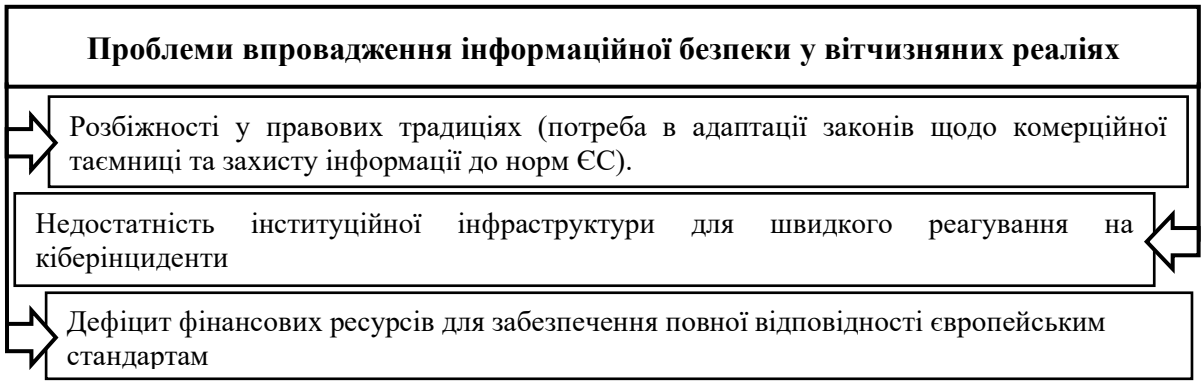


Рис. 3.2. Проблеми впровадження інформаційної безпеки у вітчизняних реаліях

Джерело: узагальнено автором на основі [3; 18].

Аналіз проблем впровадження інформаційної безпеки у вітчизняних реаліях дозволяє констатувати, що головними деструктивними чинниками виступають хронічний брак фінансових ресурсів малого й середнього бізнесу, кризова асиметрія ринку та дефіцит кваліфікованих кадрів, поглиблені нелінійними шоками воєнного стану. Національна практика менеджменту досі демонструє фрагментарний і статичний характер захисту локального периметру, що вступає у глибоку суперечність із європейськими імперативами цифрової операційної резильєнтності та персональної відповідальності керівництва. Водночас відсутність гнучких економіко-організаційних інструментів адаптації міжнародних стандартів (як-от NIS 2 чи DORA) до можливостей вітчизняних підприємств штучно стримує їхній безпековий

комплаєнс. Окреслені системні бар'єри обґрунтовують об'єктивну необхідність розроблення авторського організаційно-управлінського механізму, здатного нівелювати зазначені виклики через інноваційний маневр витратами та динамічний моніторинг захищеності бізнес-систем. Запропоновані шляхи імплементації зарубіжного досвіду у сфері забезпечення інформаційної безпеки в Україні наведено на рис.3.3.

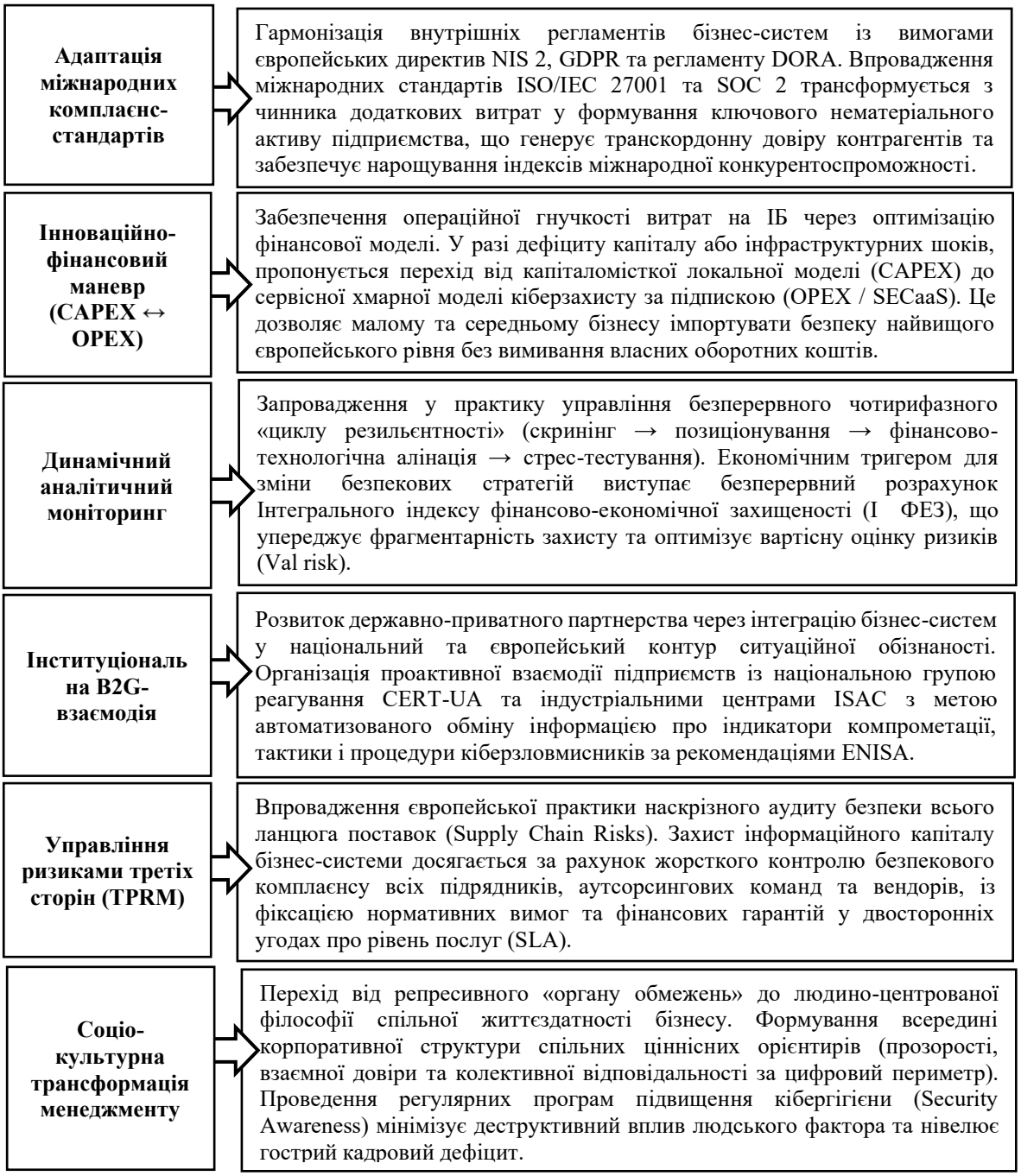


Рис. 3.3. Шляхи імплементації зарубіжного досвіду у сфері забезпечення інформаційної безпеки в Україні

Джерело: запропоновано автором

Сформовані стратегічні шляхи імплементації європейського досвіду (рис. 3.3) свідчать, що модернізація системи захисту інформаційних ресурсів вітчизняних підприємств в умовах турбулентності має базуватися не на пасивному копіюванні регуляторних вимог, а на принципах цифрової операційної резильєнтності та економічної доцільності.

Резюмуючи сутність запропонованих рішень, слід виокремити такі ключові аспекти:

1. Інтеграція жорстких європейських стандартів (NIS 2, DORA, ISO/IEC 27001) стає можливою навіть для фінансово обмежених суб'єктів господарювання завдяки гнучкому маневру витратами (CAPEX/OPEX) та переходу на шерингову модель безпеки (SECaaS).

2. Використання аналітичного індексу (Іфез) та наскрізного контролю ланцюгів поставок (TPRM/SLA) дозволяє оптимізувати вартісну оцінку ризиків (V_{alrisk}) і запобігання критичним фінансовим збиткам.

3. Ефективність технічних інструментів захисту максимізується через автоматизовану взаємодію з державним контуром кібербезпеки (CERT-UA за рекомендаціями ENISA) та трансформацію корпоративної культури в людиноцентровану філософію спільної життєздатності бізнесу.

У підсумку, практична реалізація окреслених шляхів дозволяє вітчизняним бізнес-системам подолати інфраструктурні та макроекономічні виклики, трансформуючи безпековий комплаєнс із чинника постійних капітальних витрат у дієвий важіль підвищення їхньої ділової активності та міжнародної конкурентоспроможності.

3.2. Дизайн адаптивної структурно-функціональної моделі розвитку підприємництва в умовах цифрової трансформації

Розвиток сучасних підприємницьких структур у координатах глобального цифрового простору відбувається в умовах безпрецедентної

екзогенної турбулентності, що вимагає радикальної перебудови традиційних статичних підходів до менеджменту. Ефективна цифрова трансформація бізнес-систем не може обмежуватися лише автоматизацією операційних процесів чи впровадженням новітнього програмного забезпечення; вона імперативно потребує формування адаптивної архітектури управління, де безпека інформаційного капіталу інтегрована безпосередньо в контур стратегічного розвитку. З огляду на це, виникає об'єктивна необхідність проєктування комплексного дизайну моделі розвитку підприємницької діяльності, здатного підтримувати високі індекси ділової активності та міжнародної конкурентоспроможності через механізми забезпечення цифрової операційної резилієнтності.

Розвиток сучасних підприємницьких структур у координатах глобального цифрового простору відбувається в умовах безпрецедентної екзогенної турбулентності, що вимагає радикальної перебудови традиційних статичних підходів до менеджменту. Ефективна цифрова трансформація бізнес-систем не може обмежуватися лише автоматизацією операційних процесів чи впровадженням новітнього програмного забезпечення. Обґрунтовуючи архітектоніку цих процесів, М. О. Дергалюк цілком слушно зазначає, що «у контексті глобалізації економічної діяльності та цифрової конкуренції особливо актуальним стає питання створення сприятливих умов для розвитку підприємництва в умовах цифровізації, що вимагає не лише технологічних інновацій, але й вдосконалення правової бази, фінансових механізмів підтримки та підвищення компетенцій підприємців» [19].

Розвиваючи цей комплексний підхід, слід підкреслити, що характер і масштабність зазначених перетворень мають системну макро- та мікроекономічну природу. Як наголошує колектив авторів у складі О. Ю. Литовченка, В. В. Дячека та М. О. Мітіна, «цифрова трансформація економіки змінює традиційні підходи до ведення бізнесу, сприяючи впровадженню новітніх технологій у різні галузі» [20]. Дослідники справедливо акцентують увагу на тому, що «цей процес має глибокий вплив на всі аспекти

підприємницької діяльності, включаючи маркетинг, логістику, фінансові операції та управління кадрами».

Подібний всеохоплюючий характер трансформації відкриває перед бізнесом суттєві стратегічні перспективи, зокрема через «автоматизацію процесів, поліпшення взаємодії з клієнтами та збирання великих обсягів даних для прийняття більш ефективних рішень». Водночас, закономірним наслідком таких глибинних зрушень є виникнення системних проблем, пов'язаних із «необхідністю адаптації бізнес-моделей до нових умов цифрової економіки, зокрема перехід від традиційних фізичних бізнес-структур до цифрових платформ». Реалізація такого переходу, як констатують науковці, «вимагає значних інвестицій у технології та зміни в управлінні компаніями», висуваючи на перший план жорсткі «виклики, пов'язані з безпекою даних, інтеграцією нових технологій і забезпеченням ефективності бізнес-процесів».

В. Шевцов акцентує на тому, що «для успішної адаптації підприємств до умов цифрової економіки необхідно впровадження комплексного підходу, що охоплює модернізацію цифрової інфраструктури, розвиток гнучких управлінських структур та активне залучення споживачів». При цьому вчений солідаризується з ідеєю багатовекторності трансформації, виокремлюючи як ключові аспекти «забезпечення кібербезпеки, оптимізацію роботи з великими даними та безперервне навчання персоналу», що у сукупності дозволяє суб'єктам господарювання «не лише ефективно використовувати новітні технології, але й оперативно реагувати на зміни в ринку та споживчих потребах, забезпечуючи їхню стійкість та конкурентоспроможність в довгостроковій перспективі» [21].

Оцінюючи стратегічний вектор таких адаптаційних процесів, С. О. Шут обґрунтовано вказує, що «цифрова трансформація надає підприємцям нові можливості для глобальної експансії, знижуючи бар'єри для входу на ринок і відкриваючи нові способи взаємодії з клієнтами». За твердженням дослідника, у цьому контексті «цифрові інструменти, такі як хмарні технології, штучний інтелект і Інтернет речей, стають ключовими компонентами успішної бізнес-

стратегії». Проте вчений солідаризується з думкою про двояку природу цифровізації, підкреслюючи, що вона «також породжує нові виклики. Підприємці повинні постійно адаптувати свої бізнес-моделі, враховуючи швидкі зміни технологій та ринкових умов». Зокрема, «використання цифрових платформ дає змогу масштабувати бізнес на глобальному рівні, але вимагає значних інвестицій у технологічні рішення та навчання кадрів» [22].

Аналіз емпіричних даних, наведених у рис. 3.4, дозволяє оцінити довгострокові тренди розвитку глобального цифрового ринку.

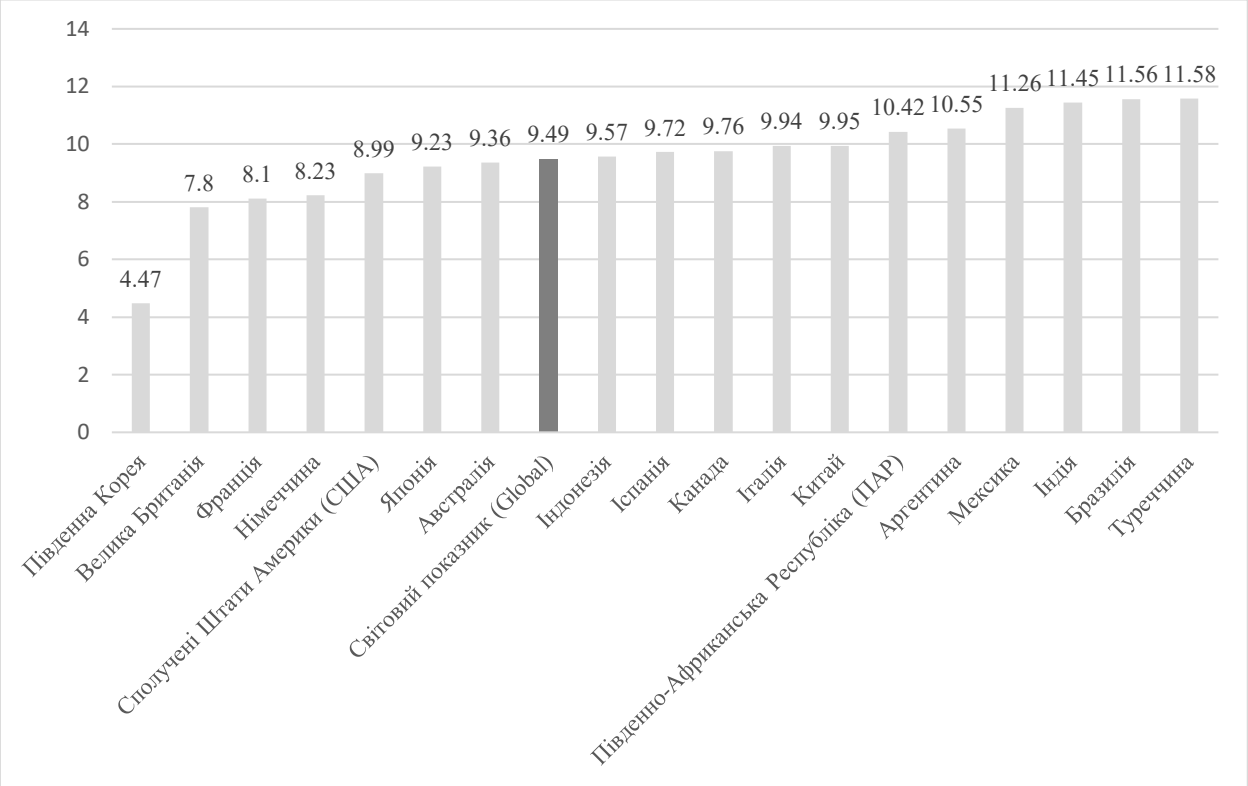


Рис. 3.4. Прогнозні середньорічні темпи зростання роздрібних продажів електронної комерції (CAGR) за країнами світу на період 2024–2029 рр.

Джерело: сформовано автором на основі [23].

Розраховані середньорічні темпи зростання роздрібної електронної комерції (CAGR) на період 2024–2029 років демонструють помітну диференціацію між розвиненими ринками та країнами, що розвиваються. Зокрема, країни з високим рівнем початкового насичення інфраструктури (такі як Південна Корея – 4,47%, Велика Британія – 7,80% та Німеччина – 8,23%) демонструють темпи зростання нижче середньосвітового орієнтиру, який

становить 9,49%. Натомість драйверами глобальної цифровізації виступають ринки Туреччини (11,58%), Бразилії (11,56%) та Індії (11,45%).

Для вітчизняних підприємств цей тренд є важливим індикатором: висока динаміка світового показника (CAGR=9,49%) підтверджує, що інтеграція в глобальні електронні платформи та оптимізація цифрових бізнес-моделей є безальтернативним вектором забезпечення їхньої довгострокової конкурентоспроможності.

Індекс цифрової економіки та суспільства (DESI) – це інтегральний (складений) індекс, який узагальнює відповідні цифрові показники та відстежує розвиток країн-членів ЄС у сфері цифрової трансформації та цифрової конкурентоспроможності [24]. Індекс DESI був розроблений відповідно до вказівок та рекомендацій Організації економічного співробітництва та розвитку (ОЕСР). Статистичні дані, які включено до індексу DESI, переважно збираються службами Європейської Комісії (зокрема, Eurostat, DG CNECT). Індекс DESI вимірюється за 100-бальною шкалою [25].

Відповідно до офіційної статистики Державної служби статистики України щодо впровадження інформаційно-комунікаційних технологій (ІКТ) суб'єктами господарювання відповідно до європейських стандартів індексу DESI (Компонент 3: «Інтеграція цифрових технологій») наведено в таблиці 3.3.

Проведений аналіз даних Державної служби статистики України за період 2020–2025 років (табл. 3.3) дозволяє виявити глибокі структурні диспропорції у процесах діджиталізації, що безпосередньо підтверджує обґрунтованість запропонованих інструментів (фінансово-організаційного моніторингу та індексу $I_{фез}$).

Частка підприємств із принаймні базовим рівнем цифрової інтенсивності у 2024–2025 роках стабілізувалася на критично низькому рівні (22,2% та 22,8% відповідно). Це означає, що майже 77% українських підприємств (із кількістю працюючих понад 10 осіб) функціонують поза

межами базових цифрових стандартів. Таке низьке насичення зумовлює високу вразливість бізнес-систем до зовнішніх шоків і актуалізує потребу в проактивному моніторингу їхньої економічної безпеки.

Таблиця 3.3

Динаміка індикаторів інтеграції цифрових технологій у діяльність підприємств України (2020–2025 рр.), відсотків

№ з/п	Найменування показника цифровізації	2020	2021	2022	2023	2024	2025
1	Частка підприємств із принаймні базовим рівнем цифрової інтенсивності (10–249 осіб)	…	…	…	…	22,2	22,8
2	Частка підприємств, що використовують програмне забезпечення ERP	…	…	5,9	…	15,2	16,7
3	Частка підприємств, що використовують соціальні медіа (загальний показник)	…	…	29,1	…	30	29.3
4	у т.ч. за кількістю використаних соціальних медіа два або більше	…	…	…	…	15,1	…
5	Частка підприємств, що купують послуги хмарних обчислень	…	10,2	9,8	…	13,7	15,9
6	Частка підприємств, що використовують технології штучного інтелекту (ШІ)	…	…	5,4	…	5,2	4,6
7	Частка підприємств, що надсилають рахунки-фактури в електронній формі	39,8	…	…	36,1	…	н/д

Джерело: згруповано автором за даними [26].

Спостерігається стрімке нарощування використання систем управління ресурсами (ERP), частка впровадження яких зросла з 5,9% у 2022 році до 16,7% у 2025 році. Такий стрибок у майже 3 рази свідчить про вимушену дефізикацію управлінських процесів і перехід бізнесу до складних архітектурних рішень. Водночас інтеграція ERP-систем належить до класу CAPEX-орієнтованих інвестицій, які вимивають дефіцитний оборотний капітал компаній. Це прямо підтверджує логіку нашої моделі: у разі падіння індексу фінансово-економічної захищеності ($I_{фез}$>0,69), підприємствам необхідно переорієнтовуватись на хмарні аналоги ERP з сервісною логікою оплати (OPEX).

Динаміка хмарних обчислень демонструє стійкий тренд до зростання з 10,2% у 2021 році до 15,9% у 2025 році. Перехід у хмари є ключовим

драйвером забезпечення цифрової операційної резильєнтності підприємств під час безпекових та інфраструктурних криз. Саме цей показник у нашій моделі виступає технологічним ядром «компенсаторного маневру», дозволяючи компаніям оперативно скорочувати витрати на утримання власних дата-центрів шляхом переходу на сервісну модель (Cloud Native).

Використання технологій штучного інтелекту (ШІ) залишається на низькому і навіть дещо спадаючому рівні: 5,4% у 2022 році та 4,6% у 2025 році. Це свідчить про те, що вітчизняний бізнес використовує цифровізацію переважно для виживання та стабілізації базових процесів, а не для високотехнологічного прориву. Обмеженість впровадження ШІ та соціальних медіа з високою інтенсивністю (лише 15,1% підприємств використовують два або більше медіа у 2024 році) вказує на дефіцит компетенцій та системні фінансові обмеження.

Особливий інтерес викликає показник електронного документообігу (надсилання рахунків-фактур в електронній формі), який у 2020 році становив 39,8%, а у 2023 році – 36,1%. Певне просідання цього індикатора у воєнний період відображає загальну деструкцію бізнес-середовища, релокацію підприємств та втрату контролю над частиною активів.

Таким чином, виявлені статистичні закономірності доводять, що цифрова трансформація українського підприємництва відбувається в умовах жорстких ресурсних обмежень та безпекових загроз. Фрагментарне впровадження технологій (наприклад, ШІ чи соціальних медіа) без комплексного фінансового забезпечення не приносить очікуваного ефекту.

Систематизація статистичних даних підкомпонента «Електронна комерція» наведено в таблиці 3.4.

Таблиця 3.4

Статистичні індикатори розвитку електронної комерції підприємств України (МСП) за даними Державної служби статистики (2020–2024 рр.), відсотків

№ з/п	Найменування аналітичного показника	2020	2021	2022	2023	2024
1	Частка підприємств, що здійснюють електронну торгівлю, у загальній кількості підприємств	4,6	4,7	5,6	6,4	8,2
2	Обсяг реалізованої продукції (товарів, послуг) підприємств, отриманий від електронної торгівлі	3,2	3,3	5,9	2,6	3,8
3	Частка підприємств, що здійснювали електронну торгівлю за місцем розташування клієнтів у державах-членах ЄС та інших іноземних державах	…	…	…	…	1,2

Джерело: згруповано автором за даними [26].

Аналіз динаміки показників за 2020–2024 роки (табл. 3.4) дозволяє розкрити глибинну специфіку реакції вітчизняних підприємств малого та середнього бізнесу на шокові екзогенні трансформації. Спостерігається стійка та безперервна позитивна динаміка залучення суб'єктів господарювання до цифрових каналів збуту. Відповідно до офіційних даних, частка підприємств, що здійснюють електронну торгівлю, зросла з 4,6% у 2020 році до 8,2% у 2024 році. Таке майже двократне зростання індикатора в умовах пандемії та повномасштабної війни доводить, що перехід від традиційних фізичних бізнес-структур до цифрових платформ (про який наголошував колектив авторів під керівництвом О. Ю. Литовченка) є не просто трендом, а безальтернативним способом виживання суб'єктів підприємництва на ринку.

Аналіз обсягів реалізованої продукції, отриманих від електронної торгівлі, виявив унікальну ринкову аномалію. У 2020–2021 роках цей показник демонстрував стабільність (3,2%–3,3%), проте у 2022 році (перший рік повномасштабного вторгнення) зафіксовано його різкий стрибок до 5,9%. Цей феномен пояснюється критичним руйнуванням традиційної логістики та фізичного ритейлу, що змусило споживачів та контрагентів миттєво переорієнтуватися на онлайн-канали. Проте вже у 2023 році відбулося просідання показника до 2,6% із подальшим помірним відновленням до 3,8% у 2024 році. Подібна волатильність доходів від е-комерції свідчить про високу

фінансову турбулентність та нестабільність інтернет-сегменту ринку, що прямо корелює з нашою гіпотезою про необхідність впровадження динамічного моніторингу Інтегрального індексу фінансово-економічної захищеності ($I_{фез}$).

По-третє, найбільш критичним розривом, який стримує довгострокову стійкість українського підприємництва, є показник транскордонної цифрової торгівлі. За даними 2024 року, частка підприємств, що здійснювали електронну торгівлю за місцем розташування клієнтів у державах-членах ЄС та інших країнах, становить усього 1,2%. «Це свідчить про те, що попри укладення Угоди про асоціацію з ЄС та режим «економічного безвізу», український малий та середній бізнес залишається ізольованим у межах внутрішнього цифрового периметру, практично не використовуючи потенціал глобальних маркетплейсів».

Даний незаперечний факт повністю підтверджує наукову позицію С. О. Шута (2024 р.) щодо того, що цифрова трансформація хоч і відкриває унікальні можливості для глобальної експансії, проте потребує значних інвестицій у технологічні рішення та гнучкі управлінські структури, яких наразі бракує вітчизняним компаніям.

Комплексний науково-аналітичний аналіз структури, динаміки та галузевих особливостей капітального інвестування в Україні наведений у таблиці 3.5.

П'ять базових індустріально-аграрних та інфраструктурних секторів акумулюють 60,4% усіх капітальних інвестицій країни. Це свідчить про вимушену концентрацію капіталу на підтриманні життєдіяльності критичної інфраструктури, енергетики та базового виробництва в умовах воєнних ризиків.

Попри те, що в середньому по економіці нематеріальні активи становлять лише 4,86%, аналіз виявив колосальну міжгалузеву асиметрію. Справжніми драйверами цифровізації та діджиталізації бізнес-моделей

виступають сектори J («Інформація та телекомунікації») та K («Фінансова та страхова діяльність»).

Таблиця 3.5

Галузевий розподіл капітальних інвестицій за січень–червень 2025 року

Місце	Сектор КВЕД	Обсяг інвестицій (тис. грн)	Частка у загальному обсязі (%)
1	C – Переробна промисловість	49 084 528	17,52
2	H – Транспорт, складське господарство, поштова діяльність	31 586 787	11,27
3	D – Постачання електроенергії, газу, пари та кондиційованого повітря	30 076 823	10,73
4	A – Сільське господарство, лісове та рибне господарство	29 547 306	10,55
5	B – Добувна промисловість і розроблення кар'єрів	28 937 877	10,33
–	Інші 14 секторів (сукупно)	110 946 748	39,60
–	УСЬОГО	280 180 069	100,00

Джерело: згруповано автором за даними [26].

Якщо згрупувати інвестиції в нематеріальні активи (софт, ліцензії, бази даних), лідерами стають зовсім інші гравці: сектор J (Інформація та телекомунікації): 4 256 419 тис. грн (31,25% від загальнонаціонального обсягу нематеріальних інвестицій); сектор K (Фінанси та страхування): 3 178 493 тис. грн (23,33% від загальнонаціонального обсягу); сектор G (Торгівля та ритейл): 1 861 356 тис. грн (13,66%). Сукупно сектори J та K генерують 54,58% усіх інвестицій країни в нематеріальні активи.

Розглянемо внутрішню частку нематеріальних активів (інтенсивність цифровізації) всередині самих секторів: сектор J (IT та Телеком) має 34,24% усіх інвестицій галузі, спрямованих на нематеріальний капітал, а сектор K (фінанси) – 32,99% інвестицій галузі – на нематеріальні активи. Для порівняння, у переробній промисловості цей показник становить лише 2,23%, а в будівництві – 0,02%.

Сектор J «Інформація та телекомунікації» за перше півріччя 2025 року залучив 12 430 984 тис. грн (4,44% від загальнодержавного обсягу), посівши

9-те місце серед галузей. Проте аналіз його внутрішньої структури (підкласи КВЕД) розкриває важливі деталі:

А. Підсектор 61 – «Телекомунікації (електрозв'язок)»:

- загальний обсяг інвестицій: 10 816 279 тис. грн (87,01% від усього сектору J);
- матеріальні активи: 7 591 405 тис. грн (придбання мережевого обладнання, серверів, базових станцій, заміна пошкодженого обладнання зв'язку);
- нематеріальні активи: 3 224 874 тис. грн, з яких 3 181 211 тис. грн (98,6%) спрямовано виключно на програмне забезпечення та бази даних (білінгові системи, ліцензії на частоти, софт для управління мережами).

Б. Підсектор 62+63 – «Комп'ютерне програмування, консультування та ІТ-послуги»

- загальний обсяг інвестицій: 1 038 487 тис. грн;
- матеріальні інвестиції: 472 310 тис. грн (45,48%);
- нематеріальні інвестиції: 566 177 тис. грн (54,52%), з яких софт та бази даних – 532 820 тис. грн.

Це єдиний великий індустріальний сектор економіки України, де обсяг інвестицій у нематеріальний капітал (софт, інтелектуальну власність) перевищує витрати на матеріальні активи (офіси, залізо, комп'ютери). Це класична ознака чистої економіки знань.

В інвестиційному полі України чітко прослідковуються два паралельних процеси. Перший – «інвестиції виживання та відновлення» у традиційному секторі (A, B, C, D, H), де 97–99% капіталу йде у фізичні об'єкти. Другий – «інвестиції розвитку та цифровізації» у фінансовому та інформаційному секторах (J, K), де третина бюджетів йде на нематеріальні активи (програмне забезпечення).

Дані за перше півріччя 2025 року наочно доводять, що цифрова трансформація українського бізнесу спирається на потужне технологічне плече телекомунікацій (інвестиції підкласу 61 складають понад 10,8 млрд грн)

та фінтеху (сектор К – 9,6 млрд грн). Саме вони створюють інфраструктурний каркас для електронної комерції та використання ERP/хмарних технологій іншими МСП, дані щодо яких аналізувалися у попередніх підрозділах.

Низька частка інвестицій у софт та бази даних у переробній промисловості (2,23%) та будівництві (0,02%) вказує на критичний дефіцит капіталу для автоматизації (Industry 4.0). Вітчизняні промислові підприємства наразі змушені фінансувати виключно первинні фізичні активи, відкладаючи глибоку цифрову модернізацію «на потім». Це підтверджує актуальність розроблених у роботі фінансово-організаційних напрямів для стимулювання інновацій.

Таким чином, зведені емпіричні дані підкомпонентів цифровізації доводять наявність «парадоксу діджиталізації» в Україні: кількість підприємств, що освоюють цифрові інструменти та е-комерцію, зростає (8,2%), проте їхня фінансова віддача (3,8%) та рівень міжнародної експансії (1,2%) залишаються мінімальними.

Головною причиною цього є дефіцит комплексного підходу, за якого модернізація цифрової інфраструктури мала б відбуватися одночасно з оптимізацією кібербезпеки та гнучким маневруванням витратами. Запропонований нами дизайн моделі покликаний подолати цей розрив, надаючи підприємствам алгоритм безпечного виходу на зовнішні цифрові платформи без ризику фінансової дестабілізації.

Спираючись на результати проведеного аналізу капітальних інвестицій, розроблено концептуальний дизайн адаптивної структурно-функціональної моделі розвитку підприємництва в умовах цифрової трансформації.

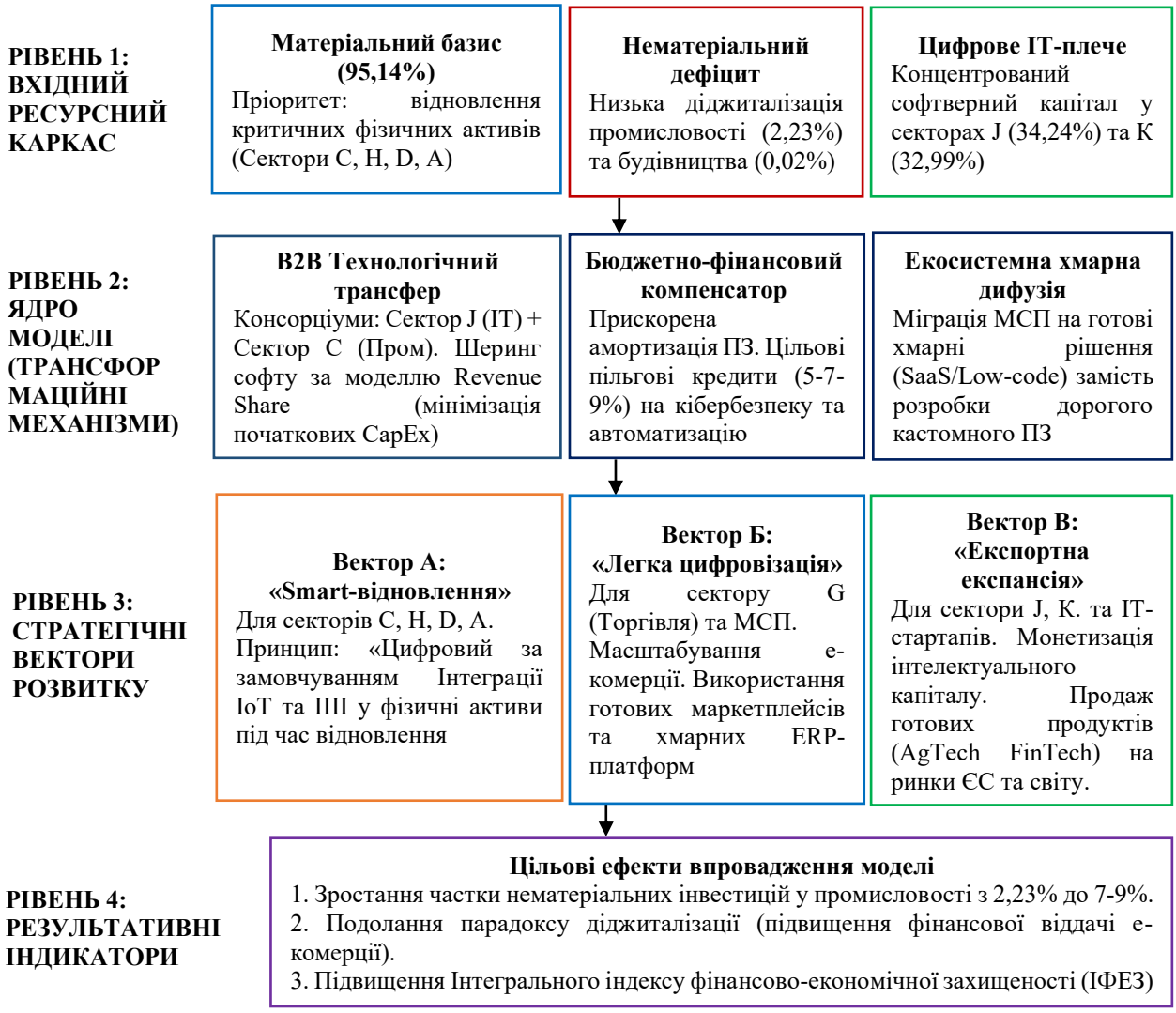


Рис. 3.5. Адаптивна структурно-функціональна модель розвитку підприємництва в умовах цифрової трансформації

Джерело: авторська розробка.

Ця модель спрямована на подолання міжгалузевого цифрового розриву та стимулювання технологічної модернізації реального сектора (промисловості, будівництва, агро) в умовах обмеженого капіталу.

Модель є багаторівневою системою, що поєднує ресурсні можливості, трансформаційні механізми та стратегічні вектори розвитку підприємницьких структур. Перший рівень базовий рівень фіксує поточні макроекономічні реалії, визначені під час аналізу даних Держстату: потреба у першочерговому фінансуванні основних засобів (обладнання, логістика, інженерні споруди) через безпекові ризики та руйнування та обмеженість вільних фінансових

ресурсів у промисловості (сектор C) та будівництві (сектор F) для фінансування класичних IT-проєктів «з нуля» Потужний пропозиційний потенціал вітчизняних секторів J (IT) та K (Фінтех), які мають надлишок експертизи у сфері софту та хмарних рішень.

Другий рівень трансформаційні механізми дозволяє для подолання розриву між потребою в діджиталізації та браком коштів у моделі передбачено три регуляторно-організаційні блоки: механізм технологічного трансферу та абсорбції (B2B-інтеграція), державно-приватне стимулювання та екосистемна платформа хмарної дифузії.

Механізм технологічного трансферу та абсорбції (B2B-інтеграція) враховує формування прямих консорціумів між підприємствами сектору J (IT) та сектору C (переробна промисловість). Замість закупівлі дорогого іноземного ПЗ, модель орієнтує вітчизняний IT-сектор на створення галузевих, гнучких рішень (наприклад, систем автоматизації, ERP/CRM) за моделлю Revenue Share(розподіл прибутку) або довгострокової оренди, що знижує капітальні витрати (CapEx) реального сектора.

Бюджетно-фінансовий компенсатор (державно-приватне стимулювання) базується на впровадженні податкових преференцій на інвестиції в нематеріальні активи для підприємств реального сектора (наприклад, прискорене амортизування витрат на софт та бази даних). Цільове субсидування або пільгове кредитування (в межах програм «5-7-9%») виключно на цифрову модернізацію (впровадження хмарних рішень, кібербезпеки).

Екосистемна платформа хмарної дифузії модель передбачає зміщення фокусу підприємств із побудови власних дата-центрів на інтеграцію в готові хмарні екосистеми (SaaS/IaaS), що дозволяє радикально скоротити витрати.

На третьому рівні формуються стратегічні вектори розвитку підприємницької діяльності реалізується через три взаємопов'язані стратегічні вектори, адаптовані під специфіку кожної групи підприємств:

Вектор А: «Smart-відновлення» для секторів С (Промисловість), Н (Транспорт), D (Енергетика), які зараз здійснюють левову частку матеріальних інвестицій. Заборона на купівлю морально застарілого обладнання. Будь-яка інвестиція у фізичний капітал (машини, верстати, логістичні вузли) має здійснюватися за принципом «Цифровий за замовчуванням» (наявність IoT-датчиків, інтегрованого софту для предиктивного аналізу). Це дозволяє діджиталізувати бізнес у межах стандартного CapEx на матеріальні активи.

Вектор Б: «Легка цифрова інтенсивність» (Cloud-first & Low-code) для малих та середніх підприємств (МСП), торгівлі (Сектор G), сфери послуг. Відмова від розробки кастомного софту. Перехід на використання готових хмарних платформ, маркетплейсів та low-code інструментів. Це дозволяє підприємствам підняти свій Індекс цифрової інтенсивності до базового чи середнього рівня без залучення великих інвестицій.

Вектор В: «Експортно-технологічна експансія» для секторів J (IT), K (фінанси) та високотехнологічних стартапів. Конвертація високої внутрішньої частки нематеріальних інвестицій (понад 34% у секторі J) в експортні продукти. Створення готових програмно-апаратних комплексів (наприклад, AgTech для сектору А або FinTech-модулів) для продажу на зовнішніх ринках з метою залучення валютної виручки в країну.

Четвертий рівень визначає індикатори ефективності та моніторинг для оцінки успішності функціонування моделі використовуються метрики, безпосередньо пов'язані з аналізованою статистикою. Структурний індикатор визначається зростанням частки нематеріальних активів у структурі інвестицій переробної промисловості (цільовий орієнтир: з поточних 2,23% до 7–9% протягом 3 років). Якісний індикатор характеризується збільшенням частки підприємств із базовим та високим рівнем цифрової інтенсивності (групування 10–249 працівників). Економічний індикатор визначається зростанням показника ROI (окупності інвестицій) за рахунок зниження операційних витрат після впровадження хмарних обчислень та ERP.

В умовах кризового дефіциту капіталу та воєнних руйнувань, цифрова трансформація підприємств реального сектора має відбуватися не через ізольовані ІТ-інвестиції, а шляхом гібридизації матеріальних інвестувань (інтеграції софту у фізичні активи під час відновлення) та екосистемного аутсорсингу ІТ-функцій у високорозвинений вітчизняний телеком- та ІТ-сектори. Це перетворює ІТ-галузь України з "ізольованого острова цифрового благополуччя" на внутрішній локомотив модернізації всієї національної економіки.

Для успішної верифікації запропонованої моделі у межах наукового дослідження розроблено детальну методику оцінки ефективності та моніторингу цифрової трансформації підприємств. Вона переводить якісні теоретичні положення у чіткі кількісні метрики та визначає алгоритм їхнього регулярного відстеження. Методика спирається як на макроекономічні дані Державної служби статистики України, так і на мікроекономічні показники внутрішньої звітності підприємств.

1. Математичне формалізування та розрахунок індикаторів

1.1. Структурний індикатор ($S_{intang}^{(c)}$)

Показує рівень інтенсивності капіталізації інтелектуальних та цифрових активів у реальному секторі економіки на прикладі переробної промисловості (Сектор С).

Формула розрахунку:

$$S_{intang}^{(c)} = \frac{I_{intang}^{(c)}}{I_{total}^{(c)}} \times 100\% \quad (3.1)$$

де:

$I_{intang}^{(c)}$ – обсяг капітальних інвестицій у нематеріальні активи сектора С за звітний період (тис. грн);

$I_{total}^{(c)}$ – загальний обсяг капітальних інвестицій сектора С за звітний період (тис. грн).

Базове значення (за І півріччя 2025 року): 2,23% (освоєно 1 093 987 тис. грн нематеріальних інвестицій із загальних 49 084 528 тис. грн).

Цільовий орієнтир досягнення рівня 7–9% протягом 3 років за рахунок дії механізмів B2B-трансферу та фінансових компенсаторів.

1.2. Якісний індикатор (D_{int})

Характеризує масштаби дифузії цифрових технологій серед малих та середніх підприємств (МСП) з чисельністю працівників від 10 до 249 осіб. Рівень цифрової інтенсивності визначається за гармонізованою методологією Євростату (Digital Intensity Index – DII, що містить 12 базових критеріїв, таких як використання ERP, хмарних обчислень, ШІ, швидкісного інтернету тощо).

Формула розрахунку:

$$D_{int} = \frac{N_{basic+}N_{high}}{N_{total}} \times 100\% \quad (3.2)$$

де:

N_{basic} – кількість опитаних підприємств із базовим (4–6 технологій) рівнем цифрової інтенсивності;

N_{high} – кількість підприємств із високим та дуже високим (7–12 технологій) рівнем цифрової інтенсивності;

N_{total} – загальна вибіркова сукупність досліджуваних підприємств у межах моніторингу.

Цільовий орієнтир збільшення частки підприємств із базовим та високим рівнем діджиталізації щонайменше на 15–20% від початкового скринінгу завдяки переходу на модель Cloud-first.

1.3. Економічний індикатор (ROI_{dig})

Відображає реальну фінансову ефективність від цифрової трансформації на рівні конкретного підприємства, нівелюючи «парадокс діджиталізації» через врахування економії операційних витрат (Opex).

Формула розрахунку:

$$ROI_{dig} = \frac{\Delta PR+\Delta OpExsaved-C_{maint}}{Inv_{dig}} \times 100\% \quad (3.3)$$

де:

ΔPR – приріст маржинального прибутку, отриманий безпосередньо через впровадження цифрових каналів (наприклад, запуск e-commerce, вихід на маркетплейси), тис. грн;

$\Delta OpEx_{saved}$ – абсолютне зниження операційних витрат підприємства за рахунок переходу на хмарні обчислення та ERP (економія на утриманні власної IT-інфраструктури, оптимізація логістики, скорочення паперового документообігу, автоматизація рутинних операцій), тис. грн;

C_{maint} – поточні щорічні витрати на підтримку та ліцензування впроваджених цифрових рішень, тис. грн;

Inv_{dig} – первинний обсяг інвестицій (капітальних або стартових операційних підписок) у цифрові інструменти, тис. грн.

Модель вважається успішною, якщо $ROI_{dig} > R_{base}$, де R_{base} – базова рентабельність капіталу підприємства до початку трансформації.

Для систематичного контролю за відхиленнями фактичних показників від цільових розроблено трирівневу матрицю моніторингу (таблиця 3.6).

Таблиця 3.6.

Система моніторингу та періодичність збору даних

Рівень моніторингу	Індикатори, що відстежуються	Періодичність	Джерело інформації (Інструментарій)
Макроекономічний (Стратегічний)	$S_{intang}^{(c)}$(Частка нематеріальних інвестицій у промисловості)	Щоквартально / Щороку	Офіційні звіти Держстату
Мезоекономічний (Галузевий / Регіональний)	D_{int} (Індекс цифрової інтенсивності МСП)	1 раз на рік	Державні статистичні спостереження щодо використання інформаційно-комунікаційних технологій на підприємствах, анкетні опитування ТПП
Мікроекономічний (Внутрішньокорпоративний)	ROI_{dig}, $\Delta OpEx_{saved}$динаміка витрат на софт	Щомісячно / Щоквартально	Дані управлінського та фінансового обліку підприємств, аналітика хмарних платформ (SaaS консолі)

Джерело: запропоновано автором.

Моніторинг не є суто констатуючим елементом – він запускає механізми адаптації моделі:

1. Якщо $S_{intang}^{(c)}$ не зростає сигнал для державних інституцій щодо неефективності діючих податкових компенсаторів. Потрібен перегляд умов пільгового кредитування для ІТ-модернізації.

2. Якщо D_{int} гальмує у секторі МСП свідчить про занадто високий поріг входження. Необхідно посилити блок Екосистемної хмарної дифузії, створюючи безкоштовні державні чи грантові Low-code/No-code шаблони автоматизації бізнесу.

3. Якщо $ROI_{dig} < 0$ на підприємстві сигнал про те, що автоматизація була проведена поверх неефективних, застарілих бізнес-процесів. Потрібно зупинити масштабування системи та провести реінжиніринг процесів (BPR).

Моделювання доводить, що основний економічний ефект цифровізації в сучасних умовах України генерується не стільки прямим зростанням продажів у мережі (що підтверджує дані Державної служби статискики у 3,8% обсягів продажів), скільки оптимізацією операційних витрат ($\Delta OpEx_{saved}$) завдяки хмарам та ERP. Завдяки цьому інтегральний ROI_{dig} сягає 60%, що робить цифровізацію високоефективною навіть у кризовий період.

Таблиця 3.7

Загальна матриця верифікації моделі за наявними даними

Показник методики	Значення за даними Держстату	Стан індикатора	Необхідна дія в межах моделі
$S_{intang}^{(c)}$(Частка софту/активів)	2,23% (2025 р.)	Критичний дефіцит	Запуск податкового компенсатора та прискореної амортизації ПЗ.
D_{int} (Цифрова інтенсивність)	22,8% (2025 р.)	Повільне зростання (+0,6%)	Масштабування екосистемної хмарної дифузії (готовий SaaS).
Використання ШІ (AI)	4,6% (2025 р.)	Регрес (-0,6%)	Впровадження B2B технологічного трансферу (ІТ-сектор + Пром-сть).
Е-комерція (Частка продажів)	3,8% (2024 р.)	Парадокс ефективності	Фокус на зниженні Орех замість агресивного маркетингу.

Джерело: розраховано автором.

Аналіз сформованої матриці верифікації наочно демонструє глибокий структурний дефіцит нематеріального капіталу в реальному секторі економіки України, про що свідчить критично низька частка інвестицій у цифрові активи переробної промисловості (2,23%). Повільна річна динаміка індексу цифрової інтенсивності МСП (+0,6%) на тлі регресу у використанні передових технологій, таких як штучний інтелект (-0,6%), підтверджує, що вітчизняний бізнес наразі фокусується лише на базовому виживанні. Крім того, зафіксований «парадокс е-комерції» доводить неефективність стихійної діджиталізації без глибокої інтеграції хмарних рішень та оптимізації операційних витрат. Це повністю обґрунтовує доцільність впровадження розробленої адаптивної моделі, яка пропонує чіткі інструменти фінансового стимулювання та B2B-трансферу для подолання кризових тенденцій. Таким чином, переорієнтація підприємств на запропоновані стратегічні вектори дозволить трансформувати точкові цифрові витрати у системне зростання показника окупності інвестицій (ROI_{dig}).

Обґрунтовано та емпірично верифіковано адаптивну модель розвитку підприємництва в умовах цифрової трансформації, яка, на відміну від існуючих підходів, інтегрує макроекономічні тренди капіталізації з мікроекономічними важелями ефективності. На основі розробленої автором системи індикаторів та моніторингу зафіксовано глибокі структурні диспропорції у вітчизняному реальному секторі, зокрема критично низьку частку інвестицій у нематеріальні активи переробної промисловості (2,23%) та регрес у використанні передових технологій (ШІ упав до 4,6%). Виявлений «парадокс е-комерції» (зростання кількості онлайн-платформ до 8,2% на тлі низької частки інтернет-продажів у 3,8%) довів, що стихійна цифровізація без оптимізації операційних витрат є неефективною. Доведено, що впровадження запропонованої моделі через механізми B2B-технологічного трансферу, бюджетно-фінансових компенсаторів та екосистемної хмарної дифузії дозволить бізнесу подолати кризові тенденції, забезпечивши високу окупність

цифрових інвестицій (ROI_{dig}на рівні 60%) за рахунок системного зниження операційних витрат.

3.3. Стратегічні засади розвитку підприємницької діяльності в умовах глобальної економічної турбулентності

Формування стратегічних засад розвитку підприємницької діяльності в сучасних реаліях вимагає докорінного перегляду класичних підходів до стратегічного управління. Традиційні статичні моделі, орієнтовані на довгострокове планування стабільних ринкових ніш, втратили свою актуальність через безпрецедентний рівень невизначеності зовнішнього середовища. Як справедливо наголошують Романюк І. А., Гіржева О. М. та Долженко Д. О. [27], стратегічний розвиток конкурентоспроможності українських підприємств у глобальному середовищі потребує комплексного підходу та узгоджених дій бізнесу й держави. Сучасні виклики екзогенного характеру — воєнні дії, руйнування критичної інфраструктури, скорочення виробничих потужностей, логістичні блокади та втрата традиційних ринків збуту й сировинних ресурсів — істотно послабили фінансово-економічні позиції багатьох компаній.

За таких умов методологічним фундаментом стратегії підприємництва має стати концепція динамічних спроможностей (Dynamic Capabilities). Вона передбачає здатність суб'єктів господарювання безперервно розпізнавати загрози та можливості, реконфігурувати власну ресурсну базу та трансформувати бізнес-моделі під впливом цифрових технологій. Водночас приклади адаптації вітчизняного бізнесу та його часткового відновлення чітко свідчать про наявність суттєвого внутрішнього потенціалу до зростання. Ключовими чинниками забезпечення конкурентоспроможності в цифровій епосі виступають інноваційність, гнучкість архітектури бізнес-процесів і якісний людський капітал.

Важливість розроблення стратегічних векторів розвитку підприємницької діяльності в умовах цифрової трансформації полягає у переході від стихійного, фрагментарного впровадження технологій до формування системної архітектури бізнесу, здатної адаптуватися до глобальних викликів. Обґрунтування чітких стратегічних орієнтирів є критично необхідним для подолання виявленого нами «парадокса діджиталізації», коли зростання присутності МСП в е-комерції до 8,2% супроводжується реальним падінням обсягів інтернет-продажів до 3,8%. Формування диференційованих векторів розвитку, таких як «Smart-відновлення» промисловості, дозволяє ліквідувати загрозливий структурний дефіцит нематеріального капіталу в секторі С, де на діджитал-софт припадає лише 1,26% від усіх капіталовкладень. Наявність стратегічної карти забезпечує раціональний розподіл дефіцитних фінансових ресурсів малих та середніх підприємств за рахунок пріоритетного переходу на готові хмарні SaaS-платформи замість кастомної розробки, що нівелює високі стартові капітальні витрати. Крім того, чітко артикульовані вектори інтеграції у європейський простір дають змогу розширити критично низьку частку вітчизняних суб'єктів господарювання, які наразі торгують із країнами ЄС (всього 1,2%). Зрештою, розроблення таких стратегічних засад створює інституційний місток для синхронізації дій бізнесу та держави, спрямовуючи державні податкові компенсатори та програми пільгового кредитування безпосередньо на підвищення інтегрального показника окупності цифрових інвестицій.

Спираючись на результати емпіричної верифікації та структурно-логічну архітектуру побудованої адаптивної моделі, стратегічні засади розвитку підприємств мають бути диференційовані за трьома взаємопов'язаними векторами. Це дозволить уникнути уніфікації управлінських рішень та врахувати галузеву специфіку капіталомісткості й поточний рівень діджиталізації бізнесу.

Вектор А: «Smart-відновлення капіталомістких галузей». Цей вектор орієнтований на сектори економіки з високою питомою вагою матеріальних основних засобів, але критично низьким рівнем інвестування у цифрові активи (переробна промисловість — Сектор С, будівництво — Сектор F, сільське господарство — Сектор А). Розрахунок структури капітальних інвестицій промисловості за перше півріччя 2025 року показав, що на фоні потужних інвестицій у матеріальну базу (понад 49 млрд грн у Секторі С), питома вага нематеріальних активів становить лише 2,23%, а безпосередньо програмного забезпечення — 1,26%.

Стратегічне завдання цього вектора полягає у впровадженні принципу «Цифровий за замовчуванням» під час фізичної релокації, модернізації або повного відновлення виробничих потужностей. Будь-яка закупівля нового технологічного обладнання, верстатів чи побудова логістичних комплексів має супроводжуватися одночасним розгортанням цифрових систем управління. Це передбачає:

- інтеграцію датчиків промислового інтернету речей (IIoT) для моніторингу зносу обладнання в реальному часі та переходу до предиктивного обслуговування;
- впровадження цифрових двійників (Digital Twins) виробничих ліній для оптимізації витрат сировини та енергоресурсівж
- пряме підключення виробничих потужностей до автоматизованих систем управління ресурсами (MES та ERP).

Математичне моделювання підтверджує, що впровадження Вектора А дозволяє максимізувати показник не за рахунок миттєвого збільшення ринкових обсягів збуту, а шляхом радикального скорочення внутрішніх втрат і операційних витрат.

Вектор Б: «Екосистемна хмарна дифузія та оптимізація електронного бізнесу». Цей напрям є базовим для сектору малого та середнього підприємництва (із чисельністю зайнятих 10–249 осіб), а також для підприємств сфери торгівлі та послуг (сектор G). Офіційна статистика

зафіксувала стагнацію інтегрального індексу цифрової інтенсивності МСП на рівні 22,8% у 2025 році. При цьому спостерігається явний структурний розрив: бізнес активно реєструється на цифрових майданчиках (ріст суб'єктів е-комерції до 8,2%), але не отримує від цього очікуваної фінансової віддачі (частка інтернет-доходів упала до 3,8%).

Стратегія «хмарної дифузії» покликана ліквідувати цей розрив шляхом системної трансформації внутрішнього менеджменту:

- МСП мають відмовитися від капіталомістких ІТ-проєктів «з нуля» на користь готових хмарних SaaS-рішень (Software as a Service) та No-code-платформ. Це дозволяє перевести витрати з категорії великих капітальних у категорію гнучких операційних підписок, суттєво знижуючи поріг цифровізації.

- Замість ізольованого використання інтернет-магазинів чи соціальних медіа (які використовують 29,3% компаній), стратегія вимагає їхньої жорсткої інтеграції з хмарними ERP- та CRM-системами. Лише автоматичний обмін даними між замовленням на сайті, складом, бухгалтерією та службою доставки дозволяє усунути людський фактор, прискорити оборотність оборотних коштів та подолати «парадокс діджиталізації».

Вектор В: «Експортна експансія та високотехнологічний B2B-трансфер». Орієнтований на високотехнологічні сегменти української економіки: ІТ-сектор (Сектор J), фінансову діяльність (Сектор K) та інноваційні наукомісткі стартапи. Особливу роль тут відіграє ІТ-сектор, який, за визначенням Романюк І. А. та колег, демонструє унікальну життєздатність та здатність до зростання навіть під час глибокої системної кризи, виступаючи орієнтиром та локомотивом для решти галузей господарства.

Стратегічна сутність цього вектора розгортається у двох напрямах:

1. Зовнішній вектор. Подолання бар'єру ізоляції та вихід на ринки Європейського Союзу. Поточний показник Держстату, згідно з яким лише 1,2% українських підприємств здійснюють транскордонну електронну торгівлю з країнами ЄС, є незадовільним. Стратегія передбачає сертифікацію

українських цифрових продуктів за стандартами GDPR, інтеграцію в європейські цифрові ланцюги створення вартості та масштабування рішень у сферах FinTech, AgTech, GovTech та MilitaryTech.

2. Внутрішній вектор. Створення консорціумів між національними IT-компаніями та вітчизняними індустріальними підприємствами. Замість аутсорсингу на західні ринки, IT-сектор має здійснювати трансфер технологій всередину країни, адаптуючи складні рішення (наприклад, ШІ, використання якого в Україні знизилося до 4,6%) під потреби локальної промисловості на умовах шерингу або розподілу майбутніх прибутків (Revenue Share).

Дослідження стратегічних засад забезпечення інноваційної конкурентоспроможності підприємств в умовах перманентних технологічних шоків потребує глибокого аналізу еволюції поглядів на категорію адаптації, яка пройшла тривалий шлях трансформації від біологічної аналогії до складної управлінської доктрини. Як обґрунтовано доводить Джерелюк Ю. О. та Попович Н. Н. [28], у межах сучасного стратегічного менеджменту доцільно виокремити три засадничі підходи, що сформували методологічний фундамент розуміння адаптивних процесів в економічних системах. Саме ретроспективний та системний аналіз цих підходів дозволяє розкрити внутрішні пружини цифровізації вітчизняного бізнесу та пояснити природу відхилень між теоретичними моделями та емпіричною реальністю.

Рис. 3.6. Методологічні підходи до адоптації в економіці

Джерело: згруповано автором [28].

Ресурсно-орієнтований підхід до адаптації розглядає адаптацію через призму внутрішньої ресурсної архітектури підприємства. Конкурентоспроможність у межах цієї парадигми забезпечується володінням унікальними, важковідтворюваними та специфічними активами (VRIN-критерії). В умовах четвертої промислової революції ключовим ресурсом стає цифровий та нематеріальний капітал.

Проте, дослідження структури капітальних інвестицій у першому півріччі 2025 року виявило глибокий деструктивний розрив у межах ресурсної парадигми вітчизняних підприємств. У капіталомісткому переробній промисловості зафіксовано катастрофічно низьку частку інвестицій у нематеріальні активи — всього 2,23% від загального обсягу капіталовкладень, а безпосередньо у програмне забезпечення та бази даних — всього 1,26%. Це свідчить про те, що класичний ресурсно-орієнтований підхід в Україні заблокований хронічним інвестиційним голодом реального сектору, який продовжує спрямовувати 97,77% ресурсів виключно на підтримання фізично зношеного матеріального капіталу (будівлі, машини, верстати), ігноруючи інноваційні фактори розвитку.

Реактивно-ситуативний (екологічний) підхід трактує адаптацію як вимушену, пасивну реакцію підприємства на агресивні та непередбачувані зміни кон'юнктури ринку (принцип «пристосуйся або помри»). Спираючись на висновки Романюк І. А., Гіржевої О. М. та Долженка Д. О. (2025), сучасні виклики у вигляді воєнних дій, фізичного знищення інфраструктури та втрати традиційних ресурсів змусили бізнес діяти за логікою негайного виживання. Державні програми релокації, пільгового кредитування та експортного стимулювання частково компенсували ці шоки, проте реактивний характер дій зумовив появу диспропорцій.

Яскравим емпіричним підтвердженням вад суто реактивного підходу є зафіксований нами «парадокс електронної комерції». Згідно з даними Держстату, у 2024 році частка підприємств МСП (10–249 працівників), що здійснюють електронну торгівлю, стрімко зросла до 8,2% (проти 4,6% у 2020

році). Це була типова реактивна адаптація — бізнес рятувався від закриття фізичних магазинів виходом в онлайн. Однак через брак стратегічного планування та наскрізної автоматизації процесів, обсяг реалізованої через інтернет продукції впав до 3,8% (у 2022 році він становив 5,9%, а в 2023 — 2,6%). Стихійне підключення до маркетплейсів без перебудови логістики та управління витратами призвело до розпорошення капіталу та зниження загальної ефективності.

Проактивно-системний підхід є найбільш прогресивним і покладений в основу розробленої нами Адаптивної моделі, розглядає адаптацію як безперервний, проактивний процес трансформації бізнес-системи, спрямований на випередження ринкових трендів і формування нових конкурентних переваг. Тут підприємство не просто реагує на кризу, а використовує цифрові технології для перебудови галузевих правил гри, створення нових ринкових ніш та оптимізації операційної архітектури.

Перехід до проактивної доктрини вимагає від менеджменту чіткого розуміння технологічних трендів. Проведений аналіз використання специфічних ІКТ-інструментів демонструє суперечливі тенденції з одного боку, спостерігається стійке проактивне зростання попиту на послуги хмарних обчислень (Cloud Computing) — з 10,2% у 2021 році до 15,9% у 2025 році, що вказує на формування екосистемного мислення у бізнесу. З іншого боку, зафіксовано небезпечний регрес у сфері впровадження технологій штучного інтелекту (AI) — падіння з 5,4% у 2022 році до 4,6% у 2025 році.

Це доводить, що проактивна адаптація українських підприємств наразі перебуває на початковій стадії («хмарна дифузія») і ще не досягла рівня глибокої інтелектуалізації процесів. Бізнес навчився переносити дані в хмари для безпеки, але ще не готовий масово делегувати аналітику алгоритмам штучного інтелекту.

Запропонована адаптивна модель розвитку підприємництва покликана здійснити теоретичну та практичну конвергенцію трьох виокремлених

Джерелюк Ю. О. та Попович Н. Н. [28] підходів та колективу авторів [29-30], трансформуючи їх у дієвий управлінський інструментарій.

Від ресурсного підходу модель переймає орієнтир на нарощування інноваційної вартості нематеріальних активів. Цільовим стратегічним завданням визначено підвищення частки діджитал-інвестицій у переробній промисловості з поточних 2,23% до 7–9% шляхом впровадження податкових стимулів (прискореної амортизації ПЗ).

У реактивному підході береться до уваги фактор швидкого реагування на безпекові ризики. Модель пропонує алгоритми негайної релокації цифрових потужностей у хмарне середовище та захисту корпоративних баз даних, що актуально в умовах воєнного стану.

Від проактивного підходу модель імпортує філософію довгострокової конкурентоспроможності. Вона орієнтує підприємства МСП на подолання «парадоксу е-комерції» не через збільшення кількості онлайн-вітрин, а через жорстку інтеграцію інтернет-каналів із хмарними ERP- та CRM-системами (показник використання ERP у 2025 році зріс до 16,7%, що є позитивним сигналом).

Математичним критерієм успішності такої триади у моделі виступає максимізація показника інтегральної окупності цифрових інвестицій (ROI_{dig}):

$$ROI_{dig} = \frac{\Delta Revenue_{dig} + \Delta OpEx_{saved}}{CapEx_{dig}} \rightarrow max \qquad (3.4)$$

де:

$\Delta Revenue_{dig}$— додатковий приріст чистого доходу від оптимізованих цифрових каналів продажів;

$\Delta OpEx_{saved}$— економія операційних витрат внаслідок впровадження хмарних систем автоматизації та усунення дублюючих процесів;

$CapEx_{dig}$— первинні капіталовкладення в придбання та розгортання цифрових інструментів.

Застосування готових рішень класу SaaS та Low-code (Вектор Б стратегії) дозволяє мінімізувати знаменник цієї формули ($CapEx_{dig}$),

забезпечуючи високу норму окупності навіть за обмежених фінансових можливостей підприємств МСП у кризовий період.

Сучасна конкурентоспроможність підприємства не може базуватися виключно на пасивному пристосуванні до зовнішніх шоків або на ізольованому накопиченні фізичних засобів виробництва. Перехід до складної управлінської доктрини вимагає системної інтеграції ресурсного, реактивного та проактивного підходів. Сформована на цих засадах адаптивна модель дозволяє вітчизняному бізнесу подолати виявлені структурні деформації — подолати інвестиційний дефіцит у сфері нематеріального капіталу промисловості та ліквідувати «парадокс електронної комерції». Це перетворює цифровізацію з хаотичної статті витрат на керований стратегічний драйвер довгострокового інноваційного зростання.

Орієнтовна схема стратегій цифрової трансформації для сектору малого підприємництва наведена на рис. 3.6.

Згідно з розробленою та верифікованою адаптивною моделлю, на національному рівні державна політика має відійти від уніфікованого (лінійного) підходу до діджиталізації та зосередитися на формуванні трьох стратегічних векторів цифрової трансформації. Кожен вектор жорстко прив'язаний до виявлених деструктивних тенденцій у статистичних даних Держстату та орієнтований на специфічні потреби різних секторів економіки.

Наведено розгорнутий опис функціонування цих векторів на загальнодержавному рівні.

1. Вектор структуризації цифрового капіталу (вектор «А»). Цей вектор спрямований на капіталомісткі базові галузі економіки (насамперед Переробну промисловість — Сектор С, АПК — Сектор А, та Будівництво — Сектор F). На національному рівні його завданням є подолання глибокого інвестиційного перекосу.

Вітчизняний індустріальний бізнес інвестує величезні кошти у матеріальні активи, але катастрофічно ігнорує цифрову складову. Частка

інвестицій у програмне забезпечення та бази даних у структурі промислових капіталовкладень становить мізерні 1,26%.

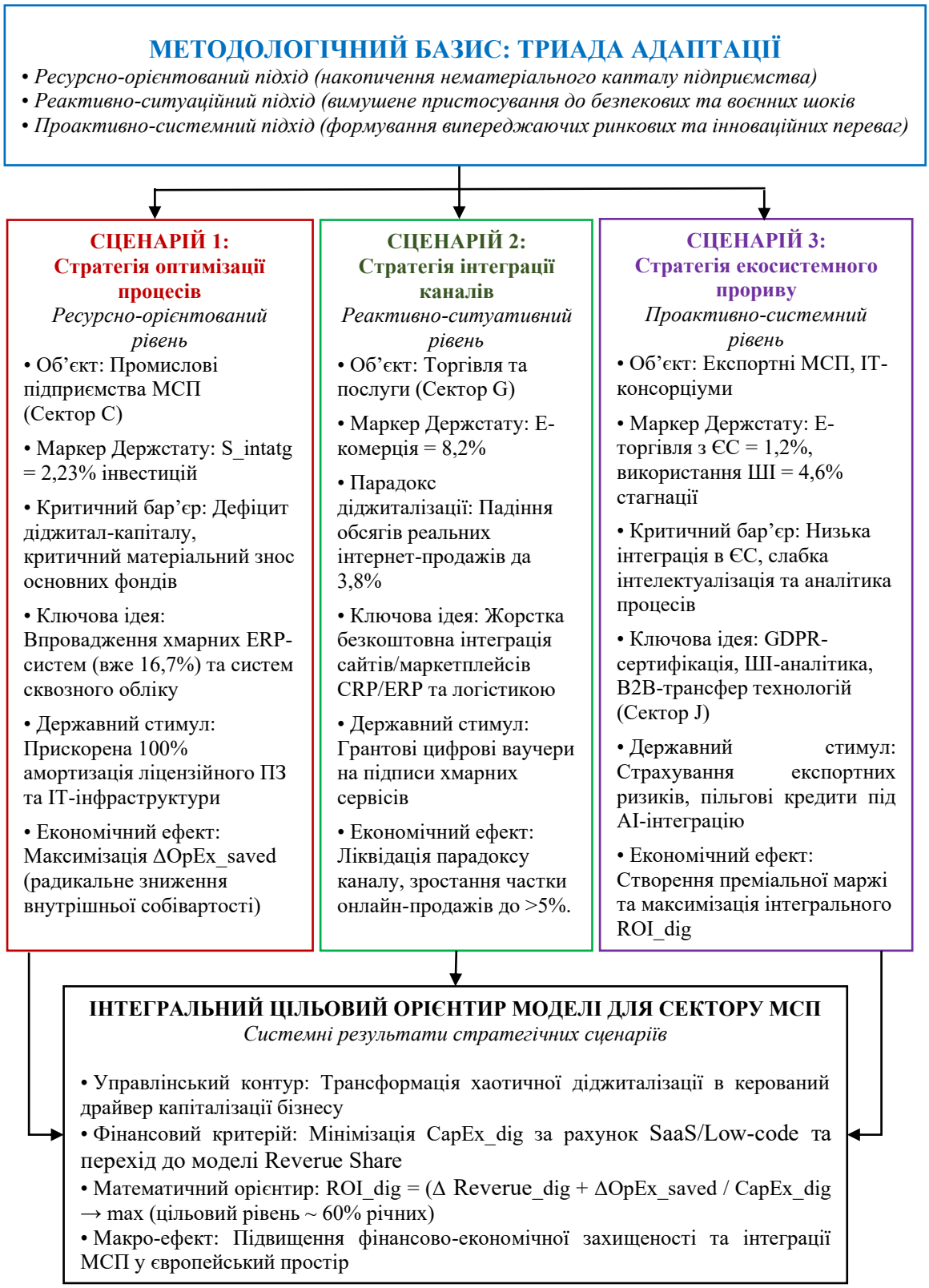


Рис. 3.7. Орієнтовані складові стратегії цифрової трансформації для сектору малого підприємництва

Джерело: запропоновано автором

Впровадження на національному рівні принципу «Цифровий за замовчуванням». Держава має стимулювати підприємства через податкові компенсатори: надати право на прискорену 100%-ву амортизацію витрат на купівлю та розгортання промислового софту (ERP, MES, PLM-систем) у перший же рік.

Цільовий орієнтир — підняти частку нематеріальних інвестицій у промисловості з поточних 2,23% до цільових 7–9%, що забезпечить інтеграцію фізичного обладнання з хмарними технологіями.

2. Вектор екосистемної хмарної дифузії (вектор «Б»). Цей вектор орієнтований на сектор малого та середнього підприємництва (МСП з чисельністю 10–249 працівників) та сферу торгівлі й послуг (Сектор G). Його мета на національному рівні — подолання стагнації цифрової інтенсивності та виправлення ринкових асиметрій.

Модель чітко зафіксувала «парадокс електронної комерції». Суб'єкти МСП масово вийшли в онлайн (присутність в е-комерції зросла до 8,2%), але реальні доходи від інтернет-продажів обвалилися до 3,8%. Це свідчить про хаотичність процесу. Інтегральний індекс цифрової інтенсивності МСП застряг на позначці 22,8%.

Запуск національної програми «Цифрових хмарних ваучерів» (Cloud Vouchers) за підтримки міжнародних донорів. Держава має субсидувати до 80% вартості перших 12–24 місяців підписки на готові хмарні SaaS-платформи (CRM, автоматизований складський та бухгалтерський облік) для МСП. Це зніме з бізнесу тягар великих початкових капітальних витрат, перевівши їх у гнучкі операційні витрати.

Цільовий орієнтир — подолати «парадокс е-комерції» за рахунок наскрізної автоматизації внутрішніх процесів та підняти національний індекс цифрової інтенсивності МСП вище 40% (відповідно до стандартів Digital Compass ЄС).

3. Вектор інтелектуалізації та технологічного трансферу (вектор «B»). Цей вектор використовує потенціал високотехнологічних секторів IT (Сектор J) та фінансової діяльності (Сектор K), як локомотив для всієї національної економіки, а також фокусується на євроінтеграції.

Спостерігається небезпечний регрес у впровадженні передових технологій: рівень використання штучного інтелекту (AI) українським бізнесом упав до 4,6%. Крім того, зафіксовано вкрай низьку інтеграцію в єдиний цифровий ринок ЄС — лише 1,2% вітчизняних підприємств здійснюють транскордонну електронну торгівлю з європейськими контрагентами.

Державний механізм реалізації:

1. Внутрішній трансфер. Стимулювання створення національних консорціумів «IT + Промисловість». Держава може надавати гранти та пільгові кредити під спільні проекти, де вітчизняний IT-сектор розробляє та впроваджує рішення на основі AI, Big Data та кібербезпеки безпосередньо для українських заводів та агрохолдингів на умовах розподілу прибутків (Revenue Share).

2. Зовнішній трансфер. Національна програма підтримки цифрового експорту, яка включає субсидування GDPR-сертифікації для МСП, адаптацію е-митниці та безшовну інтеграцію українських компаній у європейські B2B-платформи.

Цільовий орієнтир зупинити регрес у сфері високих технологій та наростити частку підприємств, які експортують продукцію через цифрові канали до ЄС, щонайменше до 5%.

Проведені дослідження підтвердили, що створення якісно нових моделей управління малого підприємництва та відповідних цифрових систем потребує реінжинірингу діючих аналогових моделей на інноваційних засадах.

Конструювання принципово нової системи управління бізнес-процесами є тим стрижневим елементом, який дозволяє малому підприємництву вийти з пастки хаотичної діджиталізації та перейти до фази

системного інноваційного зростання. Старі лінійні підходи, де кожен підрозділ чи канал продажів існував ізольовано, в сучасних реаліях лише мультиплікують операційні збитки. На рис. 3.8. наведено інтегровану модель розвитку підприємницької діяльності в умовах цифрової трансформації.

Інтегрована модель розвитку підприємницької діяльності в умовах цифрової трансформації не просто фіксує послідовність операцій, а визначає роль, місце та взаємозв'язок бізнес-процесів підприємництва у контексті впливу управлінського чинника. Саме управлінський чинник виступає тим інтегруючим і спрямовуючим вектором, який перетворює розрізнені технологічні та фінансові ресурси на єдину, високоадаптивну систему.

Особливістю моделі є те, що вона поєднує бізнес-процеси управління з операційними та технологічними процесами підприємства в єдиний синергетичний контур. Це дозволяє подолати традиційний розрив, коли стратегічні рішення топменеджменту існують ізольовано від повсякденної цифрової та виробничої практики компанії.

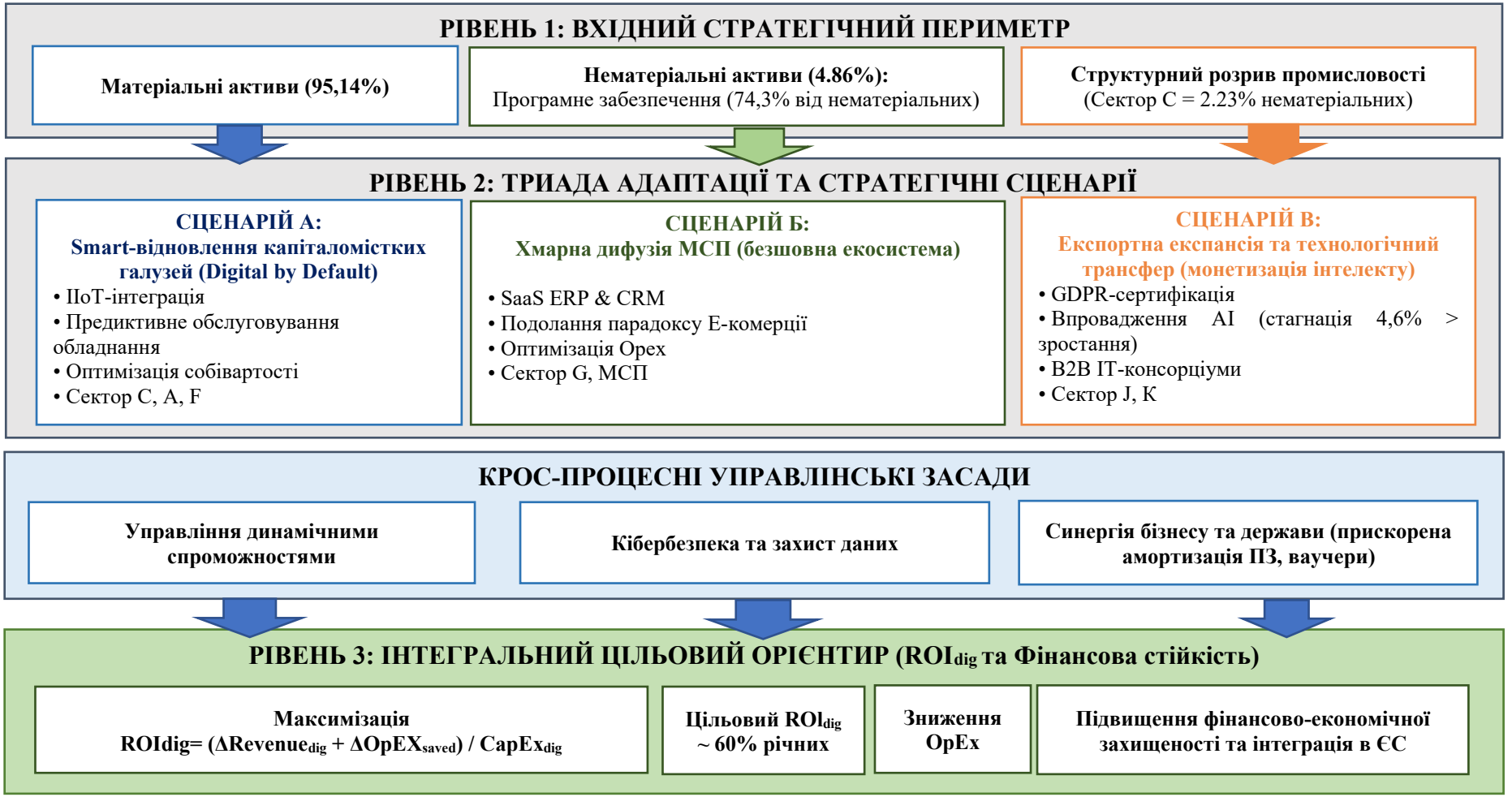


Рис. 3.7. Інтегрована модель розвитку підприємницької діяльності в умовах цифрової трансформації

Джерело: авторська розробка

У межах інтегрованої моделі ця комбінація реалізується через кілька специфічних особливостей:

1. Модель не просто декларує необхідність автоматизації, а безпосередньо пов'язує процеси прийняття рішень на основі даних Державної служби статистки (Рівень 1) із щоденними технологічними операціями (Рівень 2). Управління динамічними спроможностями стає не абстрактною теорією, а щоденним процесом моніторингу ефективності обладнання чи аналітики онлайн-продажів.

2. Бізнес-процеси управління IT-інфраструктурою (закупівля ліцензій, міграція в хмари, налаштування CRM) жорстко підпорядковані управлінню фінансовою стійкістю (Рівень 3). Модель блокує капіталомісткі витрати, якщо вони не ведуть до негайного крос-процесного зниження операційних витрат або прямого приросту маржинального доходу.

3. Особливістю системи є те, що процеси внутрішнього управління (наприклад, контур кібербезпеки та захисту даних) безпосередньо взаємодіють із зовнішніми державними регуляторами й програмами. Менеджмент одночасно управляє ризиками та інтегрує у внутрішні процеси зовнішні стимули — програми пільгового кредитування, прискорену амортизацію програмного забезпечення чи державні цифрові ваучери.

Головна управлінська перевага це поєднання різнорідних процесів, модель трансформує управління діджиталізацією з хаотичного та ризикованого IT-проєкту на передбачуваний, системний процес капіталізації малого й середнього бізнесу з чітко прорахованим показником (ROI_{dig}).

Від сумарної ефективності бізнес-процесів на кожному окремому підприємстві безпосередньо залежить не лише його локальна життєздатність, а й загальнонаціональний рівень економічної стійкості, темпи євроінтеграції та динаміка подолання наслідків системної кризи. Мале та середнє підприємництво (МСП) виступає базовим фундаментом економіки, тому кумулятивний ефект від оптимізації процесів на мікрорівні трансформується у масштабні макроекономічні зрушення.

У контексті інтегрованої моделі цей синергетичний зв'язок розгортається у кількох ключових вимірах:

1. Перехід від мікроефективності до галузевої конкурентоспроможності. Коли окремо взяті підприємства переробної промисловості (Сектор C) починають проактивно впроваджувати сценарій «Smart-Відновлення» і піднімати рівень інвестицій у діджитал-активи з поточних мізерних 2,23%, сумарний ефект ліквідує структурний дефіцит нематеріального капіталу в масштабах усієї країни. Автоматизація процесів на кожному заводі знижує внутрішню собівартість продукції, що підвищує конкурентоспроможність українських товарів на глобальному ринку.

2. Масштабне подолання ринкових асиметрій та парадоксів. Сумарне підвищення процесної ефективності у сфері торгівлі та послуг (Сектор G) дозволяє на загальнодержавному рівні розв'язати «парадокс е-комерції». Якщо кожне МСП відмовиться від хаотичного розгортання ізольованих онлайн-вітрин і перейде до безшовного управління процесами через хмарні SaaS ERP та CRM-системи, національний показник інтернет-продажів вийде із поточної стагнації у 3,8% і продемонструє стрімке зростання. Як результат, інтегральний індекс цифрової інтенсивності вітчизняного бізнесу подолає бар'єр у 22,8% і наблизиться до європейського цільового орієнтиру (>40%).

3. Кумулятивна монетизація інтелектуального капіталу та євроінтеграція

Вихід кожного окремого підприємства на рівень проактивного управління процесами (із впровадженням AI-аналітики та обов'язковою GDPR-сертифікацією) створює критичну масу бізнесів, готових до безбар'єрної роботи на єдиному цифровому ринку ЄС. Це дозволяє радикально масштабувати поточний незадовільний показник транскордонної торгівлі (де лише 1,2% компаній торгують з ЄС) та перетворити національний IT-сектор на реального технологічного донора для традиційних галузей через B2B-трансфер технологій.

4. Фінансова стійкість національної економіки через макро-фільтр ROI.

Математичний критерій ефективності бізнес-процесів інтегрованої моделі наочно демонструє цей наскрізний зв'язок:

$$\mathrm{ROI}_{\mathrm{dig}}=\frac{\Delta Revenue_{dig}+\Delta OpEx_{saved}}{CapEx_{dig}} \rightarrow 60\% \qquad (3.5)$$

Коли тисячі суб'єктів МСП одночасно оптимізують свої операційні витрати ($\Delta OpEx_{saved}$) та максимізують прибутки, держава отримує колосальний приріст капіталізації реального сектору, підвищення фінансово-економічної захищеності та успішну безбар'єрну інтеграцію українського бізнесу в єдиний цифровий простір Європейського Союзу.

Таким чином, сумарна ефективність бізнес-процесів на кожному підприємстві є тією рушійною силою, яка трансформує точкові діджитал-витрати окремого бізнесу в системне макроекономічне зростання. Державна політика, підтримуючи індивідуальну процесну стійкість підприємств через цифрові ваучери та пільгові кредити, автоматично забезпечує високий рівень фінансово-економічної захищеності та інноваційного прориву всієї національної системи.

Отже, комплексний стратегічний підхід до процесів цифрової трансформації об'єднує в єдину систему методологічну доктрину адаптації, емпіричні дослідження, трирівневу модель бізнес-процесів та вектори державної підтримки. Такий підхід дозволяє трансформувати діджиталізацію з хаотичного ІТ-інструменту на керовану архітектуру розвитку малого та середнього підприємництва. Таким чином, розроблені стратегічні засади та інтегрована модель бізнес-процесів доводять, що цифрова трансформація є не просто заміною аналогових інструментів цифровими, а повноцінною управлінською доктриною проактивної адаптації. Саме такий комплексний підхід перетворює виклики кризового періоду на стратегічні драйвери довгострокового конкурентоспроможного розвитку підприємництва на глобальному ринку.

Висновки до розділу 3

У третьому розділі дисертаційного дослідження проаналізовано Європейський досвід забезпечення інформаційної безпеки підприємницької діяльності та шляхи його імплементації у вітчизняних реаліях, розроблено дизайн адаптивної моделі розвитку підприємницької діяльності в умовах цифрової трансформації, сформовано стратегічні засади розвитку підприємницької діяльності в умовах цифрової трансформації. За результатами проведених досліджень, зроблено наступні висновки:

1. Узагальнено зарубіжний досвід цифрової трансформації та визначено орієнтири для вітчизняного бізнесу. Аналіз світових практик, зокрема стратегічних ініціатив Європейського Союзу (Digital Compass ЄС), свідчить, що успішна діджиталізація на макро- та мікрорівнях базується на жорсткому дотриманні цільових індикаторів цифрової інтенсивності, безпеки та інклюзивності. Зарубіжний досвід доводить, що перехід до індустрії 4.0 та 5.0 можливий лише за умови переведення IT-витрат з капітальних у гнучкі операційні за допомогою розвиненого ринку хмарних сервісів та державної ваучерної підтримки МСП. Для України імплементація європейських стандартів (зокрема GDPR та директив е-комерції) є не просто технічною вимогою, а базовою передумовою подолання бар'єру цифрової ізоляції та виходу вітчизняних підприємств на міжнародні ринки збуту.

2. Обґрунтовано теоретико-методологічну сутність та архітектуру розробленої адаптивної моделі. Запропонована модель розглядається як динамічний управлінський інструмент, що забезпечує безперервну реконфігурацію бізнес-процесів у відповідь на екзогенні шоки. На відміну від статичних аналогів, адаптивна модель базується на принципі зворотного зв'язку: вона акумулює вхідні деформації ресурсного периметра (Рівень 1), пропускає їх через аналітичні фільтри крос-процесних управлінських засад (Рівень 2) та трансформує у гнучкі стратегічні сценарії. Головна перевага моделі полягає в її здатності нівелювати інвестиційні ризики малого та середнього підприємництва у кризовий період, пропонуючи безшовну

екосистемну інтеграцію процесів та орієнтуючи бізнес на досягнення високої норми окупності цифрових інвестицій. Таким чином, модель виступає практичним містком для конвергенції інноваційного потенціалу компаній та інституційних стимулів держави.

3. Обґрунтовано імператив переходу від реактивного виживання до проактивно-системної доктрини адаптації. Доведено, що в умовах безпрецедентних безпекових, інфраструктурних та економічних шоків традиційні статичні моделі управління втратили свою ефективність. На основі аналізу еволюції поглядів на категорію адаптації встановлено, що забезпечення інноваційної конкурентоспроможності підприємств потребує інтеграції ресурсно-орієнтованого, реактивного та проактивного підходів. Це дозволяє трансформувати діджиталізацію з хаотичного IT-інструменту на керовану архітектуру динамічних спроможностей бізнесу.

4. Виявлено та статистично верифіковано ключові структурні диспропорції в цифровізації вітчизняного бізнесу. Розрахунки на основі офіційних даних Державної служби статистики України підтвердили наявність двох критичних бар'єрів розвитку. По-перше, зафіксовано глибокий інвестиційний дефіцит у сфері нематеріального капіталу капіталомістких галузей (у Секторі С на програмне забезпечення припадає лише 1,26% від усіх капіталовкладень). По-друге, ідентифіковано «парадокс електронної комерції» в секторі МСП (Сектор G), де стрімке зростання онлайн-присутності підприємств до 8,2% супроводжується реальним падінням обсягів інтернет-продажів до 3,8%, що доводить неефективність стихійної діджиталізації без наскрізної автоматизації процесів.Розроблено диференційовану триаду стратегічних векторів цифрової трансформації на національному рівні. Для уникнення лінійних підходів запропоновано три цільові сценарії: Вектор А («Smart-Відновлення») — реалізує принцип Digital by Default для промисловості, будівництва та АПК шляхом інтеграції IIoT та ERP у фізичний капітал; Вектор Б («Хмарна дифузія») — забезпечує подолання «парадоксу е-комерції» для МСП через міграцію на готові хмарні SaaS-рішення,

мінімізуючи стартовий; Вектор В («Експортна експансія та B2B-трансфер») спрямований на монетизацію інтелектуального капіталу IT-сектору (Сектор J), впровадження AI-технологій (падіння яких зафіксовано на рівні 4,6%) та розширення транскордонної торгівлі з ЄС (поточний рівень — мізерні 1,2%).

5. Сконструйовано та візуалізовано інтегровану адаптивну модель бізнес-процесів підприємницької діяльності. Особливістю моделі є те, що вона поєднує бізнес-процеси управління з операційними та технологічними процесами підприємства в єдиний синергетичний контур під впливом управлінського чинника. Модель працює на тлі крос-процесних засад (кібербезпека, динамічні спроможності) та зв'язує вхідні деформації ресурсів (Рівень 1) через диференційовані сценарії (Рівень 2) із жорстким фінансовим критерієм окупності інвестицій (Рівень 3).

6. Доведено, що сумарна ефективність бізнес-процесів на кожному підприємстві формує кумулятивний макроекономічний ефект. Математичний фільтр моделі орієнтує процеси на максимізацію інтегрального показника (цільовий орієнтир ~60% річних) за рахунок приросту доходів та економії операційних витрат. Сумарна оптимізація процесів тисячами суб'єктів МСП за умови синхронної державної підтримки (прискорена амортизація ПЗ, хмарні ваучери, пільгові кредити) забезпечує підвищення фінансово-економічної захищеності, стійкості національної економіки та її успішну інтеграцію в єдиний цифровий простір Європейського Союзу.

Список використаних джерел до розділу 3

1. ДИРЕКТИВА ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text

2. DORA: вимоги, особливості регулювання та практика. URL: https://legalitgroup.com/dora-vymogy-osoblyvosti-regulyuvannya-ta-praktyka/

3. Мазепа С. Міжнародний досвід захисту інформаційної безпеки: імплементація європейських правових норм в законодавство України. *Науковий вісник Ужгородського Національного Університету. Серія: Право.* 2025. Том 3. № 90 С. 289–296. DOI: https://doi.org/10.24144/2307-3322.2025.90.3.42

4. Council of Europe Convention on Cybercrime (ETS No. 185). Budapest, 23.XI.2001. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

5. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. 2016. L 194/1. 19.7.2016

6. Регламент Європейського парламенту і ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку). Офіційний вісник Європейського Союзу. L 151/15. URL: https://www.kmu.gov.ua/storage/app/sites/1/55-GOEEI/es-2019881.pdf

7. Дрига Д. Аналіз правових механізмів забезпечення інформаційної безпеки інформаційної інфраструктури Європейського Союзу. *Herald of Khmelnytskyi National University. Economic Sciences.* 2024. № 334(5). С. 46–51. DOI: https://doi.org/10.31891/2307-5740-2024-334-7

8. Ткачук Т. Ю. Забезпечення інформаційної безпеки: досвід окремих країн східної Європи. *Інформація і право*. 2017№ 4(23). С. 62–72. URL: https://ippi.org.ua/sites/default/files/8_6.pdf;

9. Пугачов О. І. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Проблеми сучасних трансформацій. Серія: право, публічне*

управління та адміністрування. 2024. № 13. DOI: https://doi.org/10.54929/2786-5746-2024-13-02-07

10. Союзу. L 151/15. URL: https://www.kmu.gov.ua/storage/app/sites/1/55-GOEEI/es-2019881.pdf

11. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. No 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

12. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: ратифіковано Законом України від 16 верес. 2014 р. No 1678-VII. Офіційний вісник України. 2014. № 75. Ст. 2125.

13. Act on the Federal Office for Information Security (BSI Act-BSIG). URL: https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz.html

14. Тихомиров О. О. Права людини: інформаційний вимір: монографія. Одеса: Видавництво «Юридика», 2023. 304 с.

15. Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG). Ausfertigungsdatum: 20.04.1994. URL: https://www.gesetze-iminternet.de/s_g/BJNR086700994.html

16. Климчук О. О., Ткачук Н. А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства, держави*. 2015. № 3. С. 75–83. URL: http://nbuv.gov.ua/UJRN/iblsd_2015_3_12;

17. Телеховський Ю. Г. Досвід трансформації спецслужб в Угорщині: висновки для України. *Стратегічні пріоритети*. 2013. № 3. С. 151–156. URL: http://nbuv.gov.ua/UJRN/spa_2013_3_22

18. CERT-UA – Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози. URL: https://cert.gov.ua/about-us

19. Дергалюк М. О. Розвиток підприємницької діяльності в умовах цифровізації економіки. *Агросвіт.* 2024. № 24. С. 95–102. DOI: https://doi.org/10.32702/2306-6792.2024.24.95

20. Литовченко О. Ю., Дячек В. В., Мітін М. О. Трансформація бізнес-моделей підприємств в умовах цифровізації економіки. *Економіка та суспільство.* 2024. Вип. 69. DOI: https://doi.org/10.32782/2524-0072/2024-69-36

21. Швецов В. А. Трансформація бізнес-моделей суб'єктів господарювання в умовах цифровізації економіки України. *European Scientific Journal of Economic and Financial Innovation.* 2025. № 3(17). DOI: https://doi.org/10.32750/2025-0343

22. Шут С. О. Інновації та цифрова трансформація як ключові фактори успіху підприємництва. *Ефективна економіка.* 2024. № 10. DOI: https://doi.org/10.32702/2307-2105.2024.10.42

23. E-commerce retail sales CAGR 2024-2029, by country. Statista Research Department. 2024. June 10. URL: https://www.statista.com/forecasts/220177/b2c-e-commerce-sales-cagr-forecast-for-selected-countries

24. The Digital Economy and Society Index (DESI). *Shaping Europe's digital future*. URL: https://digital-strategy.ec.europa.eu/en/policies/desi

25. Ратушняк Т. В., Омельчук А. А., Горбовий А. Ю., Гладченко О. В., Вишемірська Я. С. Індекс DESI як міра цифрової трансформації у країнах Європейського Союзу. *Прикладні питання математичного моделювання*. 2024. Т. 7. № 2. С. 250–258. DOI: https://doi.org/10.32782/mathematical-modelling/2024-7-2-22

26. Державна служба статистики України: офіційний сайт. URL: https://www.ukrstat.gov.ua

27. Романюк І. А., Гіржева О. М., Долженко Д. О. Стратегічне забезпечення конкурентоспроможного розвитку підприємства на глобальному ринку. *Інвестиції: практика та досвід.* 2025. № 22. С. 170–175. DOI: https://doi.org/10.32702/2306-6814.2025.22.170.

28. Джерелюк Ю. О., Попович Н. Н. Стратегічні засади забезпечення інноваційної конкурентоспроможності підприємства шляхом нарощування його адаптаційного потенціалу. *Економіка та суспільство.* 2026. Вип. 86. DOI: https://doi.org/10.32782/2524-0072/D2026-86-139.

29. Нагаєв В. М., Гіржева О. М., Чалий І. В., Міненко С. І. Digital трансформації публічних комунікацій, кібербезпеки та цифрового лідерства в системі електронного урядування. *Публічне адміністрування та національна безпека.* 2024. № 4(45). С. 78–88.

30. Шапошников, К., & Жаворонок, А. Синергія інформаційної безпеки та інноваційного відновлення підприємницької діяльності в регіоні в умовах глобальних викликів. *Економіка та суспільство*. 2026. (84). https://economyandsociety.in.ua/index.php/journal/article/view/7778

ВИСНОВКИ

У дисертації виведено теоретичні та прикладні положення щодо організаційно-управлінських механізмів забезпечення інформаційною безпекою підприємницької діяльності в умовах глобальної економічної турбулентності. Відповідно до мети та визначених завдань сформульовано такі основні висновки та пропозиції:

1. Розкрито теоретико-методичні засади організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності. Визначено, що найбільша частина науковців розглядає інформаційну безпеку як стан захищеності, незначна частина – як функціонування системи засобів. Такий поділ у наукових поглядах чітко підкреслює подвійну природу інформаційної безпеки. Охарактеризовано інструменти задля підвищення інформаційної безпеки. Наведені принципи інформаційної безпеки є фундаментом, на якому тримається вся система захисту підприємства, і без їх дотримання будь-які дорогі програми чи інструкції стають марними. Вони визначають логіку поведінки компанії у цифровому просторі, перетворюючи розрізнені технічні налаштування на чітку, послідовну філософію бізнесу. Визначено елементи механізму формування корпоративної інформаційної безпеки. Аналіз сформованої матриці впливу глобальної економічної турбулентності на систему інформаційної безпеки підприємства демонструє, що кожен дестабілізуючий імпульс глобальної турбулентності містить у собі прихований потенціал для якісного оновлення захисних систем підприємства. Визначено, що ключова помилка більшості суб'єктів господарювання полягає у спробах ліквідувати наслідки криз суто технічними методами, ігноруючи організаційні та теоретико-методологічні аспекти. Натомість представлена систематизація доводить, що ефективна протидія зовнішньому хаосу та кібератакам в умовах воєнного стану лежить у площині інтеграції класичних моделей розмежування доступу із сучасними концепціями кіберрозвідки. Доведено, що оцінювання безпекового контуру має базуватися на інтегрованій

тріаді PPT (People, Processes, Technology), яка дозволяє одночасно вимірювати стійкість інфраструктури, адаптивність регламентів і кібергігієну персоналу. Критичний перегляд наукового доробку сучасників дозволив чітко диференціювати технічні, фінансові та управлінсько-інформаційні метрики, виявивши їхні обмеження у періоди макроекономічного хаосу та воєнного стану. Для подолання цих обмежень використовують систему з 26 показників-коефіцієнтів, яка враховує рівень технологічного суверенітету компанії через частку внутрішнього програмно-технічного забезпечення.

2. Проведено структурно-динамічний аналіз макроекономічних детермінант розвитку бізнес-систем. Статистичний аналіз динаміки Індексу глобалізації KOF дозволив емпірично, що результативність діяльності локальних бізнес-систем критично залежить від трендів глобального середовища. Стабільне лідерство країн Західної Європи (Нідерланди, Бельгія, Швейцарія) зумовлене їх максимальною відкритою інтеграцією у транскордонні фінансові та інформаційні потоки. У період 2018–2020 років показники України демонстрували помірне зростання, утримуючи позиції у першій півсотні найбільш глобалізованих країн світу (44–45 місця). Стрімкий підйом України у рейтингу індексу легкості ведення бізнесу з 152-го на 64-те місце з 2014 до 2020 рр. став можливим завдяки тотальній цифровізації (перехід на електронний документообіг, онлайн-реєстрацію, державні цифрові платформи). Проведений аналізі показав, що загальний обсяг валової доданої вартості України за досліджуваний період зріс у фактичних цінах на 4 868 230 млн грн, досягнувши у 2023 році відмітки у 5 822 702 млн грн, що вказує на часткову адаптаційну стабілізацію та відновлення економічної активності бізнес-систем після катастрофічних руйнувань першого року повномасштабного вторгнення. У розрізі структурного аналізу спостерігається подолання пікових деформацій 2022 року та поступове вирівнювання траєкторій ключових галузей. Разом, сектори промисловості та оптової та роздрібної торгівлі це вектори господарювання, що забезпечують майже 35% базисного макроекономічного доходу і залишаються фундаментом

приватного підприємництва. Статистичні дані показують, що в усіх без винятку досліджуваних секторах економіки частка малого підприємництва (разом із мікро-) перевищує 94%, а у середньому по країні становить 99,24% станом на 2024 рік. Сектор промисловості традиційно залишається сферою з найвищою часткою великих (0,24% у 2024 р.) та середніх (3,84%) підприємств. Попри те, що сумарно вони становлять трохи більше 4% від кількості індустріальних суб'єктів, саме вони акумулюють основні засоби, промисловий капітал та генерують левову частку галузевої ВДВ. Здійснено розрахунок коефіцієнта щільності мікробізнесу в аналізованій сукупності (галузі, регіоні або економіці загалом), розрахунок якого здійснюється на основі офіційних пооб'єктних чи галузевих даних демографії підприємств. Розрахунок та впровадження коефіцієнта щільності мікробізнесу (Кщм) дозволили розкрити внутрішню глибину структурних деформацій, які відбулися в національній економіці під впливом воєнних та інституційних шоків. Отримані результати демонструють перехід ринкових систем від корпоративно-ієрархічної моделі до ультрадецентралізованої мережевої моделі.

3. Здійснено оцінку потенціалу розвитку підприємницької діяльності. Визначено, що станом на 2024 рік фіксується часткове відновлення виробничого потенціалу до рівня 9 388,03 млрд грн, але за умови посилення концентрації. Частка великого бізнесу знову зросла до 40,2%, а середнього – утрималася на рівні 39,8%. Економіка адаптувалася, проте її фінансовий потенціал знову сконцентрувався всередині великих корпоративних структур та мереж. Концентрація 80% усього виробничого потенціалу України у 2024 році в руках великого (40,2%) та середнього (39,8%) бізнесу науково доводить, що саме ці дві групи підприємств володіють необхідним інвестиційним ресурсом для побудови повноцінних систем захисту інформації. Аналіз показав, що операційна діяльність мікропідприємств характеризується критичною нестабільністю. Під час системних криз 2014 та 2022 років рівень їхньої операційної рентабельності падав до -30,09% та -6,99% відповідно, що вказує на пряме вимивання капіталу з операційного контуру. Ще більш

загрозливою є рентабельність всієї діяльності: у 2024 році цей показник для мікросуб'єктів залишився від'ємним (-0,19%), попри загальну стабілізацію ринку. Це означає, що фінансове навантаження (кредити, валютні коливання, логістичні витрати) повністю знецінює результати їхньої операційної роботи. Визначено, що протягом 2012–2024 років ключовими драйверами оновлення основних засобів та нематеріальних активів виступали великі корпорації та середні підприємства, які сукупно стабільно контролювали 83–88% усіх капітальних витрат у державі. Зокрема, у 2024 році із загального обсягу інвестицій у 599,97 млрд грн на частку великого бізнесу припало 48,3%, а середнього – 38,2%. Запропоновано методику оцінки інтегральної фінансово-економічної захищеності підприємств цифрового ринку. Розрахунок інтегрального індексу дозволяє подолати методологічний розрив між фінансовим аналізом і менеджментом безпеки. Він трансформує статичну бухгалтерську звітність у динамічний інструмент стратегічного управління, який чітко вказує на межі фінансової спроможності підприємства щодо забезпечення власного інформаційного та кібернетичного захисту. Розроблена методика оцінки та побудована на її основі стратегічна матриця безпекового позиціонування, що розділяє підприємства за рівнем захищеності.

4. Запропоновано організаційно-управлінський механізм управління інформаційною безпекою підприємницької діяльності в умовах глобальної економічної турбулентності. Наведено ключові підходи до визначення сутності організаційно-економічного механізму. Запропоновано структурування організаційно-управлінського механізму для забезпечення інформаційної безпеки підприємства, що охоплює три взаємопов'язані субмеханізми, кожен з яких спрямований на усунення відповідного класу дисфункцій. Обґрунтовано, що під організаційно-управлінським механізмом управління інформаційною безпекою підприємницької діяльності в умовах глобальної економічної турбулентності необхідно розуміти складну систему впливу на функціонування підприємництва, яка охоплює законодавче, інформаційно-методичне та інституційне забезпечення, цифрові інструменти

(аналітичні (індекс Іфез, стрес-тести, моніторинг БАД), фінансові (модель Сарех, Орех, кіберстрахування), організаційні (ISO 27001, аутсорсинг), технологічні (хмарні, SOC)), фактори впливу (воєнно-політичні, геополітичні, макроекономічні, ринкові, регуляторні, фінансово-економічні, організаційно-технологічні, соціально-психічні) та специфічні особливості (фінансово-економічний моніторинг виступає основною для трансформації контуру технологічного захисту), а також зорієнтована на зміну особистих та спільних ціннісних орієнтирів колективної відповідальності за збереження інформаційного капіталу та трансформація системи інформаційної безпеки із системи обмежень у систему спільної життєстійкості (резильєнтності). Це забезпечує внутрішню консолідацію підприємства та підтримує стабільні індекси його ділової активності та глобальної конкурентоспроможності незалежно від амплітуди коливань зовнішнього турбулентного середовища.

5. Досліджено європейський досвід забезпечення інформаційної безпеки підприємницької діяльності та шляхи його імплементації у вітчизняних реаліях. Проаналізовано міжнародні договори та конвенції, що регулюють інформаційну безпеку. Визначено, що ключові елементи європейського досвіду забезпечення інформаційної безпеки базуються на переході від статичного захисту периметру до філософії комплексної цифрової операційної резилієнтності бізнес-систем. Аналіз показав, що створення ефективної системи реагування на кіберінциденти в Україні відбувається з урахуванням досвіду європейських країн та рекомендацій ENISA (Агентства ЄС з питань кібербезпеки). Проведено порівняльний аналіз моделей управління інформаційною безпекою підприємств в ЄС та Україні, який показав наявність суттєвих концептуальних та інституціональних розбіжностей між двома системами. Як показав аналіз, проектування ефективного контуру кіберзахисту та ліквідації цифрових загроз на національному рівні відбувається шляхом адаптації кращих практик країн ЄС та інституційних стандартів Європейського агентства з кібербезпеки. Аналіз проблем впровадження інформаційної безпеки у вітчизняних реаліях дозволяє

констатувати, що головними деструктивними чинниками виступають хронічний брак фінансових ресурсів малого й середнього бізнесу, кризова асиметрія ринку та дефіцит кваліфікованих кадрів, поглиблені нелінійними шоками воєнного стану. Сформовано стратегічні шляхи імплементації європейського досвіду, що свідчать про модернізацію системи захисту інформаційних ресурсів вітчизняних підприємств в умовах турбулентності та повинно базуватися не на пасивному копіюванні регуляторних вимог, а на принципах цифрової операційної резильєнтності та економічної доцільності.

6. Розроблено дизайн адаптивної структурно-функціональної моделі розвитку підприємництва в умовах цифрової трансформації. Проведений аналіз середньорічних темпів зростання роздрібних продажів електронної комерції (CAGR) за країнами світу та динаміки індикаторів інтеграції цифрових технологій у діяльність підприємств України дозволив виявити статистичні закономірності, що доводять, що цифрова трансформація українського підприємництва відбувається в умовах жорстких ресурсних обмежень та безпекових загроз. За отриманими результатами проведеного аналізу капітальних інвестицій розроблено концептуальний дизайн адаптивної структурно-функціональної моделі розвитку підприємництва в умовах цифрової трансформації. Модель є багаторівневою системою, що поєднує ресурсні можливості, трансформаційні механізми та стратегічні вектори розвитку підприємницьких структур. Базовий рівень фіксує поточні макроекономічні реалії, а саме потребу у першочерговому фінансуванні основних засобів (обладнання, логістика, інженерні споруди) через безпекові ризики та руйнування та обмеженість вільних фінансових ресурсів у промисловості та будівництві для фінансування класичних IT-проєктів «з нуля». Другий рівень, трансформаційні механізми, дозволяє для подолання розриву між потребою в діджиталізації та браком коштів у моделі використання трьох регуляторно-організаційних блоків: механізм технологічного трансферу та абсорбції (B2B-інтеграція), державно-приватне стимулювання та екосистемна платформа хмарної дифузії. На третьому рівні

формуються стратегічні вектори розвитку підприємницької діяльності, які реалізуються через три взаємопов'язані стратегічні вектори, адаптовані під специфіку кожної групи підприємств. Для успішної верифікації запропонованої моделі у межах наукового дослідження розроблено методику оцінки ефективності та моніторингу цифрової трансформації підприємств. Вона переводить якісні теоретичні положення у чіткі кількісні метрики та визначає алгоритм їхнього регулярного відстеження. Доведено, що впровадження запропонованої моделі через механізми B2B-технологічного трансферу, бюджетно-фінансових компенсаторів та екосистемної хмарної дифузії дозволить бізнесу подолати кризові тенденції, забезпечивши високу окупність цифрових інвестицій (ROI_{dig}на рівні 60%) за рахунок системного зниження операційних витрат.

7. Сформовано стратегічні засади розвитку підприємницької діяльності в умовах глобальної економічної турбулентності. Доведено, що стратегічні засади розвитку підприємств мають бути диференційовані за трьома взаємопов'язаними векторами, що дозволить уникнути уніфікації управлінських рішень та врахувати галузеву специфіку капіталомісткості й поточний рівень діджиталізації бізнесу. Вектор А орієнтований на сектори економіки з високою питомою вагою матеріальних основних засобів, але з критично низьким рівнем інвестування у цифрові активи, а саме переробна промисловість, будівництво, сільське господарство. Особливістю цього вектора є те, що закупівля нового технологічного обладнання, верстатів чи побудова логістичних комплексів має супроводжуватися одночасним розгортанням цифрових систем управління. Вектор Б є базовим для сектору малого та середнього підприємництва (із чисельністю зайнятих 10–249 осіб), а також для підприємств сфери торгівлі та послуг. Особливістю цього вектора є відмова від капіталомістких IT-проєктів «з нуля» на користь готових хмарних рішень. Вектор В орієнтований на високотехнологічні сегменти української економіки: IT-сектор, фінансову діяльність та інноваційні наукомісткі стартапи. Особливістю вектора є сертифікація українських

цифрових продуктів за стандартами GDPR, інтеграцію в європейські цифрові ланцюги створення вартості та масштабування рішень у сферах FinTech, AgTech, GovTech та MilitaryTech; створення консорціумів між національними ІТ-компаніями та вітчизняними індустріальними підприємствами. Сформовано орієнтовані складові стратегії цифрової трансформації для сектору малого підприємництва. Доведено, що згідно з розробленою та верифікованою адаптивною моделлю, на національному рівні державна політика має відійти від уніфікованого (лінійного) підходу до діджиталізації та зосередитися на формуванні трьох стратегічних векторів цифрової трансформації. Запропоновано інтегровану модель розвитку підприємницької діяльності в умовах цифрової трансформації, що не просто фіксує послідовність операцій, а визначає роль, місце та взаємозв'язок бізнес-процесів підприємництва у контексті впливу управлінського чинника. Саме управлінський чинник виступає тим інтегруючим і спрямовуючим вектором, який перетворює розрізнені технологічні та фінансові ресурси на єдину, високоадаптивну систему. Доведено, що від сумарної ефективності бізнес-процесів на кожному окремому підприємстві безпосередньо залежить не лише його локальна життєздатність, а й загальнонаціональний рівень економічної стійкості, темпи євроінтеграції та динаміка подолання наслідків системної кризи. Мале та середнє підприємництво виступає базовим фундаментом економіки, тому кумулятивний ефект від оптимізації процесів на мікрорівні трансформується у масштабні макроекономічні зрушення.

ДОДАТКИ

Додаток А

Таблиця А.1

Показники оцінки інформаційної безпеки підприємства

№ з/п	Показники інформаційної безпеки	Характеристика
1	2	3
Оцінка програмно-технічної захищеності інформації		
1	Коефіцієнт фінансування програмної захищеності інформації.	Співвідношення вартості програмного забезпечення, яке застосовується для створення інформаційного захисту до загальних витрат на інформаційну безпеку.
2	Коефіцієнт фінансування технічної захищеності інформації.	Співвідношення вартості технічного забезпечення, яке застосовується для створення інформаційного захисту до загальних витрат на інформаційну безпеку.
3	Коефіцієнт технічного захисту інформації.	Співвідношення кількості відвернутих інформаційних атак до загальної кількості інформаційних атак за певний проміжок часу.
4	Коефіцієнт програмної захищеності інформації.	Співвідношення часу безперебійного функціонування корпоративної інформаційної системи до нормативного часу функціонування корпоративної інформаційної системи.
5	Коефіцієнт фінансування програмно-технічної захищеності інформації.	Співвідношення витрат на програмно-технічний захист інформаційних ресурсів до витрат на придбання інформаційних ресурсів.
6	Коефіцієнт фінансування інформаційних служб підприємства.	Співвідношення витрат утримання інформаційної служби підприємства до загальних витрат підприємства.
7	Коефіцієнт автоматизації програмно-технічної захищеності інформації.	Співвідношення автоматизованих процесів спрямованих на програмно-технічний захист інформації до загальної кількості процесів спрямованих на програмно-технічний захист інформації.
Оцінка витрат на забезпечення інформаційної безпеки		
8	Коефіцієнт фінансування інформаційної безпеки.	Співвідношення витрат на забезпечення інформаційної безпеки підприємства до загальних витрат підприємства.
9	Коефіцієнт фінансування інформаційної безпеки, що забезпечує фінансовий напрям діяльності підприємства.	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фінансового напряму діяльності підприємства до витрат на забезпечення інформаційної підприємства.
10	Коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства.	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фізичних об’єктів підприємства до витрат на забезпечення інформаційної підприємства.
11	Коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства.	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист персоналу підприємства до витрат на забезпечення інформаційної підприємства.
Оцінка інформаційної надійності персоналу		
12	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства.	Співвідношення чисельності працівників, маючих доступ до комерційної таємниці (баз даних, банків даних тощо), що працюють на підприємстві більше одного року до загальної чисельності працівників, що мають доступ до комерційної таємниці (баз даних, банків даних тощо).
13	Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства.	Співвідношення чисельності працівників, звільнених за причиною витоку інформації до загальної чисельності звільнених працівників.
14	Коефіцієнт підготовленості персоналу до розпізнавання загроз інформаційній безпеці.	Співвідношення чисельності, ненавмисні дії яких призвели до витоку інформації через низький рівень компетентності персоналу та невміння розпізнавання загроз інформаційній безпеці до загальної чисельності працівників, що мають доступ до закритої інформації.

15	Коефіцієнт правової захищеності інформації.	Співвідношення обсягу інформації, розголошення якої може спричинити негативні наслідки для підприємства до загального обсягу юридично захищеної інформації.
16	Коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку.	Співвідношення інформаційних загроз (інформаційних атак), які відвернуті через дії персоналу, який забезпечує інформаційну безпеку до загальної кількості інформаційних атак за певний проміжок часу.
Оцінка інформації, що надається особам, які приймають рішення, інформаційною службою підприємства		
17	Коефіцієнт повноти інформації.	Співвідношення обсягу інформації, що є в розпорядженні ОПР до обсягу інформації, необхідної для ухвалення обґрунтованого рішення.
18	Коефіцієнт точності інформації.	Співвідношення обсягу релевантної інформації до загального обсягу наявної в розпорядженні ОПР інформації.
19	Коефіцієнт суперечливості інформації.	Співвідношення кількості незалежних свідчень на користь ухвалення рішення до загальної кількості незалежних свідчень у сумарному обсязі релевантної інформації.
20	Коефіцієнт своєчасності надання інформації.	Співвідношення обсягу своєчасно наданої ОПР інформації до обсягу інформації, необхідної для ухвалення обґрунтованого рішення.
21	Коефіцієнт надійності інформації.	Співвідношення обсягу інформації, наданої ОПР з перевірених джерел до загального обсягу наданої ОПР інформації.
Оцінка системи захисту інформації		
22	Ступінь інформаційного ризику.	Відсоток втрат (у грошову вираженні) спричинених пошкодженням інформаційної цілісності підприємства.
23	Гнучкість системи інформаційної. безпеки підприємства.	Здатність системи управління інформаційною безпекою швидко адаптувати організаційну побудову до зовнішніх та внутрішніх потреб.
24	Коефіцієнт керованості системи інформаційної безпеки підприємства.	Співвідношення компетентностей керівного персоналу системи інформаційної безпеки до загальних компетентностей, якими повинен володіти керівник відповідного рівня.
25	Частка програмного забезпечення, розробленого працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства.	
26	Частка технічних засобів, розроблених працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства.	

Джерело: згруповано автором на основі [26; 27; 28; 29; 32; 33; 34].

Додаток Б

Довідки про впровадження

ВГО «Українська Асоціація Центрів Підтримки Бізнесу»

ЄДРПОУ 26112446, Україна, 54001, м. Миколаїв, вул. Героїв Рятувальників, 2, оф.107, а/с 400, дирекція: м. Миколаїв, вул. Марка Кропивницького, 51/1, тел: (067) 234 06 77, (050) 665 17 77 email: info@uabsc.org

2406/01-002 від 24.06.2026

ДОВІДКА

про впровадження результатів дисертаційного дослідження

Видана всеукраїнською громадською організацією «Українська асоціація центрів підтримки бізнесу» про те, що результати дисертаційного дослідження Черкаського Григорія Ігорьовича на тему: «Організаційно-управлінські механізми забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності», поданого на здобуття ступеня доктора філософії за спеціальністю 073 «Менеджмент», впроваджено та використовуються у діяльності організації.

У процесі діяльності громадської організації використано наукові положення, методичні підходи та практичні рекомендації, розроблені автором щодо формування організаційно-управлінських механізмів забезпечення інформаційної безпеки суб'єктів підприємницької діяльності в умовах зростання глобальних економічних ризиків, цифровізації економіки та посилення кіберзагроз.

Практичне застосування результатів дослідження дало можливість:

– впровадити рекомендації щодо організаційного забезпечення захисту інформаційних ресурсів та даних;

– підвищити ефективність управлінських рішень у сфері протидії інформаційним загрозам та кризовим ситуаціям;

– покращити механізми моніторингу зовнішніх і внутрішніх факторів впливу на інформаційну безпеку.

Впровадження наукових розробок Черкаського Г. І. сприяє підвищенню ефективності діяльності організації, розвитку її інституційної спроможності та формуванню сучасних підходів до управління інформаційною безпекою.

Виконавчий директор
ВГО «УКРАЇНСЬКА АСОЦІАЦІЯ
ЦЕНТРІВ ПІДТРИМКИ БІЗНЕСУ» Артем ВАЩИЛЕНКО

ВСЕУКРАЇНСЬКА
ГРОМАДСЬКА
ОРГАНІЗАЦІЯ «ПОРУЧ»
03194, Україна, Київ,
бульвар Кольцова, 9, кв.32
044 5996600
www.poruch.com.ua
e-mail: info@poruch.ua

ALL-UKRAINIAN NON-
GOVERNMENTAL
ORGANISATION «PORUCH»
03194, Ukraine, Kyiv,
Koltsov boulevard, 9, Ap.32
044 5996600
www.poruch.com.ua
e-mail: info@poruch.ua

За місцем вимоги

24.02.2026 № 15-ВНА/07-25

Цим підтверджується, що результати дисертаційного дослідження Черкаського Григорія Ігоровича, здобувача ступеня доктора філософії, на тему «Організаційно-управлінські механізми забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності», впроваджено в діяльність Громадської організації Громадська організація «Всеукраїнська громадська організація «Поруч».

У практичній діяльності організації використано науково-методичні рекомендації автора щодо:

удосконалення організаційно-управлінських механізмів забезпечення інформаційної безпеки;

оцінювання ризиків інформаційної безпеки в умовах глобальної економічної турбулентності;

розроблення заходів із підвищення рівня захисту інформаційних ресурсів та ефективності управлінських процесів;

формування системи інформаційної безпеки для забезпечення стійкого функціонування та розвитку підприємницької діяльності.

Використання результатів дисертаційного дослідження сприяє підвищенню ефективності управлінських рішень, удосконаленню процесів забезпечення інформаційної безпеки та зміцненню організаційної стійкості в умовах сучасних економічних викликів.

Довідку видано для подання за місцем вимоги.

Директор
південного офісу
ГО «ВГО «Поруч» Л. Мураховська

Україна
«ВСЕУКРАЇНСЬКА ГРОМАДСЬКА ОРГАНІЗАЦІЯ «ПОРУЧ»
Ідентифікаційний код 37962451
м. Київ

Додаток В

ПЕРЕЛІК НАУКОВИХ ПУБЛІКАЦІЙ

Статті у наукових фахових виданнях, які включені до міжнародних наукометричних баз

7. Шалухіна В. В., Ляшенко В. М., **Черкаський Г. І.**, Томчук О. О. Сучасні тенденції та вектори цифрової трансформації в Україні. *Ukrainian Journal of Applied Economics and Technology.* 2022. Vol. 7. No 2. pp. 219–225. DOI: https://doi.org/10.36887/2415-8453-2022-2-26 *(0,37 друк. арк., особистий внесок:* формування векторів цифрової трансформації – *0,15 друк. арк.).* **Входить до наукометричних баз реферування та індексування: Index Copernicus International (ICI), Google Scholar, Crossref.**

8. Шалухіна В. В., Ляшенко В. М., **Черкаський Г. І.**, Ващиленко А. М., Сумара А. О. Формування інноваційного потенціалу на макро-, мезо- та мікрорівнях в умовах цифровізації. *Український журнал прикладної економіки та техніки.* 2023. Том 8. No 1. С. 41–46. DOI: https://doi.org/10.36887/2415-8453-2023-1-6 *(0,37 друк. арк., особистий внесок:* визначення складових інноваційного потенціалу суб'єктів господарювання – *0,15 друк. арк.).* **Входить до наукометричних баз реферування та індексування: Index Copernicus International (ICI), Google Scholar, Crossref.**

9. Dubinska, I., Irtyshchev, O., & **Cherkaskyi, H.** (2025). Prerequisites for securing business activities in the conditions of global economic turbulence. *Baltic Journal of Economic Studies*, *11*(1), 86–94. DOI: https://doi.org/10.30525/2256-0742/2025-11-1-86-94. *(0,56 друк. арк., особистий внесок:* визначено чинники впливу глобальної економічної турбулентності – *0,2 друк. арк.).* **Входить до міжнародних наукометричних баз Web of Science.**

10. Ващиленко А. М., Шалухіна В. В., **Черкаський Г. І.**, Михасько Т. Ю., Бездольний Д. С. Регіональне управління в умовах віртуалізації економіки: роль у інноваційному відновленні, принципи та проблеми. *Актуальні проблеми інноваційної економіки та права*. 2025. № 4. С. 32–37. DOI: https://doi.org/10.36887/2524-0455-2025-4-8 *(0,37 друк. арк., особистий внесок:*

напрями віртуалізації економіки в Україні – *0,15 друк. арк.).* **Входить до наукометричних баз реферування та індексування: Index Copernicus International (ICI), Google Scholar, Crossref.**

11. Бойко Є. О., Павленко О. П., Бойко О. С., Арчибісова Д. С., **Черкаський Г. І.** Європейський досвід цифрової трансформації бізнес-процесів в аграрій сфері та шляхи його імплементації у національних реаліях. *Український журнал прикладної економіки та техніки*. 2025. Том 10. No 2. С. 284–288. DOI: https://doi.org/10.36887/2415-8453-2025-2-55 *(0,31 друк. арк., особистий внесок:* європейській досвід цифрової трансформації бізнесу – *0,15 друк. арк.).* **Входить до наукометричних баз реферування та індексування: Index Copernicus International (ICI), Google Scholar, Crossref.**

12. **Черкаський Г. І.** Організаційно-управлінські механізми забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності. *Актуальні питання економічних наук.* 2026. № 23. DOI: https://doi.org/10.5281/zenodo.20456912 *(0,75 друк. арк.).* **Входить до наукометричних баз реферування та індексування: Google Scholar, Index Copernicus International (ICI), Crossref, Національна бібліотека України імені В. І. Вернадського(Наукова періодика України.**

Матеріали апробаційного характеру:

6. Іртищев О. С., Гарагуля А. В., Христофоров В. О., **Черкаський Г. І.** Управління підприємствами в умовах цифрової трансформації. *Менеджмент XXI століття: глобалізаційні виклики:* матеріали VII Міжнародної науково-практичної конференції (м. Полтава, 18 травня 2023 р.). Полтава: ПДАУ, 2023. С. 202–204.

7. Михасько Т. Ю., Курбатов О. В., Ляшенко В. М., **Черкаський Г. І.**, Іртищев О.С. Управління бізнес-процесами цифрової трансформації. *Сучасні інноваційно-інвестиційні механізми розвитку національної економіки в умовах євроінтеграції*: матеріали X Міжнародної науково-практичної Інтернет-конференції (м. Полтава, 09 листопада 2023 р.) Полтава: Національний університет «Полтавська політехніка імені Юрія Кондратюка», 2023. С.72–74.

8. Іртищев О., Гарагуля А., Бандюк М., Михасько Т., **Черкаський Г.**, Білінський В. Діджиталізація бізнес-процесів в умовах викликів та загроз. *Актуальні вектори відновлювальної трансформації економіки України:* збірник матеріалів наукових економічних читань (м. Миколаїв, 30.11–01.12.2023 р.): у 2 т. Т. 1. Миколаїв: Іліон, 2023. С.60–65.

9. Бандюк М. В., Білінський В. І., **Черкаський Г. І.** Managing business development in a time of global economic turbulence. *Управління ресурсним забезпеченням господарської діяльності підприємств реального сектору економіки*: IX Всеукраїнська науково-практична Інтернет-конференція (м. Полтава, 13 листопада 2024 р.). Полтава, 2024. С. 115–117

10. Paliy V. S., Mykhasko T. U., **Cherkaskyi H. I.,** Sumara A. O. Digitization of business processes as a prerequisite for their development in an unstable environment. *Актуальні аспекти науково-технічного і соціально-економічного розвитку України: погляд молоді*: Всеукраїнська науково-практична конференція молодих вчених і здобувачів вищої освіти (м. Первомайськ, 15 травня 2025 р). Первомайськ, 2025.