

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова
праця на правах рукопису

ТОПАЛОВ ВОЛОДИМИР МИКОЛАЙОВИЧ

УДК 004.056:334.7

**ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА**

Спеціальність – 076 Підприємництво, торгівля та біржова діяльність
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.

_____ Топалов В.М.

**Науковий керівник – доктор економічних наук, професор
Ковальська Любов Леонідівна**

АНОТАЦІЯ

Топалов В.М. Забезпечення інформаційної безпеки суб'єктів підприємництва – кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 076 Підприємництво, торгівля та біржова діяльність. Луцький національний технічний університет Міністерства освіти і науки України, Луцьк, 2026.

У дисертації наведено комплексне вирішення наукового завдання - обґрунтування теоретико-методологічних засад та практичних рекомендацій забезпечення інформаційної безпеки суб'єктів підприємництва.

На основі системного аналізу наукових підходів до вивчення процесів забезпечення інформаційної безпеки суб'єктів підприємництва, узагальнено теоретичні аспекти визначення дефініцій «інформаційна безпека», «економічна безпека» та «інформаційна безпека підприємства», а також запропоновано авторське визначення дефініції «інформаційна безпека суб'єктів підприємництва», як динамічного процесу захищеності інформаційного середовища, що забезпечує збереження, цілісність, конфіденційність і доступність інформації та сприяє досягненню стратегічних і економічних цілей підприємства. Узагальнено наукові підходи до змістовного наповнення інформаційної безпеки (процесний, проєктний, системний), що дозволило сформулювати комплексне уявлення про її сутність як складової економічної безпеки.

Обґрунтовано значення інформаційної безпеки як основного чинника конкурентоспроможного розвитку підприємств, що визначається здатністю мінімізувати інформаційні ризики, забезпечувати безперервність бізнес-процесів, захищати інтелектуальний капітал та підвищувати рівень довіри з боку партнерів і споживачів. Доведено, що ефективність функціонування суб'єктів підприємництва залежить від рівня захищеності інформаційних ресурсів та інтеграції системи інформаційної безпеки у стратегію управління підприємством.

Визначено та обґрунтовано функціонально-компонентний підхід до змісту інформаційної безпеки підприємства, який дозволяє розглядати її як інтегровану систему, що включає технічні, організаційні, економічні та правові складові. Запропонований підхід враховує внутрішні та зовнішні процеси впливу, а також базується на основних характеристиках інформаційної безпеки (конфіденційності, цілісності, доступності, регламентованості, адаптивності та економічної ефективності).

Розроблено підхід до структуризації інформаційної безпеки суб'єктів підприємництва, який дозволяє систематизувати її складові за такими напрямками, як захист інформаційних ресурсів підприємства, протидія негативному впливу зовнішнього інформаційного середовища та інформаційне забезпечення виробничих або сервісних процесів. Запропонований підхід дозволяє визначити основні джерела загроз та підібрати ефективні інструменти їх нейтралізації.

Досліджено світовий досвід забезпечення інформаційної безпеки суб'єктів підприємництва, на основі чого визначено основні тенденції розвитку систем кіберзахисту, до яких віднесено, інтеграцію інформаційної безпеки у стратегії розвитку підприємств, використання інноваційних технологій захисту, формування культури кібербезпеки та активізацію міжнародного співробітництва. Доведено, що ефективні системи інформаційної безпеки підприємств, базуються на поєднанні технічних, організаційних і інституційних інструментів.

Розроблено методичний підхід до оцінки рівня забезпечення інформаційної безпеки суб'єктів підприємництва, який дозволяє враховувати вплив внутрішніх та зовнішніх чинників, рівень цифровізації підприємства, стан інформаційної інфраструктури та ефективність управління інформаційними ризиками. Запропонований підхід забезпечує можливість комплексної діагностики стану інформаційної безпеки та визначення напрямів її удосконалення, а також сприяє підвищенню обґрунтованості управлінських рішень у сфері інформаційної безпеки, дозволяє своєчасно виявляти критичні

зони ризику та забезпечує формування адаптивної системи захисту, здатної реагувати на динамічні зміни зовнішнього середовища. Застосування такого підходу, створює підґрунтя для проведення регулярного аудиту інформаційної безпеки та інтеграції результатів оцінювання у стратегічне управління підприємством, що в цілому сприяє підвищенню рівня його конкурентоспроможності та стійкості до інформаційних загроз.

Проведено діагностику стану забезпечення інформаційної безпеки суб'єктів підприємництва в Україні, на основі розробленого алгоритму, який інтегрує аналітичну оцінку стану безпеки з формуванням і реалізацією адаптивних стратегій на основі порогових значень, залежності витрат від результатів та інструментів стратегічного аналізу, зокрема матриці BCG. Виявлено основні проблеми в забезпеченні інформаційної безпеки, до яких віднесено недостатній рівень впровадження сучасних технологій захисту, обмеженість фінансових ресурсів, низький рівень цифрової грамотності персоналу, відсутність комплексного підходу до управління інформаційною безпекою. Систематизовано позитивні тенденції, пов'язані з розвитком цифрової економіки та зростанням уваги до кібербезпеки.

Здійснено оцінку рівня інформаційної безпеки суб'єктів підприємництва, що дозволило визначити їх сильні та слабкі сторони, а також можливості та загрози зовнішнього середовища. Проведений аналіз базувався на основних компонентах системи інформаційної безпеки, зокрема технічне забезпечення, організаційно-управлінські механізми, кадрова складова та рівень нормативно-правового забезпечення, що дало змогу комплексно оцінити стан захищеності інформаційного середовища підприємств. Доведено, що сильні сторони пов'язані переважно з поступовим впровадженням цифрових технологій, зростанням обізнаності щодо кіберзагроз та використанням базових засобів захисту інформації, тоді як слабкі сторони зумовлені недостатнім рівнем фінансування заходів безпеки, відсутністю системного підходу до управління інформаційними ризиками, низьким рівнем підготовки персоналу та фрагментарністю впровадження сучасних технологій кіберзахисту.

Запропоновано концепцію забезпечення інформаційної безпеки суб'єктів підприємництва розглядати як цілісну систему заходів, спрямованих на формування безпечного інформаційного середовища, що базується на принципах системності, комплексності, адаптивності та інклюзивної інституційності. В основі концепції лежить інтеграція інформаційної безпеки у стратегічне управління підприємством та формування культури інформаційної відповідальності.

Систематизовано інституційно-організаційні передумови забезпечення інформаційної безпеки, які включають нормативно-правове регулювання, міжнародні стандарти, внутрішні політики підприємства та механізми державної підтримки. Визначено, що ефективність інформаційної безпеки значною мірою залежить від узгодженості дій усіх зацікавлених сторін.

Розроблено структурно-компонентну модель формування системи інформаційної безпеки підприємства, що забезпечує комплексний і системний підхід до управління захистом інформаційних ресурсів, поєднуючи цільову, теоретико-методологічну, функціонально-ресурсну, аналітичну та результативну складові в єдину логічно узгоджену конструкцію. Перевагою запропонованої моделі є інтеграція методологічних підходів, принципів, інструментів та аналітичних процедур, що дозволяє враховувати специфіку діяльності суб'єктів підприємництва, мінімізувати ризики та забезпечити безперервність і адаптивність системи до змін зовнішнього середовища. Модель орієнтована на досягнення стратегічних цілей підприємства через підвищення рівня інформаційної безпеки, що, у свою чергу, сприяє зміцненню економічної стійкості та конкурентоспроможності.

Ключові слова: інформаційна безпека, економічна безпека підприємства, кібербезпека, кіберзагрози, цифровізація, цифрова трансформація, цифрова економіка, управління інформаційними ризиками, політика інформаційної безпеки, аудит інформаційної безпеки, захист даних, інформаційні технології, цифрова стійкість підприємства, чат-боти, конкурентоспроможність підприємства.

ANNOTATION

Topalov V.M. Ensuring Information Security of Business Entities – a qualifying scientific work presented as a manuscript.

The dissertation is submitted for the degree of Doctor of Philosophy in specialty 076 *Entrepreneurship, Trade and Exchange Activities*. Lutsk National Technical University of the Ministry of Education and Science of Ukraine, Lutsk, 2026.

The dissertation provides a comprehensive solution to the scientific problem of substantiating the theoretical and methodological foundations and developing practical recommendations for ensuring the information security of business entities.

Based on a systematic analysis of scientific approaches to studying the processes of ensuring information security of business entities, the theoretical aspects of defining the concepts of «information security», «economic security», and «information security of an enterprise» have been generalized. In addition, the author proposes a definition of «information security of business entities» as a dynamic process of protecting the information environment that ensures the preservation, integrity, confidentiality, and availability of information, and contributes to achieving the strategic and economic goals of the enterprise. Scientific approaches to the substantive content of information security (process, project-based, and system-based) have been generalized, which made it possible to form a comprehensive understanding of its essence as a component of economic security.

The importance of information security as a key factor in the competitive development of enterprises has been substantiated, determined by the ability to minimize information risks, ensure business continuity, protect intellectual capital, and increase the level of trust among partners and consumers. It has been proven that the effectiveness of business entities depends on the level of protection of information resources and the integration of the information security system into the enterprise management strategy.

A functional-component approach to the content of enterprise information security has been identified and substantiated, enabling it to be considered as an

integrated system that includes technical, organizational, economic, and legal components. The proposed approach takes into account both internal and external processes of influence and is based on the key characteristics of information security, namely confidentiality, integrity, availability, compliance (regulation), adaptability, and economic efficiency.

An approach to structuring the information security of business entities has been developed, which makes it possible to systematize its components according to such areas as the protection of enterprise information resources, counteraction to the negative impact of the external information environment, and information support of production or service processes. The proposed approach enables the identification of key sources of threats and the selection of effective tools for their neutralization.

The global experience of ensuring information security of business entities has been studied, which made it possible to identify the main trends in the development of cybersecurity systems. These include the integration of information security into enterprise development strategies, the use of innovative protection technologies, the formation of a cybersecurity culture, and the intensification of international cooperation. It has been proven that effective enterprise information security systems are based on a combination of technical, organizational, and institutional instruments.

A methodological approach to assessing the level of information security of business entities has been developed, which takes into account the influence of internal and external factors, the level of enterprise digitalization, the state of information infrastructure, and the effectiveness of information risk management. The proposed approach enables a comprehensive diagnosis of the state of information security and the identification of directions for its improvement. It also enhances the validity of managerial decision-making in the field of information security, allows for the timely identification of critical risk areas, and ensures the formation of an adaptive protection system capable of responding to dynamic changes in the external environment. The application of this approach provides a basis for conducting regular information security audits and integrating evaluation results into enterprise strategic management,

which ultimately contributes to increasing its competitiveness and resilience to information threats.

A diagnostic assessment of the state of information security of business entities in Ukraine has been conducted based on a developed algorithm that integrates analytical evaluation of the security level with the formation and implementation of adaptive strategies. This algorithm is grounded on threshold values, the relationship between costs and outcomes, and strategic analysis tools, in particular the BCG matrix. The main problems in ensuring information security have been identified, including the insufficient implementation of modern protection technologies, limited financial resources, low levels of digital literacy among personnel, and the lack of a comprehensive approach to information security management. At the same time, positive trends have been systematized, particularly those related to the development of the digital economy and the growing attention to cybersecurity.

An assessment of the level of information security of business entities was carried out, which made it possible to determine their strengths and weaknesses, as well as opportunities and threats from the external environment. The analysis was based on the main components of the information security system, in particular, technical support, organizational and management mechanisms, personnel and the level of regulatory and legal support, which made it possible to comprehensively assess the state of security of the information environment of enterprises. It is proven that the strengths are mainly associated with the gradual introduction of digital technologies, increased awareness of cyber threats and the use of basic information protection tools, while the weaknesses are due to the insufficient level of funding for security measures, the lack of a systematic approach to information risk management, low level of personnel training and the fragmented implementation of modern cyber protection technologies.

A concept for ensuring the information security of business entities has been proposed, which considers it as a holistic system of measures aimed at forming a secure information environment, based on the principles of systemacity, complexity, adaptability, and inclusive institutionalism. The concept is grounded in the integration

of information security into the strategic management of the enterprise and the formation of a culture of information responsibility.

The institutional and organizational prerequisites for ensuring information security have been systematized, including regulatory and legal frameworks, international standards, internal enterprise policies, and mechanisms of state support. It has been determined that the effectiveness of information security largely depends on the coordination of actions among all stakeholders.

A structural-component model for the formation of an enterprise information security system has been developed, which ensures a comprehensive and systematic approach to managing the protection of information resources by integrating target, theoretical-methodological, functional-resource, analytical, and result-oriented components into a single logically consistent framework. The advantage of the proposed model lies in the integration of methodological approaches, principles, tools, and analytical procedures, which makes it possible to take into account the specifics of business entities' activities, minimize risks, and ensure the continuity and adaptability of the system to changes in the external environment. The model is aimed at achieving the strategic goals of the enterprise through enhancing the level of information security, which, in turn, contributes to strengthening economic stability and competitiveness.

Keywords: information security, economic security of the enterprise, cybersecurity, cyber threats, digitalization, digital transformation, digital economy, information risk management, information security policy, information security audit, data protection, information technologies, digital resilience of the enterprise, chatbots, enterprise competitiveness.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України

1. Ковальська Л., Топалов В., Топалов Р. (2023) Інформаційна безпека регіону: підходи до розгляду та економічна сутність. *Економічний форум*. № 13 (2), С. 18-24. DOI: <https://doi.org/10.36910/6775-2308-8559-2023-2-3>. (Здобувачем проведено огляд літератури поняття інформаційна безпека за ознакою «стабільний та стійкий стан системи державного управління в інформаційному просторі»).
2. Топалов В.М. (2024). Забезпечення інформаційної безпеки бізнесу України в умовах сучасних загроз. *Цифрова економіка та економічна безпека*, 6 (15), С. 157-161. DOI: <https://doi.org/10.32782/dees.15-24>.
3. Топалов В.М. (2025). Забезпечення інформаційної безпеки як детермінанта конкурентоспроможного розвитку підприємства. *Актуальні питання економічних наук*, № 10. DOI: <https://doi.org/10.5281/zenodo.15585336>.
4. Топалов В.М. (2025). Розвиток системи інформаційної безпеки суб'єктів малого підприємництва. *Бізнес-навігатор*, № 4 (81). DOI: <https://doi.org/10.32782/business-navigator.81-34>.
5. Топалов В.М. (2025). Стратегічні орієнтири забезпечення інформаційної безпеки суб'єктів малого підприємництва. *Економіка та суспільство* № 75 *Економіка та суспільство*, (75). DOI: <https://doi.org/10.36910/6775-2308-8559-2023-2-3>.
6. Топалов В.М. (2025). Формування інституційної моделі забезпечення інформаційної безпеки бізнесу в регіоні. *Економічні науки: збірник наукових праць*. Серія Регіональна економіка. Випуск 22 (87). Редкол.: відп. ред. д.е.н., професор Л.Л. Ковальська. Луцьк: ВІП ЛНТУ. С.503-516. DOI: [https://doi.org/10.36910/2707-6296-2025-22-\(87\)-47](https://doi.org/10.36910/2707-6296-2025-22-(87)-47).

Опубліковані праці апробаційного характеру

7. Топалов В. Напрями цифровізації сільськогосподарських підприємств. *Цифрова трансформація: виклики та стратегії: матеріали Міжнародної науково-*

практичної конференції, 25 лютого 2025 р., м. Луцьк: ЛНТУ, 2025. 272 с. С. 73-75.
URL: https://lib.lntu.edu.ua/sites/default/files/2025-06/ЗбірникЛНТУ_2.pdf.

8. Топалов В. Забезпечення інформаційної безпеки суб'єктів підприємництва в умовах воєнного стану. Проблеми гарантування безпеки людини в умовах сучасних викликів: *матеріали II Всеукраїнської науково-практичної конференції* 29-30 квітня 2025 р. м. Луцьк: ЛНТУ, 2025. 114 с. С. 38-40.
URL:

<https://drive.google.com/file/d/1X8kkzQkoV4U8y18aHLB4ADkSQcrZaVEX/view>.

9. Топалов В.М. Удосконалення інформаційної системи підприємства. Підприємництво та торгівля: сучасний стан та перспективи розвитку: матеріали IV Міжнародної науково-практичної конференції 16 травня 2024 р., м.Луцьк. С.125-126.
URL:

https://drive.google.com/file/d/1lp2l7io__RInLtgUwlb4CHS4pTZW2IH/view.

9. Топалов В. Чинники впливу на забезпечення інформаційної безпеки суб'єктів малого підприємництва. Підприємництво та бізнес-адміністрування: відновлення, сталий розвиток та інновації у післявоєнний час: *матеріали Міжнародної науково-практичної інтернет конференції*, 1-28 лютого 2025 р., м. Харків. 257 с. С. 167-168.
URL:

<https://eprints.kname.edu.ua/67924/1/Збірник%202025.pdf>.

10. Топалов В. Інформаційна безпека як фактор стійкості та конкурентоспроможності суб'єктів підприємництва. Актуальні проблеми управління соціально-економічними системами: *матеріали XI Міжнар. наук.-практ. конф.*, Частина 1. Луцьк, 5 груд. 2025 р., Луцьк: Надстир'я, 2025. 414 с. С.86-89. URL: <https://repository.lntu.edu.ua/entities/studycollections/8b6e684a-3751-4528-bcd4-e8c3592ca926>.

Публікації у іноземних виданнях

12. Topalov V. (2025). Prospects for ensuring information security of business entities as a vector of their sustainable development. *Global Prosperity*, 5(3). DOI: <https://doi.org/10.5281/zenodo.18703697>.

ЗМІСТ

ВСТУП	13
РОЗДІЛ 1 КОНЦЕПТУАЛЬНІ ЗАСАДИ ФОРМУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА	25
1.1 Зміст та значення інформаційної безпеки в розвитку суб'єктів підприємництва	25
1.2 Забезпечення інформаційної безпеки як детермінанта конкурентоспроможного розвитку підприємства	45
1.3 Світовий досвід забезпечення інформаційної безпеки суб'єктів підприємництва	65
Висновки до розділу 1	78
 РОЗДІЛ 2 ДІАГНОСТИКА СТАНУ ТА ПЕРСПЕКТИВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА	82
2.1 Методичні засади дослідження стану та перспектив забезпечення інформаційної безпеки суб'єктів підприємництва	82
2.2 Детермінанти розвитку суб'єктів малого підприємництва України	106
2.3 Оцінка рівня забезпечення інформаційної безпеки суб'єктів підприємництва	137
Висновки до розділу 2	166
 РОЗДІЛ 3 НАУКОВО-МЕТОДИЧНИЙ ІНСТРУМЕНТАРІЙ УДОСКОНАЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА	169
3.1 Науково-методичні підходи до побудови системи інформаційної безпеки підприємства	169
3.2 Методика проведення аудиту інформаційної безпеки підприємства	183
3.3 Стратегічні орієнтири розвитку системи забезпечення інформаційної безпеки суб'єктів малого підприємництва	199
Висновки до розділу 3	225
 ВИСНОВКИ	228
СПИСОК ВИКОРИСТАНОЇ ДЖЕРЕЛ	231
ДОДАТКИ	253

ВСТУП

Актуальність теми. Забезпечення інформаційної безпеки суб'єктів підприємництва в сучасних умовах виступає одним із факторів їх стабільного функціонування та розвитку. Попри стрімке поширення цифрових технологій та зростання залежності бізнесу від інформаційних ресурсів, рівень захищеності інформаційного середовища підприємств в Україні залишається недостатнім. Посилення процесів цифровізації економіки, розширення використання інформаційно-комунікаційних технологій, активізація кіберзагроз, зростання ролі інформації як стратегічного ресурсу, обумовлюють доцільність удосконалення підходів до забезпечення інформаційної безпеки суб'єктів підприємництва, як важливої складової їх конкурентоспроможності та економічної стійкості.

В сучасних мінливих умовах функціонування бізнесу, зокрема в умовах глобалізаційних трансформацій, воєнних викликів та нестабільності економічного середовища, питання забезпечення інформаційної безпеки набувають особливої актуальності. Здатність підприємств ефективно протистояти інформаційним загрозам, забезпечувати захист конфіденційних даних, підтримувати безперервність бізнес-процесів та довіру з боку партнерів і споживачів, визначає їх конкурентні позиції на ринку. Зважаючи на зазначене, інформаційна безпека перетворюється на інструмент захисту та на стратегічний ресурс розвитку підприємства, що безпосередньо впливає на його інноваційний потенціал та адаптивність до змін зовнішнього середовища.

Проблематиці теоретичних і прикладних аспектів забезпечення інформаційної безпеки суб'єктів підприємництва присвячено праці вітчизняних і зарубіжних учених, зокрема: Бехтер А.А., Бойко І.М., Борзенкова О.Д., Вавдіюк Н.С., Ворохоб М.В., Гринчуцького В.І., Дейнега І.О., Кравчук І.М., Ковальської Л.Л., Корзун Л.С., Косінський П.М., Кошовий Б.-П.О., Легомінова С.В., Мамалиги В.О., Мельничук Г.С., Саврас І.З., Савченко В.А., Сніщенко Р.Г., Струтинської І.В., Тульчинської С.О., Чубаєвського В.І., Шрамко О.О., Шульги В.І., Фединець Н.І., Фролової Л.В., Якименко Ю.М.

Незважаючи на значну кількість наукових праць, слід зазначити, що окремі теоретико-методологічні та прикладні аспекти забезпечення інформаційної безпеки суб'єктів підприємництва залишаються недостатньо сформованими. Зокрема, потребують уточнення підходи до трактування сутності інформаційної безпеки в умовах цифрової економіки, систематизації її структурних компонентів, визначення детермінант впливу на рівень захищеності підприємств. Особливої актуальності набуває формування комплексного науково-методичного інструментарію забезпечення інформаційної безпеки, удосконалення підходів до її оцінювання, а також розробка стратегічних орієнтирів її інтеграції у систему управління підприємством. Зважаючи на зазначене, виникає необхідність подальших досліджень у цьому напрямі з метою підвищення рівня стійкості, конкурентоспроможності та ефективності функціонування суб'єктів підприємництва в умовах цифрових трансформацій.

Зв'язок роботи з науковими програмами, планами, темами. Основні положення та результати дослідження узгоджуються з напрямами державної політики у сфері цифрового розвитку та забезпечення інформаційної безпеки, зокрема відповідають завданням Стратегії кібербезпеки України, Національної програми інформатизації, а також Концепції розвитку цифрової економіки та суспільства України. Отримані в дослідженні результати спрямовані на вирішення завдань щодо зміцнення інформаційної безпеки підприємств як складової економічної безпеки та конкурентоспроможності України.

Робота відповідає стратегічним орієнтирам регіонального розвитку, зокрема положенням Державної стратегії регіонального розвитку на 2021-2027 роки, де визначено необхідність цифрової трансформації регіонів, розвитку інноваційної економіки та підвищення рівня безпеки господарської діяльності. У цьому контексті, забезпечення інформаційної безпеки суб'єктів підприємництва розглядається як передумова сталого розвитку регіонів, підвищення їх інвестиційної привабливості та інтеграції у національні і міжнародні економічні процеси.

Дисертаційне дослідження виконано відповідно до плану науково-дослідних робіт кафедри підприємництва, торгівлі та логістики Луцького

національного технічного університету, у межах наукової теми «Потенціал синергії управління логістики та інновацій як основа розвитку кросрівневої підприємницької діяльності» (номер державної реєстрації 0126U002654). У межах виконання зазначеної теми автором здійснено обґрунтування алгоритму аналізу та оцінки інформаційної безпеки суб'єктів підприємницької діяльності, що дозволить виявити рівні її забезпечення; визначення можливих ризиків порушення інформаційної безпеки підприємства та кореляційної залежності обсягів доходів суб'єктів підприємництва та рівня витрат на забезпечення інформаційної безпеки, що дозволяє виявити роль інформаційної безпеки у зміцненні конкурентоспроможності малого бізнесу в умовах цифрової трансформації та загроз зовнішнього середовища (акт №807/01-14 від 18.03.2026).

Мета та завдання дослідження. Метою дослідження є обґрунтування теоретико-методичних засад та розробка науково-практичних рекомендацій щодо формування і удосконалення системи забезпечення інформаційної безпеки суб'єктів підприємництва в умовах цифрової трансформації економіки для підвищення їх конкурентоспроможності, стійкості до зовнішніх і внутрішніх загроз та ефективності функціонування.

Для досягнення мети сформульовано та вирішено такі *завдання*:

- узагальнити та систематизувати теоретико-методичні засади формування системи інформаційної безпеки суб'єктів підприємництва в умовах цифрової трансформації економіки;
- систематизувати сучасні виклики та бар'єри забезпечення інформаційної безпеки суб'єктів підприємництва з урахуванням особливостей функціонування підприємств різного масштабу;
- удосконалити структурно-компонентну модель формування системи інформаційної безпеки підприємства на основі інтеграції її цільових, методологічних, функціональних та результативних складових;
- сформулювати концептуальну модель забезпечення інформаційної безпеки суб'єктів підприємництва, що поєднує процеси виявлення, аналізу, попередження та нейтралізації загроз із системою управління підприємством;

- удосконалити організаційну модель системи управління інформаційною безпекою суб'єктів господарювання з урахуванням впливу внутрішнього та зовнішнього середовища;
- розвинути функціонально-компонентний підхід до забезпечення інформаційної безпеки підприємства на основі інтеграції внутрішніх і зовнішніх процесів впливу та принципів ефективного управління безпекою;
- удосконалити методичний підхід до оцінювання стану інформаційної безпеки суб'єктів підприємництва шляхом використання системи кількісних і якісних показників та матричних методів стратегічного аналізу;
- запропонувати комплексний алгоритм створення та функціонування системи інформаційної безпеки підприємства, який охоплює етапи стратегічного планування, організаційного забезпечення, впровадження та моніторингу;
- обґрунтувати підхід до формування системи інформаційної безпеки на основі деталізації її ключових компонентів, сучасних технологічних рішень і міжнародних стандартів, а також визначити можливості використання TOGAF-підходу в процесах забезпечення інформаційної безпеки;
- удосконалити методику проведення аудиту інформаційної безпеки підприємства на основі інтеграції внутрішнього та зовнішнього аудиту та ризик-орієнтованого підходу;
- розробити систему формування та реалізації стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва на основі цифровізації, управління ризиками та стратегічного планування.

Об'єктом дослідження є процеси формування та забезпечення інформаційної безпеки суб'єктів підприємництва в умовах цифрової трансформації економіки.

Предметом дослідження є теоретико-методичні засади та науково-практичні підходи до формування, оцінювання та удосконалення системи забезпечення інформаційної безпеки суб'єктів підприємництва.

Методи дослідження. Теоретико-методологічною базою дослідження визначено фундаментальні та загальнонаукові положення економічної теорії,

теорії управління, економічної безпеки, інформаційної безпеки, цифрової економіки та підприємництва. Для формування концептуальних і прикладних засад забезпечення інформаційної безпеки суб'єктів підприємництва, використано сукупність методів, а саме: діалектичний – для виявлення закономірностей розвитку інформаційної безпеки в умовах цифрової трансформації економіки; абстрагування і логічного узагальнення – при дослідженні змісту основних дефініцій, категорій та формуванні висновків; системного аналізу – для розкриття змісту та структури інформаційної безпеки як складової економічної безпеки підприємства; структурно-функціонального аналізу – для визначення складових і функцій системи інформаційної безпеки суб'єктів підприємництва; економіко-статистичні методи, методи порівняння та аналогій – для обробки та аналізу статистичних даних, оцінки рівня забезпечення інформаційної безпеки підприємств; метод експертних оцінок – для визначення вагомості факторів впливу на рівень інформаційної безпеки; методи економічного аналізу – для оцінювання стану та ефективності системи інформаційної безпеки; стратегічного аналізу – для обґрунтування напрямів розвитку системи забезпечення інформаційної безпеки суб'єктів підприємництва; графічного аналізу – для візуалізації теоретичних і аналітичних результатів дослідження; матричний метод – для формування підходів до вибору стратегічних орієнтирів забезпечення інформаційної безпеки підприємств.

Інформаційну базу дослідження становили: законодавчі та нормативно-правові акти Верховної Ради України та Кабінету Міністрів України у сфері інформаційної та кібербезпеки, цифровізації та розвитку підприємництва; нормативні документи Міністерства цифрової трансформації України, Державної служби спеціального зв'язку та захисту інформації України, а також інших міністерств та відомств; офіційні матеріали Державної служби статистики України, аналітичні звіти міжнародних організацій; статистичні та аналітичні матеріали щодо розвитку підприємництва, цифрової економіки та кібербезпеки, оприлюднені у відкритих джерелах; матеріали наукових публікацій вітчизняних і зарубіжних учених, монографії, статті у фахових виданнях, ресурси мережі

Інтернет; а також результати власних досліджень автора, отримані в процесі оцінювання рівня забезпечення інформаційної безпеки суб'єктів підприємництва.

Наукова новизна одержаних результатів полягає в обґрунтуванні теоретичних і методичних підходів до формування та забезпечення інформаційної безпеки суб'єктів підприємництва в умовах цифрової трансформації економіки. Найбільш вагомі результати дисертаційного дослідження полягають у наступному:

удосконалено:

—структурно-компонентну модель формування системи інформаційної безпеки підприємства, яка, на відміну від існуючих, ґрунтується на комплексі конститутивних елементів (інтеграції цільової, теоретико-методологічної, функціонально-ресурсної, аналітичної та результативної складових у межах єдиної цілісної системи управління) та забезпечує системне поєднання стратегічних цілей підприємства з методологічними засадами, принципами, інструментарієм реалізації, механізмами оцінювання ефективності інформаційної безпеки, що дозволяє враховувати як внутрішні, так і зовнішні чинники впливу;

— підхід до ідентифікації викликів та бар'єрів забезпечення інформаційної безпеки суб'єктів підприємництва, який на відміну від існуючих, систематизує виклики інформаційної безпеки, диференціює їх залежно від масштабу бізнесу (малий, середній, великий) та поєднує багаторівневу класифікацію викликів (кіберзагрози, регуляторні вимоги, людський фактор, економічні обмеження) із деталізованою структурою бар'єрів їх подолання, що включає фінансові, технічні та організаційні аспекти;

— концептуальну модель забезпечення інформаційної безпеки суб'єктів підприємництва, яка на відміну від існуючих, інтегрує процеси ідентифікації, аналізу, попередження і нейтралізації загроз із функціонально-управлінськими, організаційними та стратегічними компонентами системи безпеки, а також комплексно поєднує цілі, принципи, функції та інструменти реалізації інформаційної безпеки в єдину логічно узгоджену систему, орієнтовану на

забезпечення стійкості підприємства та його адаптації до динамічних умов цифрового середовища;

- організаційну модель системи управління інформаційною безпекою суб'єктів господарювання, яка на відміну від існуючих, базується на інтеграції процесу формування політики інформаційної безпеки з урахуванням інклюзивних інституцій, внутрішніх процесів функціонування підприємства, вимог зовнішнього середовища та забезпечує узгодження вихідних вимог до системи управління інформаційною безпекою з очікуваними результатами стійкого розвитку підприємства через механізм постійного оцінювання відповідності та адаптації управлінських рішень;

- функціонально-компонентний підхід, який на відміну від існуючих, інтегрує внутрішні та зовнішні процеси впливу на інформаційну безпеку підприємства в єдину системну модель та ґрунтується на поєднанні базових принципів (конфіденційність, цілісність, доступність, регламентованість) із управлінськими характеристиками (комплексність, економічна ефективність, інтегрованість у бізнес-процеси, адаптивність), що дозволяє забезпечити узгоджене функціонування механізмів захисту інформації;

- підхід до оцінювання стану інформаційної безпеки, шляхом інтеграції кількісних та якісних показників, а також використання матриці BCG для позиціонування суб'єктів підприємництва за рівнем інформаційної безпеки та ефективністю витрат на її забезпечення, що дозволяє обґрунтовувати стратегічні пріоритети розвитку.

набули подальшого розвитку:

- комплексний алгоритм послідовності дій зі створення системи інформаційної безпеки підприємства, який інтегрує етапи стратегічного планування, організаційного забезпечення, технічної реалізації та постійного моніторингу в єдину логічно завершену систему, а також забезпечує послідовний перехід від аналізу зовнішнього та внутрішнього середовища до впровадження та вдосконалення системи інформаційної безпеки, що дозволяє враховувати специфіку діяльності підприємства та динаміку змін у середовищі функціонування;

– підхід до формування системи інформаційної безпеки шляхом деталізації її компонентів (автентифікація, керування доступом, моніторинг, мережевий захист, резервне копіювання, політики та навчання персоналу) у взаємозв'язку з сучасними технологічними рішеннями та міжнародними стандартами, що забезпечує підвищення рівня стандартизації та сумісності системи;

– обґрунтування доцільності використання TOGAF-підходу як інструменту структуризації процесів забезпечення інформаційної безпеки, що сприяє підвищенню гнучкості, керованості та ефективності системи захисту інформації в умовах цифрової трансформації та зростання кіберризиків, а також забезпечує узгодженість між стратегічними цілями підприємства та технічними засобами їх досягнення;

– методика проведення аудиту інформаційної безпеки підприємства, яка поєднує внутрішній та зовнішній аудит у межах єдиної системи оцінювання з урахуванням специфіки діяльності суб'єктів підприємництва і їх ресурсних обмежень та ґрунтується на інтеграції ризик-орієнтованого підходу, системи принципів аудиту, структуризації об'єктів перевірки та впровадженні чітких критеріїв збору аудиторських доказів, що передбачають розмежування ідентифікації дій і результатів забезпечення інформаційної безпеки;

– система побудови стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва, яка інтегрує стратегічне планування, управління ресурсами та бізнес-процесами, цифровізацію і механізми управління ризиками в єдину послідовну модель формування і реалізації стратегії та забезпечує логічний взаємозв'язок між місією і баченням розвитку системи інформаційної безпеки, аналітичним етапом, визначенням цілей і стратегічних напрямів, а також їх практичною реалізацією через інновації та цифрові технології.

Практичне значення одержаних результатів полягає у можливості використання запропонованих теоретико-методичних положень, науково-практичних рекомендацій і висновків при формуванні та реалізації систем забезпечення інформаційної безпеки суб'єктів підприємництва. Розроблені підходи можуть бути застосовані у діяльності підприємств різних сфер

господарювання з метою підвищення рівня захищеності інформаційних ресурсів, мінімізації ризиків кіберзагроз, забезпечення безперервності бізнес-процесів та зміцнення конкурентоспроможності. Окремі результати дослідження можуть бути використані органами державної влади та місцевого самоврядування при розробці програм цифрового розвитку, кібербезпеки та підтримки підприємництва, а також впроваджені у практичну діяльність суб'єктів господарювання та навчальний процес закладів вищої освіти. Зокрема, науково-методичні положення та практичні рекомендації щодо забезпечення інформаційної безпеки суб'єктів підприємництва використані у роботі Львівської обласної ради при розробці підходу до обґрунтування вибору стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва (довідка №02-вих.523 від 24.03.2026); підхід автора щодо побудови матриці рівнів інформаційної безпеки підприємств, а також модифікованої матриці VCSG використано у роботі Департаменту економічної політики Луцької міської ради; підхід автора щодо розробленої моделі забезпечення інформаційної безпеки суб'єктів підприємництва, що дозволить інтегрувати процеси ідентифікації, аналізу, попередження і нейтралізації загроз по забезпеченню інформаційної безпеки, а також забезпечити стійкість та адаптацію підприємств до динамічних умов розвитку цифрового суспільства використано у роботі Волинської обласної ради (довідка №729/51/2-26 від 08.05.2026); підхід автора щодо запропонованого алгоритму дослідження процесу забезпечення інформаційної безпеки суб'єктів підприємництва, який дозволяє оцінити загрози та вразливості зовнішнього середовища, які зумовлюють порушення інформаційної безпеки суб'єктами підприємництва, сформувати порогові значення забезпечення інформаційної безпеки, порівняти фактичні значення показників, які характеризують інформаційну безпеку із нормативними значеннями, та на цій основі виявити рівень забезпечення інформаційної безпеки суб'єктом підприємницької діяльності використані у роботі (довідка №1-20.03.26 від 20.03.2026).

Понятійний апарат, який характеризує інформаційну безпеку підприємства, її функції та принципи; розроблена модель системи управління інформаційною

безпекою підприємства; формування концептуальних засад забезпечення інформаційної безпеки підприємства – використано при розробці навчально-методичних матеріалів, а також викладанні освітніх компонент «Інформаційна безпека», «Інформаційно-комунікаційні технології в підприємстві та торгівлі», «Економічна безпека» на факультеті бізнесу та права Луцького національного технічного університету (довідка №806/01-14 від 18.03.2026).

Особистий внесок здобувача. Дисертаційне дослідження є самостійно виконаною науковою працею, у якій висвітлено теоретико-методичне обґрунтування підходів до забезпечення інформаційної безпеки суб'єктів підприємництва в умовах цифрової трансформації економіки. Теоретичні положення, науково-практичні рекомендації та висновки, що містяться у дослідженні, отримані автором особисто на основі проведеного аналізу, систематизації та узагальнення вітчизняного і зарубіжного досвіду, а також результатів власних досліджень. З наукових праць, опублікованих у співавторстві, у дисертаційній роботі використано лише ті положення, ідеї та висновки, які належать особисто автору, що відображено у переліку наукових публікацій.

Апробація результатів дослідження. Теоретичні та практичні результати і висновки дослідження доповідались та обговорювались на Міжнародних конференціях, зокрема: Міжнародній науково-практичній інтернет конференції «Підприємництво та бізнес-адміністрування: відновлення, сталий розвиток та інновації у післявоєнний час» (Харків, 2025); II Всеукраїнській науково-практичній конференції «Проблеми гарантування безпеки людини в умовах сучасних викликів» (Луцьк, 2025); Міжнародній науково-практичній конференції «Цифрова трансформація: виклики та стратегії» (Луцьк, 2025); Міжнародній науково-практичній конференції «Актуальні проблеми управління соціально-економічними системами» (Луцьк, 2025).

Публікації результатів дослідження. За результатами дисертаційного дослідження опубліковано 12 наукових праць, з яких 6 статей у наукових фахових виданнях України, 1 – стаття у міжнародному виданні та 5 тез наукових доповідей.

Структура та обсяг дисертації. Дисертація складається із вступу, трьох розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації – 269 сторінок, в тому числі – 39 рисунків, 27 таблиць, список використаних джерел з 210 найменувань та 3 додатки на 7 сторінках. Обсяг основного тексту дисертації – 210 сторінок.

Перелік умовних позначень

GDPR (EU Regulation 2016/679) – загальний регламент захисту персональних даних;

NIS 2 Directive (EU 2022/2555) – директива про кіберстійкість критичної цифрової інфраструктури;

ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 – міжнародні стандарти управління інформаційною безпекою;

NIST Cybersecurity Framework – рамкова модель управління кіберризиками;

SBA – акт з питань малого бізнесу для Європи;

SIEM – лог-сервери (Graylog, Wazuh, ELK);

ACL – списки контролю доступу;

RBAC – модель контролю доступу, яка надає права доступу до ресурсів на основі ролей користувачів;

IAM – управління ідентифікацією та доступом;

OCTAVE – оперативно критична оцінка загроз, активів і вразливостей;

CRAMM – методологія аналізу та управління ризиками;

TOGAF (The Open Group Architecture Framework) – загальновизнаний міжнародний стандарт архітектурного управління;

ADM (Architecture Development Method) – метод побудови архітектури;

MFA – мультифакторна автентифікація;

CISO – керівник відділу IT-безпеки;

DBMS – система керування базами даних;

ERP – комплексне програмне забезпечення, призначене для автоматизації та управління всіма основними бізнес-процесами компанії;

EDW – централізоване сховище великих обсягів корпоративних даних, призначене для підтримки аналітичної обробки та прийняття рішень;

PLM – управління життєвим циклом продукції;

D4SME – глобальна ініціатива ОЕСР, яка спрямована на підтримку цифрової трансформації малих та середніх підприємств;

DSA – криптографічний алгоритм з використанням відкритого ключа для створення електронного підпису;

DMA – закон про цифрові ринки;

ISO – Міжнародна організація зі стандартизації;

OECD – Організації економічного співробітництва та розвитку;

ЮНЕСКО – Організація об'єднаних націй з питань освіти, науки і культури;

ЄС – Європейський Союз;

HANA – багатомодельна in-memory база даних компанії SAP;

OCTAVE – система для виконання математичних розрахунків, що надає інтерпретовану мову, сумісну з Matlab;

ІБ – інформаційна безпека;

МСБ – малий та середній бізнес;

ФОП – фізичні особи підприємці;

CRM-системи – прикладне програмне забезпечення для підприємств;

ІКТ – інформаційно-комунікаційні технології;

ІТ – інформаційні технології;

ВВП – валовий внутрішній продукт;

BCG – провідна міжнародна компанія, що спеціалізується на менеджмент-консалтингу.

РОЗДІЛ 1

КОНЦЕПТУАЛЬНІ ЗАСАДИ ФОРМУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Зміст та значення інформаційної безпеки в розвитку суб'єктів підприємництва

Сучасні бізнес-процеси суб'єктів господарювання все частіше залежать від інформаційних технологій, що, з одного боку, підвищує ефективність управління та комунікацій, а з іншого – створює ризики витоку, спотворення або втрати важливих даних. Забезпечення інформаційної безпеки дозволяє захистити комерційні та фінансові дані підприємств, підтримувати довіру з боку партнерів і споживачів, а також уникати економічних втрат, пов'язаних із кібератаками та іншими загрозами. Інформаційна безпека визначає здатність суб'єктів підприємництва ефективно протистояти зовнішнім та внутрішнім загрозам, забезпечуючи стабільність економічного розвитку. Формування ефективної системи забезпечення інформаційної безпеки потребує комплексного підходу, що включає нормативно-правове регулювання, технічні засоби захисту, організаційно-економічні механізми та підвищення рівня цифрової грамотності суб'єктів.

Значення інформаційної безпеки для підприємницької діяльності полягає як у захисті конфіденційної інформації так і у забезпеченні конкурентоспроможності суб'єктів господарювання. Використання ефективних заходів інформаційної безпеки дозволяє підприємствам мінімізувати ризики, пов'язані з кіберзлочинністю, промисловим шпигунством та несанкціонованим доступом до даних. Інформаційна безпека є важливим чинником сталого та конкурентоспроможного розвитку бізнесу, сприяючи впровадженню інноваційних технологій, оптимізації управлінських процесів і підвищенню рівня довіри до пропонованої продукції чи послуг.

В умовах цифрової трансформації суспільства формується новий тип економіки, в якій концептуальним ресурсом виступає інформація, а її захист – важливим елементом функціонування суб'єктів підприємництва. Аналіз наукової літератури засвідчує використання різних підходів до приналежності інформаційної безпеки тому чи іншому типу економічної діяльності. В науковій літературі зустрічаються назви інформаційна економіка, цифрова економіка, економіка знань, а в деяких випадках – економіка кібербезпеки, залежно від специфіки акценту. Інформаційна економіка трактується науковцями як тип господарювання, в якому головну роль відіграє виробництво, зберігання, обробка і поширення інформації. У її межах інформаційна безпека стає основою довіри до електронних транзакцій, безпечного зберігання даних і сталого розвитку бізнесу. Такий підхід активно описаний у роботах науковців, наприклад М. Портера та В. Мілера [1], а також у звітах Організації економічного співробітництва та розвитку (OECD, 2015) [2].

Цифрова економіка концентрується на використанні цифрових технологій, інтернету, штучного інтелекту та великих даних для створення вартості. Тут інформаційна безпека розглядається як інфраструктурна складова, що забезпечує захист цифрових платформ, кіберпростору та бізнес-процесів. Наприклад, у «Digital Economy Outlook» від OECD (2020) зазначено, що стійкість цифрової економіки прямо залежить від рівня кіберзахисту [3].

Економіка знань є моделлю, де головними чинниками виробництва виступають знання, досвід, ноу-хау, інтелектуальна власність. Інформаційна безпека, у цьому випадку, необхідна для збереження унікальних технологій і конкурентних переваг. ЮНЕСКО у своїх звітах (2005, 2013) підкреслює роль знань як рушія інноваційної економіки [4, 5].

У вузькоспеціалізованих дослідженнях, науковці вживають термін «економіка кібербезпеки», яка охоплює ринок товарів і послуг з кіберзахисту, оцінку впливу кіберінцидентів на економіку, страхування кіберризиків тощо. Згідно зі звітами McKinsey (2022), ринок кібербезпеки стрімко зростає і має системний вплив на фінансову стійкість підприємств [6].

Усі зазначені підходи визнають інформацію стратегічним ресурсом, а її захист – необхідною умовою стабільного функціонування підприємств бізнесу, інноваційного розвитку та довіри до цифрового середовища. Інформаційна безпека забезпечує безперервність бізнес-процесів, збереження інтелектуального капіталу, мінімізацію фінансових і репутаційних ризиків, а також підтримку конкурентоспроможності підприємств у глобальному інформаційному просторі. Аналіз наукової літератури з досліджуваної проблеми засвідчує, що сьогодні спостерігають перехід до стратегії «розумної промисловості», що змінює традиційну орієнтацію виробництва на модель зорієнтовану на споживача, яка доповнюється цифровими технологіями сервісного обслуговування, де інформаційна безпека є основою успіху. Так, орієнтовані на конкурентоспроможне майбутнє виробники можуть досягти успіху, якщо забезпечать інформаційну безпеку та зроблять послуги з підтримкою цифрових технологій основою як свого бізнесу, так і операційних моделей.

Комплексність та багатогранність поняття інформаційної безпеки, яку в переважній більшості трактують як сукупність заходів, спрямованих на захист інформаційних ресурсів від несанкціонованого доступу, втрат, модифікації або зловмисного використання, зумовлює необхідність інтегрованого підходу до її забезпечення. В умовах стрімкого розвитку цифрових технологій та зростання кіберзагроз інформаційна безпека охоплює технічні аспекти, такі як захист баз даних, системи контролю доступу чи антивірусні рішення, а також організаційні, економічні та правові механізми. Зокрема, формування культури кібербезпеки серед працівників, запровадження політик управління ризиками та дотримання міжнародних стандартів у сфері захисту інформації є важливими складовими стійкої системи інформаційної безпеки. Такий підхід забезпечує захист важливих даних та сприяє стабільному функціонуванню підприємств, підтримці їх конкурентоспроможності та підвищенню рівня довіри з боку партнерів і споживачів.

Термін «інформаційна безпека» розвинувся наприкінці 80-х років у науковій праці німецького вченого Жаркова Я., де він намагався розкрити проблеми безпеки, що комплексно пов'язані з інформаційними загрозами. В українській науці проблеми інформаційної безпеки починають розглядатися з кінця 1991 року [7]. Досліджуючи інформаційну безпеку суб'єктів господарювання, вчені по-різному трактують дане поняття. Абакумов В. трактує поняття «інформаційна безпека підприємництва», як «сукупність заходів, визначених на рівні нормативно-правових актів, що регламентують підприємницьку діяльність і визначають особливості захисту інформації суб'єктами господарювання в Україні, та внутрішніх правил конкретного підприємства, спрямованих на захист інформаційного ресурсу підприємств, нейтралізацію та ліквідацію загроз ефективному функціонуванню інформаційної системи суб'єкта господарської діяльності зокрема та діяльності цього суб'єкта в цілому» [8]. Відповідно до Концепції інформаційної безпеки України досліджуване поняття розглядається як «стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, за якого попереджається шкода через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій» [9].

Аналіз наукової літератури засвідчує багатогранність поняття «інформаційна безпека». Вчені розглядають цю дефініцію з кількох позицій. В переважній більшості, науковці трактують поняття інформаційної безпеки з технічного, правового та соціального аспектів. Технічний аспект охоплює методи захисту інформаційних систем від несанкціонованого доступу, кібератак і збоїв, правовий – зосереджується на нормативно-правовому регулюванні інформаційної діяльності, включаючи законодавчі механізми захисту персональних даних та інтелектуальної власності, соціальний аспект передбачає

вплив інформаційної безпеки на суспільство, зокрема на інформаційну культуру, етику та рівень цифрової грамотності.

Зважаючи на мету нашого дослідження та багатогранність підходів вчених до змістовного наповнення поняття інформаційної безпеки, пропонуємо систематизувати підходи до визначення досліджуваного поняття на основ трьохвекторної площини, а саме: з позицій процесного підходу, де інформаційна безпека розглядається вченими як процес захисту суб'єктів підприємництва; з позицій проєктного підходу, як стану захищеності суб'єктів підприємництва; з позицій системного підходу, де запропоновано розглядати інформаційну безпеку, як складову економічної безпеки суб'єктів підприємництва (табл. 1.1).

Таблиця 1.1 – Систематизація підходів вчених до змісту поняття «інформаційна безпека»

Автори	Підхід до трактування
1	2
<i>Процесний підхід як процес захисту</i>	
Сороківська О., Гевко В.	«Суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності»
Козачок В.А., Гайдур Г.І., Гахов С.О.	«Події, які шляхом потенційно можливого впливу на інформаційну систему прямо та/або опосередковано завдають збитку її власникам і користувачам»
Забродський В.А., Кізім Н.А., Янов Л.І.	«Кількісна і якісна характеристика властивостей фірми, що відбиває здатність «самовиживання» і розвитку в умовах виникнення зовнішньої і внутрішньої економічної загрози»
Гладченко Т.Н.	«Захищеність життєво важливих інтересів підприємства від внутрішніх і зовнішніх загроз, організація якої здійснюється адміністрацією й колективом підприємства шляхом реалізації системи заходів правового, економічного, організаційного, інженерно-технічного й соціально-психологічного характеру»
Могильний А.І., Безчастний В.М., Винокуров Ю.О.	«Забезпечення стану життєдіяльності, при якому реалізуються його основні інтереси, воно захищено від внутрішніх та зовнішніх загроз і дестабілізуючих чинників»
<i>Проєктний підхід як стан захищеності</i>	
Кицюк В.М., Пупинін О.С.	«Стан інформаційного середовища господарюючого суб'єкта, при якому зберігаються властивості інформації й інформаційних потоків, та створюються умови протистояння впливу внутрішніх і зовнішніх загроз з метою досягнення бізнес-цілей підприємства»
Якименко Ю.М., Савченко В.А., Легомінова С.В.	«Стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держав»
Шульга В.І.	«Стан інформаційної системи, у якому вона може протистояти впливу внутрішніх і зовнішніх ризиків, не ініціюючи їхнє виникнення для елементів системи й зовнішнього середовища»
Хофман Л.	«Стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації»
Горбатюк О.	«Інформаційна безпека являє собою стан захищеності потреб в інформації особистості, суспільства і держави, за якого забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз»

Продовження табл. 1.1

1	2
Богущ В.	«Стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації»
Кочубей Л.О.	«Особливий стан захищеності життєво важливих інтересів та з ними інформаційної безпеки інформаційних суб'єктів, за якого будь-які інформаційні впливи на них не викликають деструктивних думок чи дій, результатом яких будуть негативні відхилення в розвитку цих предметів»
Чубаєвський В.І. (2023)	«Стан захищеності інтересів підприємства від недобросовісних дій (умисних та неумисних) щодо корпоративної інформації, що спрямовані на всі компоненти корпоративного інформаційного простору та доведено чіткий взаємозв'язок між захистом корпоративної інформації та досягненням високих економічних результатів функціонування підприємства, які і є відображенням його інтересів»
Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»	«Стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації»
<i>Системний підхід як складова економічної безпеки</i>	
Сніщенко Р.Г., Гринчуцький В.І.	«Інформаційна безпека підприємства як складова його економічної безпеки охоплює не тільки проблемну сферу втрат суб'єкта господарювання в результаті реалізації інформаційних загроз, а й проблемну сферу підвищення ефективності його діяльності в результаті впровадження сучасних інформаційних технологій»
Борзенкова О.Д., Шрамко О.О.	«Інформаційна безпека підприємства забезпечується заходами правового забезпечення щодо державної політики в напрямках правового поля, прав та обов'язків суб'єктів, зокрема інформаційного права; організаційного забезпечення, що визначає правила та заходи надходження та обробки інформації на підприємстві; програмно-технічного забезпечення, що уможливорює захист інформації за допомогою технічних засобів, а також надає можливість прийняття технічних рішень»
Озарко К., Андрухів Т.	«Складова економічної безпеки та охоплює проблемну сферу втрат суб'єктів господарювання в результаті реалізування інформаційних загроз та проблемну сферу підвищення рівня ефективності їх діяльності у результаті розроблення, впровадження та використання сучасних інформаційних технологій»
Бехтер А.А.	«Одна із основних складових економічної безпеки виступає станом захищеності діяльності підприємства, його інформаційного середовища від негативного впливу дестабілізуючих чинників, яке забезпечує збереження основних властивостей інформації, досягнення соціальних, економічних цілей створення підприємства»
<i>Інституційно-системний підхід, як механізм формування стійкого середовища суб'єкта підприємництва</i>	
Власне бачення	«Діагностичний процес захищеності інформаційного середовища суб'єкта підприємництва, який забезпечує збереження, доступність, цілісність та конфіденційність інформації, дозволяючи мінімізувати ризики впливу внутрішніх і зовнішніх загроз, а також сприяючи досягненню стратегічних та економічних цілей шляхом формування та впровадження інклюзивних інституцій, як інструменту сталого розвитку суб'єктів підприємництва»

Джерело: складено автором на основі [10-26].

Проведений аналіз даної проблеми засвідчив, що інформаційна безпека розглядається науковцями з різних підходів. Процесний підхід акцентує увагу на заходах і процесах, які забезпечують захист інформаційного середовища суб'єкта господарювання. Вчені, що підтримують цей підхід (Сороківська О., Гевко В., Козачок В., Гайдур Г., Гахов С., Забродський В., Кізім Н., Янов Л., Гладченко Т., Могильний А., Безчастний В., Винокуров Ю.), визначають інформаційну безпеку як стан, що захищає від внутрішніх та зовнішніх загроз, забезпечуючи функціонування підприємства. Деякі дослідники трактують її як характеристику здатності підприємства до виживання і розвитку в умовах інформаційних загроз.

Проектний підхід, прихильниками якого є Кицюк В., Пупинін О., Якименко Ю., Савченко В., Легомінова С., Шульга В., Хофман Л., Горбатюк О., Богуш В., Кочубей Л., Чубаєвський В., зосереджується на стані захищеності інформаційного середовища, в якому зберігаються властивості інформації та інформаційних потоків. Такий підхід враховує як внутрішні, так і зовнішні загрози та їхній вплив на підприємство, державу та суспільство загалом. Особливо важливим у цьому контексті є забезпечення збереження інформації, її доступності та цілісності, що дозволяє підприємствам уникати небажаних наслідків, пов'язаних із несанкціонованим доступом чи втратами важливих даних.

Аналіз наукової літератури підтверджує, що інформаційна безпека є невід'ємною складовою економічної безпеки суб'єктів підприємництва. Системний підхід інтегрує інформаційну безпеку в загальну економічну безпеку підприємства. Він розглядає інформаційний захист як один із основних чинників стабільного функціонування підприємства, що запобігає втратам через інформаційні загрози та сприяє підвищенню ефективності діяльності за рахунок впровадження сучасних інформаційних технологій. Таким чином, інформаційна безпека постає як захист від загроз та як стратегічний інструмент розвитку підприємств у цифрову епоху.

Дослідники зазначають, що в умовах цифровізації та глобалізації бізнес-процесів роль інформаційної складової в забезпеченні економічної безпеки значно зросла. Зокрема, Сніщенко Р. та Гринчуцький В. у своїй роботі наголошують на необхідності розробки політик кібербезпеки та впровадження систем моніторингу загроз для захисту інформаційних ресурсів підприємств [23]. Інші науковці, такі як Борзенкова О. та Шрамко О., акцентують увагу на важливості інтеграції інформаційної безпеки в загальну систему економічної безпеки підприємства. Вони зазначають, що захищеність інформаційного середовища сприяє мінімізації чинників впливу та загроз в умовах мінливого зовнішнього середовища [24]. Озарко К., Андрухів Т. вважають інформаційну безпеку підприємств складовою економічної безпеки, яка охоплює проблемну сферу втрат суб'єктів господарювання в результаті реалізування інформаційних загроз та проблемну сферу підвищення рівня ефективності їх діяльності у результаті формування, впровадження та використання інформаційних технологій [25]. Бехтер А. розглядає інформаційну безпеку як одну з складових економічної безпеки, яка виступає станом захищеності діяльності підприємства, його інформаційного середовища від негативного впливу дестабілізуючих чинників, яке забезпечує збереження основних властивостей інформації, досягнення соціальних, економічних цілей створення підприємства [26].

Таким чином, аналіз наукової літератури засвідчує, що інформаційна безпека є важливим елементом економічної безпеки підприємств, а її забезпечення вимагає комплексного підходу, який включає технічні, організаційні та правові заходи. На основі проведеного аналізу та зважаючи на мету нашого дослідження, пропонуємо трактувати інформаційну безпеку як *динамічний процес захищеності інформаційного середовища суб'єкта підприємництва, який забезпечує збереження, доступність, цілісність та конфіденційність інформації, дозволяючи мінімізувати ризики впливу внутрішніх і зовнішніх загроз, а також сприяючи досягненню стратегічних та економічних цілей за рахунок формування та впровадження інклюзивних інституцій, як інструменту сталого розвитку суб'єктів підприємництва.*

Інклюзивні інституції, будучи базисом для прозорого управління, рівного доступу до інформаційних ресурсів і справедливого регулювання, забезпечують підприємствам стабільне нормативне та правове середовище, в якому інформаційна безпека регламентується та ефективно впроваджується на практиці. Вони сприяють поширенню культури цифрової відповідальності, підвищують рівень довіри між бізнесом, державою та суспільством, що є важливим чинником в умовах цифровізації економіки та зростання кіберзагроз. У результаті, підприємства отримують змогу реагувати на ризики та ефективно управляти інформаційною безпекою як стратегічним активом.

Ряд дослідників вважає, що інформаційна безпека, виходячи з двоєдиної суті інформації має бути направлена як на захист об'єктивної, так і суб'єктивної її складової. У першому випадку вона виступає у вигляді безпеки інформації, в другому – у вигляді інформаційно-психологічної безпеки [27].

У контексті дослідження проблем забезпечення інформаційної безпеки суб'єктів підприємництва доцільно враховувати, що інформація як об'єкт захисту має дві сутнісні складові – об'єктивну та суб'єктивну. Ряд дослідників наголошує, що комплексна інформаційна безпека повинна охоплювати технічний і організаційний захист даних та інформаційно-психологічний аспект, пов'язаний із впливом інформаційного середовища на свідомість персоналу, управлінські рішення та репутацію підприємства [28]. З одного боку, безпека інформації передбачає збереження цілісності, конфіденційності та доступності даних, з іншого – необхідність протидії маніпуляціям, дезінформації та інформаційним атакам, які можуть негативно впливати на поведінку працівників і стратегічні позиції підприємства. Такий підхід розширює традиційне розуміння інформаційної безпеки і дозволяє формувати більш ефективні моделі захисту, що враховують і технологічні ризики і людський фактор.

В умовах стрімкої цифровізації економіки та зростання рівня інформаційних загроз проблема забезпечення інформаційної безпеки є особливо актуальною для суб'єктів підприємництва. Ефективне функціонування будь-якого підприємства залежить як від технічного захисту інформації, так і від

системного управління всіма елементами, які формують її безпеку загалом. На нашу думку, доцільно застосувати функціонально-компонентний підхід, що дозволяє комплексно дослідити внутрішні та зовнішні чинники впливу на інформаційну безпеку, а також розкрити її зміст через призму основних характеристик – конфіденційності, цілісності, доступності, регламентованості та адаптивності [29]. Такий підхід сприяє інтеграції системи інформаційної безпеки у загальну стратегію управління підприємством та забезпечує стійкість до викликів сучасного інформаційного середовища. Функціонально-компонентний підхід до змісту інформаційної безпеки підприємств візуалізовано на рис. 1.1.



Рис. 1.1. Функціонально-компонентний підхід до змісту інформаційної безпеки підприємств

Джерело: розроблено автором.

У межах запропонованого підходу до забезпечення інформаційної безпеки підприємств, доцільно розглядати її як багатокomпонентну систему, функціонування якої забезпечується взаємодією внутрішніх і зовнішніх чинників. Такий функціонально-компонентний підхід, базується на принципі системності та комплексності, що дозволяє структурувати зміст інформаційної безпеки та ідентифікувати її основні складові з урахуванням як технічних, так і організаційно-управлінських аспектів.

Інформаційна безпека підприємства як складова його стратегічного управління, включає сукупність характеристик, що забезпечують цілісне та ефективне функціонування системи захисту. Відповідно до змісту нашого дослідження, основними серед них є: цілісність (як гарантія збереження інформації від несанкціонованих змін); конфіденційність (як захист критичних даних від доступу третіх осіб); доступність (як забезпечення оперативного доступу до інформації в потрібний момент); регламентованість (як відповідність внутрішнім політикам та зовнішнім стандартам); економічна ефективність (як оптимальне співвідношення витрат на безпеку і потенційних втрат); комплексність (як охоплення технічних, організаційних, правових і кадрових заходів тощо); адаптивність та динамічність (як здатність системи оперативно реагувати на зміни в інформаційному середовищі) [30].

З позицій функціонально-компонентного підходу внутрішні процеси впливу інформаційної безпеки формуються в межах самого підприємства та підлягають прямому управлінському впливу. До них належать організаційна структура, система доступу до даних, кадрова політика, регламентована документація, внутрішні стандарти та технічна інфраструктура. Такі процеси визначають функціональні межі інформаційної безпеки як складника внутрішньої корпоративної культури та загальної бізнес-стратегії підприємства.

Зовнішні процеси відображають вплив середовища, у якому діє підприємство, це законодавчі вимоги, державна політика у сфері кіберзахисту, технологічні тенденції, діяльність підрядників, ризики кіберзлочинності. Такі компоненти хоча і є менш контрольованими, проте потребують постійного

моніторингу та адаптації системи інформаційної безпеки відповідно до змін. Залучення зовнішніх консультантів, аудитів і кіберстрахування стає невід'ємною частиною захисту в умовах відкритої економіки.

Вважаємо за доцільне зазначити, що уваги в межах функціонально-компонентного підходу заслуговує подвійна природа інформації – об'єктивна та суб'єктивна. Захист об'єктивної інформації охоплює технічні аспекти збереження даних, програмного забезпечення, баз даних, внутрішніх систем. Захист суб'єктивної інформації (інформаційно-психологічної складової) полягає у запобіганні дезінформації, впливу на свідомість персоналу, маніпуляціям або поширенню фейків, які можуть вплинути на прийняття управлінських рішень [31]. Обидві складові мають бути інтегрованими у систему безпеки підприємства на рівні політик, процедур і технологічних рішень.

Таким чином, інформаційна безпека розглядається як інтегрована функціональна система, яка є частиною загальної стратегії управління підприємством. Застосування функціонально-компонентного підходу до розкриття змісту інформаційної безпеки підприємств дозволяє сформулювати цілісне уявлення про її складову структуру та взаємозв'язки між елементами системи захисту, а також розробити модель формування системи інформаційної безпеки підприємства, адаптовану до умов сучасного ринкового середовища, з урахуванням специфіки сфери економічної діяльності, масштабу діяльності, типу інформаційних активів та ступеня ризику. Такий підхід сприяє інтеграції інформаційної безпеки в загальну стратегію підприємства, посиленню її адаптивності до змін зовнішнього середовища та підвищенню рівня стійкості підприємства до сучасних викликів цифрової економіки.

Зважаючи на специфіку дослідження та багатогранність змістовного наповнення інформаційної безпеки суб'єктів підприємництва, пропонуємо визначити структурні взаємозв'язки інформаційної безпеки суб'єктів підприємництва на основі представленої схеми (рис. 1.2).



Рис. 1.2. Логіка взаємозв'язку інформаційної безпеки суб'єктів підприємництва.

Джерело: складено автором.

Запропонована структура взаємозв'язків інформаційної безпеки суб'єктів підприємництва демонструє її комплексний характер, оскільки вона тісно взаємодіє з іншими складовими загальної системи безпеки підприємства. Економічна безпека є одним з основних елементів конкурентоспроможного розвитку суб'єктів підприємництва, адже інформаційні загрози можуть призвести до фінансових втрат, втрати конкурентних переваг і зниження прибутковості. Репутаційна безпека пов'язана із захистом іміджу підприємства від негативних інформаційних впливів, витоків конфіденційної інформації та маніпуляцій у медіапросторі. Соціальна безпека забезпечує стабільність у трудовому колективі, запобігаючи деструктивним впливам на співробітників через інформаційні атаки або маніпуляції. Юридична безпека регулює дотримання нормативно-правових актів у сфері інформаційного захисту, включаючи дотримання законів про персональні дані та кібербезпеку.

Деталізація структури інформаційної безпеки також включає організаційну та технічну безпеку, що вказує на необхідність створення ефективних механізмів управління інформаційними ризиками. Організаційна безпека передбачає впровадження політик інформаційної безпеки, проведення аудитів та навчання персоналу, тоді як технічна безпека орієнтована на використання засобів шифрування, систем моніторингу та кіберзахисту.

Важливими підсистемами є криптографічний захист, що забезпечує конфіденційність даних, адміністративна безпека, яка регулює доступ до інформаційних ресурсів, операційна безпека, спрямована на контроль за обробкою даних, та фізична безпека, що захищає інфраструктуру підприємства від несанкціонованого доступу. Таким чином, проведений аналіз доводить, що інформаційна безпека є технічним та стратегічним аспектом функціонування сучасного підприємства.

Суб'єкти підприємництва за своїм змістом та сутністю являють собою діяльність, спрямовану на організацію, виробництво, обмін і розподіл товарів та послуг з метою отримання прибутку, задоволення потреб ринку та забезпечення власної конкурентоспроможності. Така діяльність базується на принципах самостійності, ініціативності, інноваційності та ризиковості, що визначає підприємництво як динамічний процес, який постійно адаптується до змін зовнішнього середовища. Важливою складовою успішного функціонування підприємницької діяльності є ефективне управління ресурсами, включаючи фінансові, матеріальні, інформаційні та людські. Забезпечення інформаційної безпеки суб'єктів підприємництва може бути досягнуто шляхом захисту інформаційних ресурсів підприємства, інформаційного забезпечення виробничих або сервісних процесів, а також протидії негативного впливу зовнішнього потоку інформації (рис. 1.3).

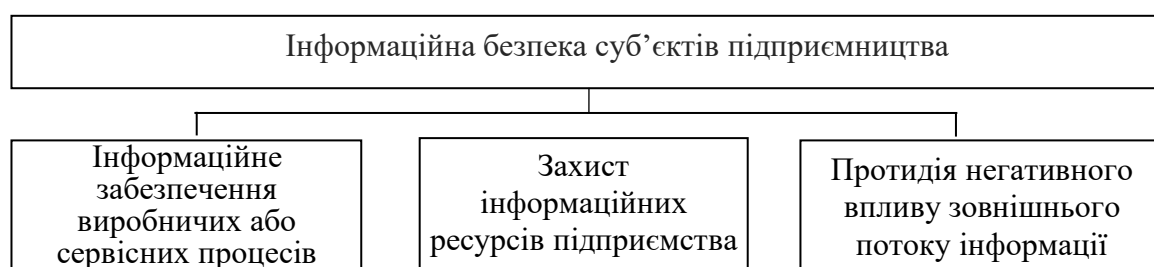


Рис. 1.3. Структура інформаційної безпеки суб'єктів підприємництва.

Джерело: складено автором.

Структурні компоненти інформаційної безпеки суб'єктів підприємництва, охоплюють три основні напрями, а саме: захист інформаційних ресурсів

підприємства, протидію негативному впливу зовнішнього потоку інформації та інформаційне забезпечення виробничих або сервісних процесів. Такий підхід підкреслює важливість комплексного забезпечення інформаційної безпеки, оскільки сучасні підприємства функціонують у цифровому середовищі, де інформація є стратегічним активом. Захист інформаційних ресурсів спрямований на мінімізацію ризиків втрати, витоку або модифікації важливих даних, що може негативно вплинути на діяльність підприємства [30]. Такий підхід включає технічні заходи, такі як шифрування, контроль доступу, резервне копіювання та кіберзахист.

Протидія негативному впливу зовнішнього потоку інформації має особливе значення у сучасному бізнес-середовищі, де підприємства часто стикаються з інформаційними атаками, маніпуляціями, неправдивими відомостями та іншими видами інформаційного впливу. Такий підхід передбачає моніторинг інформаційного середовища, управління корпоративною репутацією, боротьбу з дезінформацією та формування стратегії інформаційного захисту. Важливою складовою є також інформаційна гігієна серед працівників підприємства, що допомагає мінімізувати внутрішні загрози, пов'язані з необачним поведінням із корпоративною інформацією.

Важливим є інформаційне забезпечення виробничих або сервісних процесів, яке забезпечує ефективний доступ до необхідних даних та їхню своєчасну обробку, що включає інтеграцію сучасних інформаційних систем, автоматизацію бізнес-процесів, підтримку систем управління підприємством та використання великих даних для прийняття стратегічних рішень. Забезпечення інформаційної безпеки виробничих або сервісних процесів суб'єктів підприємництва торкається документів підприємства, технологій виробництва, нових товарів та послуг, електронних носіїв, знань та ділових взаємовідносин суб'єкта підприємництва (рис. 1.4). У цьому контексті важливим є комплексний підхід до захисту інформаційних активів, що включає впровадження сучасних технологій кібербезпеки, контроль доступу до конфіденційних даних, резервне копіювання важливої інформації та використання засобів шифрування.

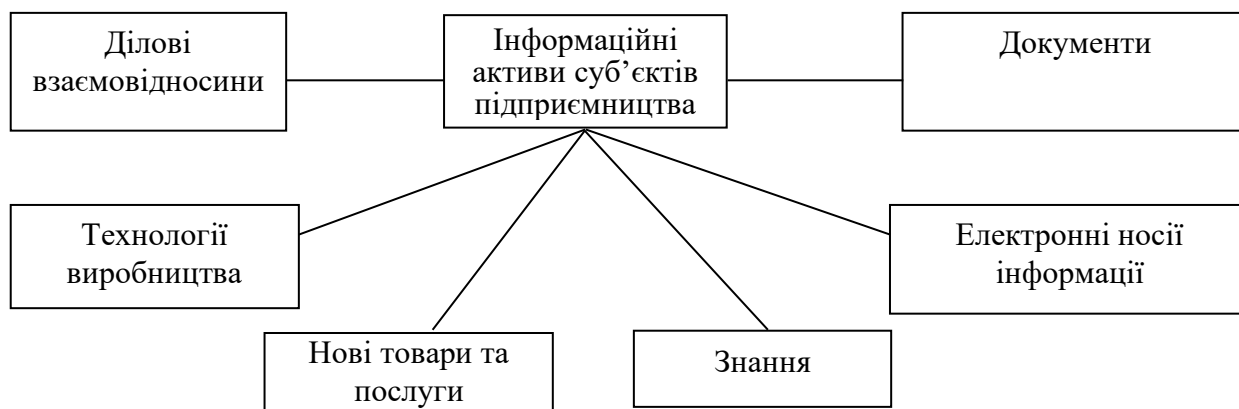


Рис. 1.4. Інформаційні активи суб'єктів підприємництва як об'єкт інформаційної безпеки.

Джерело: складено автором.

Особливу увагу слід приділити захисту інтелектуальної власності підприємства, адже витік інформації про нові технології, розробки або бізнес-стратегії може призвести до втрати конкурентних переваг. Також доцільно враховувати ризики, пов'язані з використанням електронних носіїв, хмарних сервісів та дистанційного доступу до корпоративних ресурсів, що потребує чіткої політики інформаційної безпеки. Крім того, ділові взаємовідносини суб'єкта підприємництва повинні бути захищені через укладання договорів про конфіденційність із працівниками, партнерами та постачальниками, що допоможе мінімізувати ризики витоку комерційної таємниці [32]. Забезпечення інформаційної безпеки виробничих або сервісних процесів підприємства є важливим елементом загальної системи безпеки, що гарантує стійкість та ефективність його діяльності в умовах сучасного інформаційного середовища.

Ефективне забезпечення інформаційної безпеки потребує як впровадження технічних засобів захисту та і чітко визначеної системи функціональних завдань, які охоплюють усі аспекти діяльності організації. У цьому контексті важливо дослідити функції інформаційної безпеки як структурні складові, що забезпечують превентивний захист, контроль, реагування, відновлення та стратегічне управління ризиками. Аналіз зазначених функцій дозволяє

сформувати цілісну систему управління інформаційною безпекою відповідно до потреб сучасного підприємницького середовища.

Інформаційна безпека підприємства виконує низку важливих функцій, які забезпечують захист інформаційних ресурсів, мінімізацію ризиків, підвищення стійкості до зовнішніх і внутрішніх загроз, а також підтримку безперервності бізнес-процесів (табл. 1.2).

Таблиця 1.2 – Функції інформаційної безпеки підприємств

Функції	Зміст функцій
Захисна функція	Забезпечення конфіденційності, цілісності та доступності інформації; протидія несанкціонованому доступу, витоку, втраті або модифікації даних.
Моніторингова	Постійне спостереження за станом інформаційної системи, виявлення потенційних загроз і вразливостей.
Превентивна	Ідентифікація ризиків, вжиття заходів для їх усунення або мінімізації до настання інциденту.
Аналітична	Оцінка ефективності заходів безпеки, аналіз подій, аудит систем захисту.
Регламентуюча	Розробка внутрішніх політик, процедур, інструкцій щодо поводження з інформацією та реагування на інциденти.
Інформаційно-освітня	Підвищення обізнаності працівників щодо правил інформаційної безпеки, проведення тренінгів, навчань, інструктажів.
Відновлювальна	Реагування на інциденти, відновлення пошкоджених даних або систем, мінімізація наслідків.
Економічна	Рациональне використання ресурсів на заходи безпеки, оцінка ефективності інвестицій у кіберзахист.
Управлінська	Формування та реалізація стратегії інформаційної безпеки, інтеграція ІБ у загальну систему управління підприємством.

Джерело: систематизовано автором на основі [27, 28, 31, 32].

Система функцій інформаційної безпеки підприємства відображає багатовимірний та системний підхід до організації захисту інформаційних ресурсів. Такі функції можна класифікувати відповідно до результатів впливу. Наприклад, превентивні, контрольні, аналітичні, відновлювальні та стратегічні. Так, захисна, моніторингова та превентивна функції спрямовані на виявлення та недопущення загроз, зниження рівня ризиків і забезпечення сталого функціонування інформаційної інфраструктури. Такі функції формують першочергову лінію оборони підприємства та базуються на принципах конфіденційності, цілісності та доступності даних. У свою чергу, аналітична, регламентуюча та інформаційно-освітня функції, забезпечують оцінку

ефективності заходів безпеки, розробку нормативно-процедурної бази та формування культури безпеки серед працівників.

Одну з важливих ролей у забезпеченні цілісного управління інформаційною безпекою відіграють економічна, відновлювальна та управлінська функції.

Економічна функція дає змогу оптимізувати витрати на інформаційної безпеки у співвідношенні з потенційними втратами, пов'язаними з інцидентами. Відновлювальна функція орієнтована на мінімізацію негативних наслідків після порушень інформаційної безпеки шляхом оперативного реагування та відновлення пошкоджених систем і даних. Управлінська функція має стратегічний характер і передбачає інтеграцію політики інформаційної безпеки у загальну систему управління підприємством, що забезпечує її узгодженість із бізнес-цілями організації. У сукупності зазначені функції формують функціональну модель, здатну адаптуватися до сучасних викликів цифрової економіки та забезпечити стабільність і стійкість підприємства в інформаційному середовищі.

Системи взаємопов'язаних функцій забезпечує комплексний підхід до захисту інформаційних ресурсів, що дозволяє запобігати загрозам і оперативно реагувати на інциденти, а також інтегрувати заходи безпеки в управлінські, економічні та освітні процеси підприємства [24]. Такий підхід сприяє підвищенню адаптивності суб'єктів господарювання до сучасних викликів кіберсередовища та формує підґрунтя для сталого функціонування й збереження конкурентоспроможності в умовах цифрової трансформації.

Забезпечення інформаційної безпеки на підприємстві базується на дотриманні низки принципів, які регламентують підходи до організації, управління та контролю в цій сфері. Такі принципи формують основу функціонування ефективної та адаптивної системи захисту інформаційних ресурсів у сучасному цифровому середовищі.

Принципи забезпечення інформаційної безпеки підприємства систематизовано в таблиці 1.3.

Таблиця 1.3 – Принципи забезпечення інформаційної безпеки підприємства

Принцип	Зміст принципів
Комплексність	Забезпечення захисту на всіх рівнях: технічному, організаційному, правовому, кадровому та інформаційному.
Системність	Інформаційна безпека як цілісна система з узгодженими компонентами: технологіями, людьми, процесами.
Безперервність	Система безпеки має функціонувати постійно й адаптуватися до змін.
Пріоритет превентивних заходів	Основна увага приділяється запобіганню загрозам, а не лише реагуванню на інциденти.
Мінімізація прав доступу	Надання працівникам мінімально необхідного рівня доступу.
Персональна відповідальність	Кожен елемент інформаційної безпеки має відповідального виконавця.
Прозорість і контрольованість	Можливість контролю, аудиту й відстеження дій у системі.
Відповідність стандартам	Забезпечення дотримання законодавчих норм та міжнародних стандартів (ISO, NIST тощо).
Адаптивність	Спроможність системи змінюватися відповідно до нових загроз.
Економічна доцільність	Баланс між рівнем захисту та витратами на його досягнення.
Інклюзивної інституційності	Залучення всіх зацікавлених сторін до досліджуваних процесів.

Джерело: доповнено автором на основі [27, 28, 29, 31, 32].

До основних принципів інформаційної безпеки віднесемо: комплексність, що передбачає захист на всіх рівнях (технічному, організаційному, правовому та кадровому); системність – як визнання безпеки цілісною системою взаємопов’язаних компонентів; безперервність – як необхідність постійного моніторингу, оновлення та вдосконалення заходів захисту; пріоритет превентивних заходів – як фокус на попередженні загроз; мінімізація прав доступу – як забезпечення лише необхідного рівня доступу користувачам; персональна відповідальність – як чіткий розподіл обов’язків та визначення відповідальних осіб; прозорість і контрольованість – як можливість здійснення аудиту та перевірок; відповідність стандартам – як дотримання міжнародних та національних нормативних вимог; адаптивність – як спроможність реагувати на нові виклики; а також економічна доцільність – як забезпечення балансу між витратами та рівнем безпеки.

Принцип інклюзивної інституційності в інформаційній безпеці підприємства передбачає активну участь усіх зацікавлених сторін – керівництва, персоналу, зовнішніх партнерів, регуляторів – у формуванні, впровадженні та контролі політик захисту інформації. Такий підхід базується на ідеї відкритості, залучення та відповідальності кожного учасника інформаційного процесу, що дозволяє створити стійке інституційне середовище для підтримки інформаційної безпеки. Інклюзивність забезпечує кращу комунікацію між рівнями управління та підвищує ефективність системи безпеки за рахунок більшої обізнаності, узгодженості дій та формування культури інформаційної відповідальності в організації.

Система принципів інформаційної безпеки підприємства формується як багаторівнева концептуальна основа для побудови ефективної та стійкої політики захисту інформаційних ресурсів. Принцип інклюзивної інституційності акцентує увагу на важливості залучення всіх зацікавлених сторін до досліджуваних процесів, що підвищує прозорість, адаптивність і відповідальність усередині суб'єкта господарювання. Сукупне застосування зазначених принципів створює цілісну модель інформаційної безпеки, здатну ефективно функціонувати в умовах постійної зміни цифрового середовища та зростання інформаційних загроз.

Отже, інформаційна безпека є важливим елементом сталого функціонування та стратегічного розвитку суб'єктів підприємництва в умовах цифрової трансформації економіки. Її зміст охоплює захист інформаційних ресурсів від внутрішніх і зовнішніх загроз, а також формування умов для безперервності бізнес-процесів, збереження конкурентних переваг та довіри з боку партнерів і споживачів.

Забезпечення належного рівня інформаційної безпеки сприяє зниженню ризиків, підвищенню інвестиційної привабливості та інтеграції підприємств у глобальні економічні процеси, виступаючи при цьому не витратною статтею, а стратегічним активом сучасного бізнесу.

1.2 Забезпечення інформаційної безпеки як детермінанта конкурентоспроможного розвитку підприємства

У сучасних умовах цифрової трансформації інформаційна безпека стала основним чинником стабільного та ефективного функціонування підприємств. Зростання обсягів даних, використання хмарних технологій та розширення дистанційних форматів роботи створюють як нові можливості, так і додаткові загрози. Несанкціонований доступ, витік конфіденційної інформації або кібератаки можуть спричинити значні фінансові втрати, порушення ділових процесів та зниження рівня довіри з боку споживачів та партнерів.

Забезпечення інформаційної безпеки підприємств, передбачає комплексний підхід, що включає технічні, організаційні та правові механізми захисту. Інвестиції в сучасні засоби кібербезпеки, навчання персоналу, контроль доступу до важливої інформації та впровадження політик управління ризиками є невід’ємними складовими стратегії сталого розвитку підприємства. Ефективна інформаційна безпека мінімізує ризики та сприяє підвищенню конкурентоспроможності, формуванню позитивного іміджу компанії та зміцненню довгострокових партнерських відносин. Інформаційна безпека є стратегічним чинником розвитку бізнесу [33]. Вона впливає на всі аспекти діяльності підприємства, від збереження комерційної таємниці до підтримки стабільності операційних процесів. Усвідомлення важливості цієї складової та впровадження ефективних механізмів її забезпечення дозволяє компаніям адаптуватися до нових викликів, знижувати ризики та розвиватися в умовах глобальної цифрової економіки.

Сьогодні, очевидно є залежність рівня цифровізації підприємств від рівня їх добробуту і темпів економічної динаміки. Високий рівень цифрової досконалості дозволяє компаніям ефективніше використовувати ресурси, оптимізувати бізнес-процеси та швидше адаптуватися до змін ринкового середовища. Підприємства, які активно впроваджують сучасні інформаційні технології, підвищують свою продуктивність та зміцнюють конкурентні позиції,

що, у свою чергу, сприяє їх фінансовій стійкості та інвестиційній привабливості. Недостатній рівень цифровізації може обмежувати можливості зростання, збільшувати операційні ризики та знижувати ефективність захисту інформації, що негативно позначається на загальному рівні розвитку бізнесу.

В умовах зростаючої ролі інформації у функціонуванні підприємства, збільшуються ризики втрати інформації, особливо внаслідок кібератак. Зловмисники використовують все складніші методи для отримання несанкціонованого доступу до конфіденційних даних, що може призвести до фінансових втрат, репутаційних ризиків та правових наслідків для компанії. Тому, впровадження комплексних заходів кібербезпеки, таких як багаторівнева система автентифікації, шифрування даних, регулярний моніторинг загроз і навчання персоналу основам інформаційної безпеки, є важливими для запобігання можливим атакам [34]. Захист інформації, на нашу думку, повинен стати не разовою ініціативою суб'єкта господарювання, а безперервним процесом, який дозволяє підприємству ефективно реагувати на нові виклики цифрової епохи.

Доцільність запровадження заходів забезпечення інформаційної безпеки суб'єктів підприємництва декларується як на рівні держави, так і на рівні окремих суб'єктів господарювання. Так, відповідно до Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр.», основними пріоритетами відповідно до теми нашого дослідження є створення умов для розвитку інформаційної інфраструктури, забезпечення кібербезпеки та підвищення рівня цифрової грамотності суб'єктів господарювання. Зокрема, законодавство акцентує увагу на необхідності впровадження сучасних технологій захисту інформації, розвитку систем електронного документообігу та створення ефективного механізму управління інформаційними ресурсами. Також, серед основних напрямів визначено формування державної політики у сфері інформаційної безпеки, що передбачає гармонізацію національних стандартів із міжнародними вимогами та адаптацію бізнесу до глобальних цифрових викликів. Таким чином, реалізація зазначених пріоритетів сприятиме

підвищенню стійкості суб'єктів підприємництва до інформаційних загроз, зміцненню їх конкурентних позицій та створенню безпечного середовища для ведення бізнесу.

У наукових працях вчених, значна увага приділяється забезпеченню економічної безпеки підприємств, складовою якої є інформаційна безпека. Вчені наголошують, що ефективний захист інформаційних ресурсів є важливим чинником стабільного функціонування бізнесу, оскільки дозволяє мінімізувати ризики фінансових втрат, запобігти витоку конфіденційних даних та уникнути зловживань з боку конкурентів або кіберзлочинців [33]. Дослідження також підкреслюють взаємозв'язок між рівнем цифрової безпеки та загальною конкурентоспроможністю підприємства, адже високий рівень інформаційного захисту сприяє підвищенню довіри з боку партнерів, споживачів і державних інституцій. Крім того, значна увага приділяється питанням розробки стратегій інформаційної безпеки, інтеграції сучасних технологій захисту даних та вдосконалення нормативно-правового регулювання у цій сфері, що дозволяє забезпечити комплексний підхід до управління ризиками в умовах цифрової економіки.

В умовах цифровізації бізнесу та зростання кіберзагроз інформаційна безпека набуває важливого значення для стабільного функціонування підприємств. Ефективна система захисту інформаційних ресурсів неможлива без чіткого розуміння суб'єктного складу, який бере участь у процесах її формування, впровадження та підтримки. Визначення та категоризація учасників інформаційної безпеки суб'єктів підприємництва, дозволяє розподілити відповідальність на окремі аспекти захисту та забезпечити скоординовану взаємодію між усіма залученими сторонами в межах внутрішнього середовища підприємства та його зовнішніх зв'язків. Категоризація учасників процесу забезпечення інформаційної безпеки суб'єктів підприємництва систематизовано в таблиці 1.4.

Таблиця 1.4 – Категоризація учасників процесу забезпечення інформаційної безпеки підприємства

Категорії	Основні функції
<i>Зовнішні учасники</i>	
Контрагенти, партнери	Обмін даними, підписання договорів з ІБ-застереженнями (NDA, SLA тощо).
Провайдери ІТ-послуг, хостингів	Надання інфраструктури, програмних рішень, хмарних сервісів.
Аудитори, консалтингові компанії	Проведення аудитів інформаційної безпеки, сертифікація, оцінка ризиків.
Державні органи	Контроль за дотриманням законодавства, розслідування інцидентів.
Страхові компанії	Пропонують кіберстрахування на випадок інформаційних інцидентів.
<i>Внутрішні учасники</i>	
Керівництво підприємства	Прийняття стратегічних рішень, затвердження політики ІБ, фінансування заходів.
ІТ-відділ, технічні фахівці	Впровадження технічних засобів захисту, адміністрування систем, моніторинг загроз.
Служба безпеки, служба ІБ	Розробка процедур безпеки, контроль доступу, розслідування інцидентів.
Працівники, користувачі	Дотримання внутрішніх правил ІБ, відповідальне поводження з даними.
Відділ кадрів, юристи	Формування політик конфіденційності, захист персональних даних, супровід юридичних аспектів ІБ.

Джерело: систематизовано автором на основі [30, 32, 33, 34].

Система інформаційної безпеки підприємства є багаторівневою та багатокомпонентною структурою, яка передбачає участь різних категорій суб'єктів. На нашу думку, доцільним є розподіл учасників інформаційної безпеки на внутрішні та зовнішні. Внутрішні учасники – це структурні одиниці самого підприємства, як наприклад, керівництво, яке формує політику безпеки; ІТ-відділ, що впроваджує технічні засоби захисту; служба безпеки, яка контролює дотримання правил; юридичні та кадрові служби, відповідальні за правову підтримку; а також всі працівники, які щоденно працюють з інформацією [30]. Їхня взаємодія забезпечує реалізацію системного, комплексного підходу до інформаційної безпеки в межах організації.

Зовнішні учасники, зі свого боку, не входять до штату підприємства, але значною мірою впливають на загальний рівень його інформаційної захищеності. До них належать контрагенти, провайдери цифрових послуг, аудитори,

консалтингові фірми, державні органи, а також страхові компанії, що надають послуги кіберстрахування. Їхня участь є основою в забезпеченні відповідності підприємства зовнішнім стандартам, законодавчим вимогам та регуляторним нормам [32]. Такий розподіл учасників дозволяє створити комплексну систему управління інформаційними ризиками, яка враховує як внутрішні процеси, так і зовнішнє середовище функціонування підприємства.

В умовах цифровізації бізнес-процесів та зростання кіберзагроз питання забезпечення інформаційної безпеки набуває стратегічного значення для підприємств різних сфер. Інформація перетворюється на основний ресурс, а її захист – на важливу умову стабільного функціонування, збереження конкурентних переваг і довіри з боку партнерів та споживачів. Прийняття рішень щодо інвестування в інформаційну безпеку потребує врахування як зовнішніх викликів, так і внутрішніх характеристик підприємства, що визначає доцільність дослідження та визначення чинників, які впливають на ці процеси. Основні чинники, що впливають на рішення суб'єктів підприємництва інвестувати в інформаційну безпеку систематизовано на рис. 1.5.



Рис. 1.5. Чинники, що впливають на рішення суб'єктів підприємництва інвестувати в інформаційну безпеку

Джерело: систематизовано автором на основі [33, 34].

Комплекс системи чинників, що впливають на рішення суб'єктів підприємництва інвестувати в інформаційну безпеку, відображає системний підхід до управління інформаційною безпекою як до складового елементу стратегічного розвитку підприємства. Такі чинники пропонуємо розділити на дві категорії – зовнішні та внутрішні, що підкреслює багаторівневу природу прийняття рішень у зазначеній сфері.

Зовнішні чинники включають ті умови, які формуються поза межами підприємства, але мають значний вплив на його політику безпеки. Зокрема, конкурентний тиск змушує компанії впроваджувати сучасні заходи інформаційного захисту для збереження ринкових позицій. Репутаційні ризики стимулюють інвестиції в безпеку, оскільки витік конфіденційної інформації може мати серйозні наслідки для іміджу компанії. Загрози з боку кіберзлочинців дедалі частіше стають рушієм технологічного переоснащення ІТ-систем. Крім того, регуляторні вимоги та законодавство зобов'язують дотримуватись стандартів безпеки, порушення яких може призвести до санкцій. До цієї ж групи належать організація інформаційної безпеки на глобальному рівні, страхування кіберризиків як інструмент фінансового захисту, та глобальні тенденції, які визначають загальний вектор розвитку цифрової безпеки.

Внутрішні чинники відображають внутрішній потенціал та особливості самого підприємства. Рівень цифрової досконалості показує, наскільки підприємство готове до впровадження та підтримки інформаційної безпеки. Фінансові можливості безпосередньо впливають на обсяги інвестування в цю сферу. Наявність ІТ-інфраструктури забезпечує технічну базу для реалізації заходів безпеки. Вкрай важливим, на нашу думку, є власний досвід кіберзагроз, який формує усвідомлення важливості захисту даних. Вимоги керівництва та стратегічні пріоритети вказують на роль управлінських рішень у формуванні політики безпеки. Цінність і важливість даних визначають економічну доцільність інвестицій у їх захист.

Науково обґрунтовані рішення підприємств щодо інвестування в інформаційну безпеку, формуються під впливом як об'єктивних зовнішніх

чинників, так і суб'єктивних внутрішніх характеристик, та є частиною комплексного стратегічного управління. Рішення суб'єктів підприємництва щодо інвестування в інформаційну безпеку є результатом взаємодії зовнішніх загроз та внутрішніх ресурсів підприємства, що зумовлює необхідність системного підходу до управління ризиками. Усвідомлення цінності даних як стратегічного активу стає важливим мотиватором для створення інтегрованої системи інформаційної безпеки, що є передумовою сталого функціонування та конкурентоспроможності сучасного підприємства.

На шляху до формування ефективної системи забезпечення інформаційної безпеки, суб'єкти підприємництва стикаються з численними викликами та бар'єрами, які мають різну природу та ступінь впливу залежно від масштабів бізнесу. Недостатність фінансування, нестача кваліфікованих кадрів, технічна застарілість інфраструктури та опір змінам є типовими труднощами, що обмежують здатність суб'єктів підприємництва адаптуватися до зростаючих загроз [34].

Додаткову загрозу становлять застарілі ІТ-інфраструктури, слабкий контроль доступу до інформаційних ресурсів, низький рівень цифрової культури та слабка взаємодія суб'єктів підприємництва з державними інституціями у сфері кіберзахисту. Усе зазначене ускладнює своєчасне реагування на інциденти безпеки та знижує загальну стійкість підприємства до зовнішніх і внутрішніх загроз, що вимагає стратегічного переосмислення підходів до інформаційної безпеки на всіх рівнях управління. Аналіз таких викликів і бар'єрів дає змогу сформулювати цілісне уявлення про проблематику інформаційної безпеки в підприємницькому середовищі та визначити напрямки для підвищення її ефективності. Виклики та можливі бар'єри забезпечення інформаційної безпеки суб'єктів підприємництва систематизовано на рис. 1.6.



Рис. 1.6. Виклики та можливі бар'єри забезпечення інформаційної безпеки суб'єктів підприємництва.

Джерело: розроблено автором.

Систематизований комплекс викликів та бар'єрів, що стоять перед суб'єктами підприємництва в процесі забезпечення інформаційної безпеки дозволяє визначити основні перешкоди на шляху до створення ефективної системи інформаційного захисту та виявити залежність між масштабом підприємства і типом ризиків, з якими воно стикається. Виокремлено як

універсальні виклики в сфері інформаційної безпеки, так і специфічні труднощі, що характерні для підприємств малого, середнього та великого бізнесу. Загальні виклики в сфері інформаційної безпеки включають чинники, що формують глобальне середовище загроз. До них належать зростання кіберзлочинності, витоки даних, гібридна війна, а також необхідність інтегрувати безпеку у всі бізнес-процеси [35]. Однією з важливих проблем, на нашу думку, є недостатня обізнаність персоналу, що створює ризик внутрішніх загроз. Регуляторні вимоги також тиснуть на підприємства, змушуючи їх адаптовуватись до нових стандартів захисту.

Виклики та бар'єри, в залежності від типу підприємства, відображають особливості ресурсного забезпечення та організаційної структури бізнесу. Наприклад, малий бізнес, стикається з обмеженими фінансами, нестачею знань і відсутністю формалізованих політик. Середній бізнес має справу з розширеною ІТ-інфраструктурою та зовнішнім тиском з боку партнерів. Великий бізнес, змушений протистояти складним атакам, управляти масштабними кіберризиками та відповідати міжнародним стандартам безпеки.

Можливі бар'єри забезпечення інформаційної безпеки пропонуємо поділяти на фінансові, технічні та організаційні. Фінансові бар'єри охоплюють високу вартість технічних рішень, навчання персоналу і сертифікації. Технічні бар'єри включають використання застарілого обладнання, відсутність фахівців і складність інтеграції безпекових систем. Організаційні проблеми зумовлені низьким рівнем уваги керівництва до інформаційної безпеки, опором до змін та браком кризових стратегій тощо.

Такий підхід формує цілісне уявлення про багаторівневі загрози та обмеження в інформаційній безпеці, дозволяючи виокремити пріоритетні напрямки для удосконалення процесу забезпечення інформаційної безпеки з урахуванням розміру, ресурсів та організаційної культури підприємства. Система бар'єрів ускладнює реалізацію заходів захисту, особливо для малого та середнього бізнесу, який має обмежені можливості адаптації до динамічних умов цифрового середовища. У великого бізнесу зростає складність управління

ризиками через масштаб цифрової інфраструктури та необхідність дотримання міжнародних норм, що вимагає стратегічного підходу до забезпечення інформаційної безпеки, орієнтованого на інституційне зміцнення, підвищення цифрової культури персоналу та інтеграцію безпеки у всі рівні управління підприємством.

У сучасному цифровому середовищі інформаційна безпека перетворюється на один із чинників ефективного функціонування підприємств. З огляду на зростання загроз, підвищену цінність даних та жорсткі регуляторні вимоги, суб'єкти підприємництва все частіше усвідомлюють необхідність інвестування у системи захисту інформації. Проте, забезпечення інформаційної безпеки не слід розглядати лише як захисну функцію, вона набуває ознак стратегічного ресурсу, здатного створювати додаткову цінність для бізнесу. У цьому контексті аналіз стимулів, що спонукають суб'єктів підприємництва до впровадження заходів з забезпечення інформаційної безпеки, є важливою умовою формування ефективної, проактивної політики захисту. Стимули забезпечення інформаційної безпеки суб'єктів підприємництва систематизовано на рис. 1.7.



Рис. 1.7. Стимули забезпечення інформаційної безпеки суб'єктів підприємництва.

Джерело: розроблено автором

Стимули забезпечення інформаційної безпеки суб'єктів підприємництва відображають багатовекторну мотивацію бізнес-структур до впровадження заходів з забезпечення інформаційної безпеки, що дозволяє розглядати таку безпеку і як відповідь на загрози і як інструмент стратегічного розвитку та підвищення конкурентоспроможності підприємств. Пропонуємо систему стимулів, згрупувати в чотири категорії – економічні, регуляторні, репутаційні та стратегічні, що загалом формує обґрунтовану модель зацікавленості суб'єктів господарювання у забезпеченні належного рівня інформаційної безпеки.

Економічні стимули є важливим умовою для підприємств, оскільки дозволяють зменшити фінансові ризики, уникати непрямих витрат, пов'язаних із кіберінцидентами, а також оптимізувати загальні витрати на ІТ-забезпечення. Важливою перевагою є доступ до страхування кіберризиків, яке набирає популярності як інструмент управління ризиками. Ефективна система безпеки може стати джерелом конкурентної переваги та відкривати можливості для залучення грантів або державної підтримки, що особливо актуально для малих та середніх підприємств.

Регуляторні стимули пов'язані із необхідністю дотримання вимог законодавства в сфері кібербезпеки, що дозволяє уникати фінансових санкцій, юридичної відповідальності та репутаційних втрат. Також відповідність нормативним актам спрощує вихід підприємств на міжнародні ринки, де дотримання стандартів кіберзахисту часто є обов'язковою умовою партнерства.

Репутаційні стимули відіграють суттєву роль у формуванні довіри з боку споживачів, інвесторів та партнерів. Надійний захист даних зміцнює імідж компанії, підвищує лояльність споживачів і запобігає репутаційним втратам у разі інцидентів [36]. В умовах інформаційного суспільства, де публічність кіберзагроз є високою, репутаційна стійкість стає важливою конкурентною характеристикою.

Стратегічні стимули включають довгострокові вигоди, такі як підвищення стійкості бізнесу до зовнішніх і внутрішніх загроз, забезпечення безперервності операцій, підтримка цифрової трансформації та можливість залучення нових

партнерів. Інформаційна безпека в цьому контексті розглядається як основний чинник стратегічної стабільності та адаптивності підприємства в умовах динамічного цифрового середовища.

Такий підхід доводить, що забезпечення інформаційної безпеки є як витратною необхідністю так і умовою сталого розвитку, що формує конкурентоспроможність, довіру та інноваційний потенціал сучасного бізнесу. Стимули забезпечення інформаційної безпеки суб'єктів підприємництва мають багатовимірний характер і охоплюють економічні, регуляторні, репутаційні та стратегічні аспекти, що свідчить про її інтегровану роль у сучасному бізнес-середовищі. Вони знижують ризики та втрати від потенційних кіберінцидентів, та створюють передумови для сталого розвитку суб'єктів підприємництва, посилення ринкових позицій та зміцнення довіри з боку зацікавлених сторін.

У сучасних умовах кіберінциденти здатні призвести до фінансових втрат, репутаційних ризиків, переривання операційної діяльності та юридичної відповідальності. Відтак забезпечення ефективного захисту інформаційних ресурсів вимагає системного підходу, який охоплює як технічні рішення так і управлінські, організаційні та нормативно-правові аспекти [35]. Зростаюча складність цифрового середовища зумовлює потребу в постійному вдосконаленні політик безпеки, інфраструктури та підвищенні обізнаності персоналу.

Вивчення чинників, що впливають на ефективність інформаційної безпеки суб'єктів підприємництва, дозволяє сформулювати цілісне уявлення про основні умови забезпечення стійкості підприємства до кіберзагроз. Пропонуємо до чинників впливу на ефективність забезпечення інформаційної безпеки суб'єктів підприємництва віднести фінансові ресурси, цифрову досконалість, рівень ІТ-інфраструктури, кадрову компетентність, відповідність законодавству, актуальні загрози, довіру споживачів та геополітичні виклики. Такий підхід дозволяє ідентифікувати сильні та слабкі сторони існуючих систем безпеки та орієнтує управлінські рішення на досягнення високого рівня стійкості підприємства в динамічному цифровому середовищі (таблиця 1.5).

Таблиця 1.5 – Чинники впливу на ефективність забезпечення інформаційної безпеки суб'єктів підприємництва

Категорія чинників	Вплив на ефективність забезпечення інформаційної безпеки
Фінансові ресурси	Чим більше коштів виділено, тим якісніший захист можна забезпечити.
Цифрова досконалість бізнесу	Рівень автоматизації та використання цифрових технологій визначає потребу в інформаційній безпеці.
Кваліфікація персоналу	Висока обізнаність персоналу зменшує ризик людських помилок.
Рівень IT-інфраструктури	Сучасні технології, регулярне оновлення програмного забезпечення та засоби захисту покращують безпеку.
Політики та стандарти безпеки	Чіткі політики доступу, управління ризиками та дотримання стандартів підвищують захист.
Реакція на кіберінциденти	Наявність плану реагування на інциденти забезпечує швидке відновлення роботи після атак.
Регуляторні вимоги та законодавство	Дотримання законодавчих норм дозволяє уникнути штрафів та санкцій.
Кіберзагрози та хакерські атаки	Постійне вдосконалення методів захисту необхідне через еволюцію кіберзагроз.
Довіра споживачів та партнерів	Компанії з надійною ІБ користуються більшою довірою серед клієнтів та партнерів.
Технологічні тренди	Впровадження нових технологій, таких як Zero Trust, допомагає адаптувати безпеку до сучасних викликів.
Глобальні події та геополітична ситуація	Глобальні конфлікти, кібератаки на державному рівні впливають на рівень безпеки підприємств.

Джерело: складено автором.

Визначені чинники, що впливають на ефективність забезпечення інформаційної безпеки суб'єктів підприємництва, відображають системний підхід до аналізу інформаційної безпеки, акцентуючи увагу на взаємозалежності внутрішніх ресурсів підприємства, зовнішніх загроз і нормативно-правового середовища. Кожен чинник має своє функціональне значення в побудові цілісної моделі інформаційної безпеки. Фінансові ресурси відіграють базову роль, оскільки масштаб і якість захисних заходів безпосередньо залежать від обсягів інвестицій. Недостатнє фінансування часто призводить до застарілого обладнання, обмеженої кількості фахівців та вразливої інфраструктури. Цифрова досконалість бізнесу визначає рівень інтеграції IT у всі бізнес-процеси, що прямо пов'язано з обсягом і складністю завдань щодо інформаційної безпеки. Чим вищий рівень цифровізації, тим більше виникає точок потенційного доступу до критичних даних.

Кваліфікація персоналу є важливим чинником у контексті запобігання помилкам та несанкціонованим діям. Людський фактор залишається одним із головних джерел вразливостей, тому підвищення цифрової грамотності персоналу має важливе значення. Рівень IT-інфраструктури, включаючи оновлення програмного забезпечення та захисних засобів, впливає на здатність підприємства оперативно реагувати на загрози. Політики та стандарти безпеки, зокрема політики доступу, управління ризиками та дотримання міжнародних стандартів, формують нормативну основу ефективної інформаційної безпеки. Реакція на кіберінциденти демонструє рівень готовності підприємства до кризових ситуацій: наявність планів реагування забезпечує швидке відновлення діяльності та мінімізацію збитків. Регуляторні вимоги та законодавство стимулюють відповідальне ставлення до інформаційної безпеки через правові механізми впливу, а кіберзагрози та хакерські атаки змушують підприємства постійно адаптувати та вдосконалювати свої системи захисту [34].

Довіра споживачів та партнерів має стратегічне значення, адже надійна інформаційна безпека зміцнює репутацію підприємства, сприяє залученню нових партнерів і споживачів. Технологічні тренди, такі як «Zero Trust», хмарні рішення, блокчейн тощо, формують нові стандарти безпеки та забезпечують конкурентоспроможність. Глобальні події та геополітична ситуація виступають зовнішніми модифікаторами рівня загроз – у часи міжнародної напруженості або воєнного конфлікту зростає ризик таргетованих кібератак на бізнес-структури. Тому, ефективне забезпечення інформаційної безпеки є результатом комплексної взаємодії внутрішніх можливостей підприємства, технологічного рівня, кадрової підготовки та зовнішнього середовища, що підтверджує необхідність інтегрованого підходу до процесу захисту інформації в умовах сучасної цифрової економіки. Показник ефективності забезпечення інформаційної безпеки суб'єктів підприємництва залежить від цілісної взаємодії фінансових, технологічних, організаційних та зовнішньополітичних чинників. Зовнішні умови (дотримання регуляторних вимог, врахування технологічних трендів і адаптація до глобальних викликів), суттєво впливають на стратегічну

стійкість підприємства, що підтверджує необхідність комплексного, адаптивного підходу до формування системи інформаційної безпеки як важливої складової цифрового розвитку бізнесу.

З огляду на мету нашого дослідження, пропонуємо для побудови блоку цільової функції забезпечення інформаційної безпеки застосувати методологію «IDEF0» [37], яка дає змогу побудувати графічну модель, що відображає логіку забезпечення інформаційної безпеки суб'єктів підприємництва на основі взаємодії основних елементів: входних даних, механізмів реалізації, управлінських впливів і результатів. У контексті нашого дослідження основна функція – забезпечення інформаційної безпеки – представлена у вигляді центрального блоку, що підпорядковується впливу нормативно-правових актів, внутрішньої політики підприємства та міжнародних стандартів (рис. 1.8).

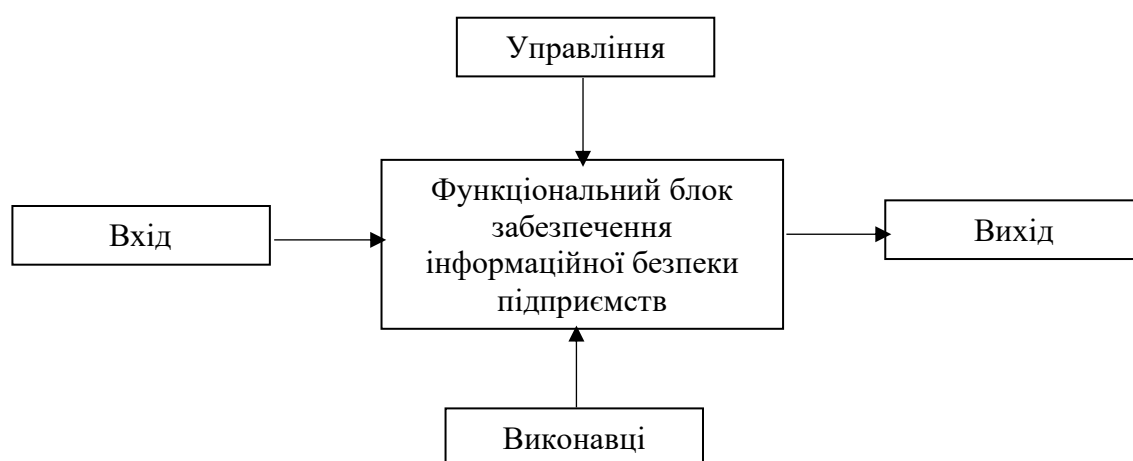


Рис. 1.8. Блок цільової функції забезпечення безпеки.

Джерело: доопрацьовано автором з використанням методології «IDEF-0» [37].

Функціональна модель «IDEF0», розроблена для відображення процесу забезпечення інформаційної безпеки суб'єктів підприємництва, демонструє взаємодію основних компонентів системи безпеки: інформаційних ресурсів як входних даних, нормативно-правового регулювання та внутрішньої політики як механізмів управління, технічних і людських ресурсів як виконавців, і результатів у вигляді захищеного інформаційного середовища. Така структура дозволяє візуально формалізувати процеси захисту інформації, виявити критичні

точки контролю, забезпечити системний підхід до управління ризиками та створити основу для оптимізації політик безпеки на всіх рівнях діяльності підприємства. Функціонально-компонентний підхід до змісту інформаційної безпеки підприємств візуалізовано на рис. 1.9.

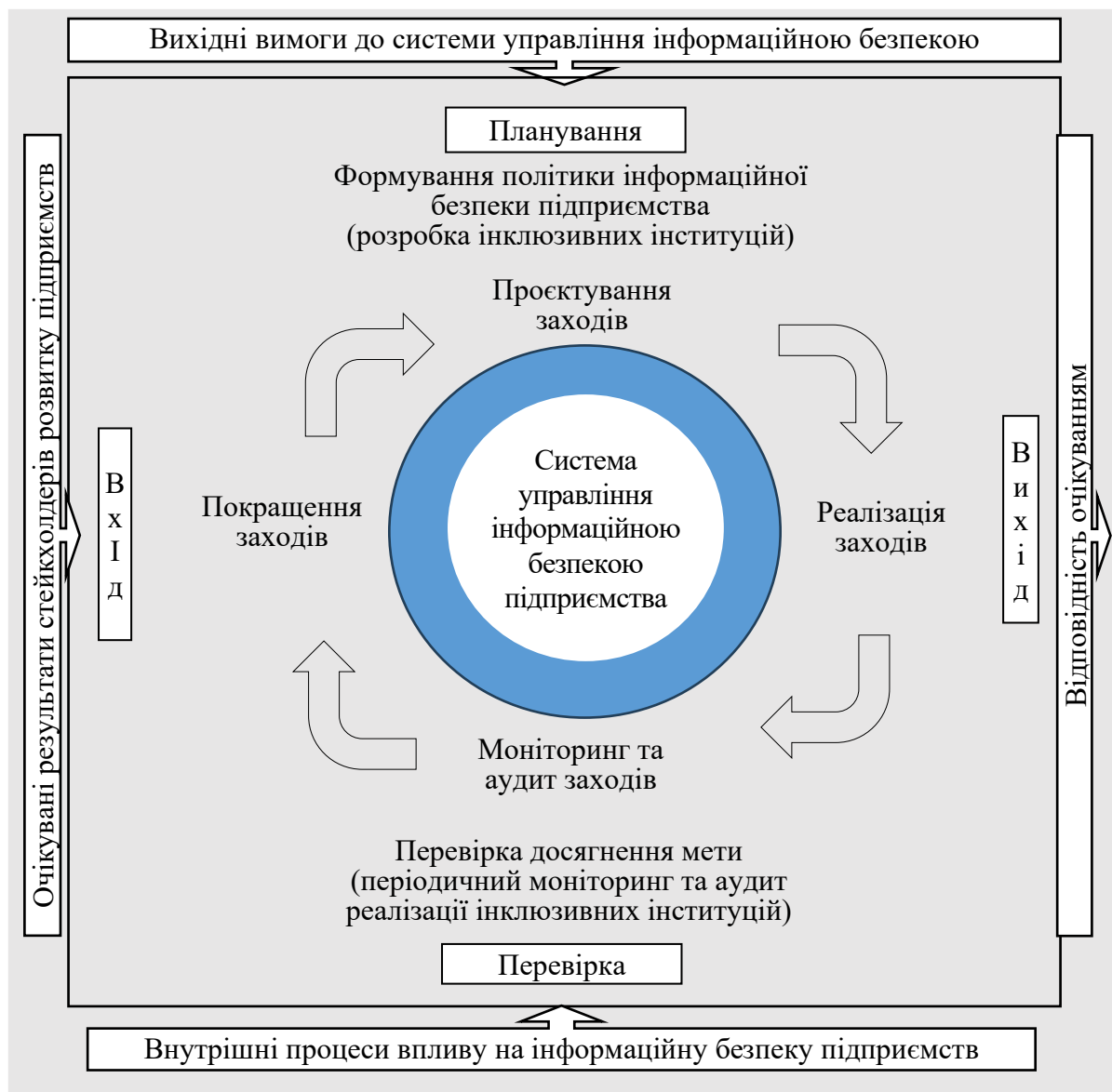


Рис. 1.9. Організаційна модель системи управління інформаційною безпекою суб'єктів господарювання.

Джерело: розроблено автором

Організаційна модель системи управління інформаційною безпекою підприємства є циклічною структурою управління, що базується на принципах системного підходу, управління якістю та інституційної інтеграції. Вона поєднує

вимоги зовнішнього середовища, очікування зацікавлених сторін, внутрішні процеси та періодичну оцінку ефективності як елементи цілісної системи інформаційної безпеки.

Запропонована система управління інформаційною безпекою містить в основі вихідні вимоги, які відображають як зовнішні нормативно-правові та ринкові чинники, так і очікування стейкхолдерів (споживачів, партнерів, інвесторів). Формування політики інформаційної безпеки з урахуванням цих вимог є важливим управлінським рішенням. У цьому випадку, розробка інклюзивних інституцій слугує механізмом правового, організаційного та етичного супроводу системи, підвищуючи її адаптивність і прозорість.

Цикл управління інформаційною безпекою, структуровано за логікою моделі «PDCA» (Plan-Do-Check-Act), яка широко використовується в системах управління якістю, зокрема ISO/IEC 27001. Етап планування передбачає розробку заходів із забезпечення інформаційною безпекою, далі доцільно реалізувати заходи та здійснити моніторинг і аудит, після чого потрібно сформувати алгоритм з посилення заходів – внесення змін, спрямованих на зменшення ризиків та усунення виявлених недоліків.

Актуальною частиною запропонованої моделі є перевірка відповідності очікуванням, що підкреслює важливість регулярного аудиту результатів роботи системи з урахуванням інтересів стейкхолдерів. В даному випадку, під управлінням інформаційною безпекою будемо вважати внутрішньоорганізаційний процес та стратегічну взаємодія з зовнішнім середовищем. Такий підхід створює передумови для підвищення довіри, відкритості та ефективності управлінських рішень. Запропонована організаційна модель, являє собою інтегровану систему, яка включає регуляторний, процесний, інституційний і стратегічний рівні управління. Така модель здатна адаптуватися до змін і забезпечувати як стійкість підприємства до загроз, так і підтримку його конкурентоспроможності в умовах цифрової економіки сьогодення.

Розроблена організаційна модель системи управління інформаційною безпекою підприємства підтверджує, що ефективне забезпечення досліджуваних процесів є результатом цілеспрямованого, системного та інтегрованого підходу, який враховує як внутрішні ресурси підприємства, так і зовнішні регуляторні та ринкові вимоги. Важливим елементом такої системи виступає безперервний управлінський цикл «планування – реалізація – контроль – вдосконалення», що забезпечує адаптацію до змін, підвищення якості управлінських рішень і зменшення ризиків кіберзагроз. Значною перевагою моделі, є її спрямованість на інституційну сталість і врахування очікувань усіх зацікавлених сторін, що дозволяє забезпечити захист інформаційних активів та формувати довіру до підприємства як учасника цифрової економіки. В умовах глобальної цифровізації, зростання кіберризиків і євроінтеграційного курсу України, така модель управління інформаційною безпекою повинна розглядатися як стратегічний інструмент забезпечення конкурентоспроможності, стійкості та інноваційного розвитку вітчизняних суб'єктів підприємництва.

Сьогодні стабільність діяльності суб'єктів підприємництва, дедалі більше залежить від надійності інформаційних систем та захищеності даних. Тож, у сучасних умовах цифрової трансформації економіки питання забезпечення інформаційної безпеки набуває особливого значення для суб'єктів підприємництва, [38]. Зростання кількості та складності кіберзагроз вимагає від бізнесу технічних рішень та системного підходу до побудови цілісної стратегії безпеки, що враховує організаційні, нормативні, управлінські та людські чинники. У цьому контексті актуальним є формування науково обґрунтованої, концептуальної моделі інформаційної безпеки, яка дозволить підприємствам адаптуватися до ризикового середовища та забезпечити сталий розвиток в умовах цифрової економіки. Концептуальні засади забезпечення інформаційної безпеки суб'єктів підприємництва представлено на рис. 1.10.



Рис. 1.10. Концептуальні засади забезпечення інформаційної безпеки суб'єктів підприємництва.

Джерело: розроблено автором

Концептуальні засади забезпечення інформаційної безпеки суб'єктів підприємництва є цілісною моделлю, що відображає сучасний науково-обґрунтований підхід до побудови ефективної системи управління інформаційною безпекою в умовах цифрової трансформації бізнесу. Згідно з цією моделлю, інформаційна безпека не є лише технічним процесом захисту, а виступає інтегрованим управлінським механізмом, який охоплює стратегічні цілі, функціональні завдання, принципи дії, нормативне регулювання та постійне адаптування до нових викликів.

Основною метою досліджуваних процесів є формування та підтримка ефективної системи управління інформаційною безпекою, що забезпечує стійкість підприємства до загроз та його економічну стабільність. Досягнення цієї мети передбачає реалізацію важливих цілей, серед яких забезпечення конфіденційності, цілісності та доступності інформації, захист активів від несанкціонованого доступу, відповідність нормативним вимогам, а також підвищення довіри з боку споживачів і партнерів.

У межах запропонованої концепції, визначено вісім основних функцій інформаційної безпеки, до яких віднесено: захисну, моніторингову, попереджувальну, аналітичну, інформаційно-освітню, відновлювальну, економічну та управлінську. Такий функціональний спектр засвідчує, що інформаційна безпека є міждисциплінарною сферою, яка охоплює як технічні процеси, так і управлінські рішення, а також соціально-інституційні компоненти. Концептуальне підґрунтя моделі доповнено принципами, що включають системність, безперервність, ризик-орієнтованість, мінімізацію ризиків, контроль і аудит, а також відкритість та довіру, що є базовими умовами для побудови сучасної стійкої системи інформаційної безпеки.

Організаційні заходи включають формування політики інформаційної безпеки, створення регламентів, навчання персоналу, призначення відповідальних осіб, управління інцидентами, впровадження резервного копіювання, а також використання автоматизованих систем моніторингу. Важливим елементом концептуального підходу є процес постійного

вдосконалення, який відображає здатність системи реагувати на новітні загрози шляхом тестувань, аудитів, аналізу інцидентів та адаптації стратегії.

Концептуальний підхід передбачає врахування джерела загроз, як зовнішніх (потoki інформації, кібератаки), так і внутрішніх (інформаційна незахищеність у виробничих процесах, помилки персоналу), що свідчить про глибоке розуміння складності ризикового середовища. Процес управління інцидентами, націлений на зменшення негативного впливу загроз, попередження їх повторення та збереження ділової репутації. Такий підхід базується на поєднанні системного, ризик-орієнтованого та інституційного аспектів щодо управління інформаційною безпекою підприємств. Запропонований підхід, формує методологічну основу для впровадження політик, регламентів і технічних рішень, спрямованих на забезпечення стабільності, конкурентоспроможності та цифрової стійкості підприємств.

Запропонована концептуальна модель забезпечення інформаційної безпеки суб'єктів підприємництва демонструє цілісний та науково обґрунтований підхід до побудови дієвої системи інформаційної безпеки, яка охоплює як стратегічні, так і операційні компоненти. Поєднання функціональних завдань, основних принципів, організаційних заходів та циклу безперервного вдосконалення дозволяє підприємствам ефективно протидіяти сучасним інформаційним загрозам та забезпечувати стійкість, довіру з боку партнерів і відповідність вимогам цифрового ринку. Така модель, є важливим інструментом управління інформаційними ризиками та підтримки конкурентоспроможності бізнесу в умовах цифровізації економіки.

1.3 Світовий та вітчизняний досвід забезпечення інформаційної безпеки суб'єктів підприємництва

У сучасних умовах глобалізації та цифрової трансформації інформаційна безпека набуває вирішального значення для сталого розвитку суб'єктів підприємництва. Постійне зростання обсягів обробки даних, розширення

цифрових інфраструктур, використання хмарних сервісів та мобільних технологій створюють нові можливості для бізнесу, тим самим підвищуючи його вразливість до кіберзагроз. Тому, питання кіберзахисту вже давно вийшло за межі технічної сфери та стало стратегічним елементом корпоративного управління. Аналіз світового досвіду досліджуваної проблеми свідчить, що успішні моделі забезпечення інформаційної безпеки базуються на комплексному підході, який поєднує технічні рішення, нормативно-правову регламентацію, організаційні механізми та культуру кібергігієни. Розвинені країни активно впроваджують інноваційні концепції, такі як «Security by Design», «Zero Trust», кіберстійкість, а також використовують міжнародні стандарти (ISO/IEC 27001, NIST, GDPR), що створюють єдині рамки для управління інформаційними ризиками. Значну роль у цьому процесі відіграє державне регулювання, публічно-приватне партнерство, сертифікація постачальників ІТ-послуг та обов'язкове навчання персоналу [39].

Визначення кращих світових практик забезпечення інформаційної безпеки є важливим та необхідним для формування ефективних політик у цій сфері, а також для адаптації найкращих практик у діяльність українських підприємств, що дозволить підвищити їх цифрову стійкість, зміцнити довіру споживачів та партнерів, забезпечити відповідність міжнародним вимогам, а також підготувати бізнес до викликів сучасного кіберсередовища, яке є доволі мінливим.

У глобалізованому цифровому середовищі, де кібератаки стають все більш складнішими та масштабнішими, забезпечення інформаційної безпеки перетворюється на стратегічний пріоритет для суб'єктів підприємництва. Зростаюча кількість загроз, посилення регуляторних вимог, зміна форматів ведення бізнесу та геополітична нестабільність вимагають впровадження сучасних, комплексних підходів до кіберзахисту. У цьому випадку, світові тренди формують нові стандарти забезпечення безпеки, спрямовані на технічний захист та на посилення цифрової стійкості, безперервності діяльності та довіри з боку партнерів та споживачів. Аналіз таких трендів, дозволяє виявити основні

напрямки розвитку інформаційної безпеки, які доцільно враховувати підприємствам для адаптації до сучасних викликів (таблиця 1.6).

Таблиця 1.6 – Світові тренди забезпечення інформаційної безпеки суб'єктів підприємництва

Тренди	Зміст тренду	Приклади підприємств
Zero Trust	Модель повної перевірки всіх користувачів і пристроїв без винятку	Google, Microsoft, Cisco
Хмарна безпека	Захист даних у хмарних середовищах за допомогою шифрування, контролю доступу	Amazon (AWS), Dropbox, Salesforce
AI, ML у кіберзахисті	Застосування штучного інтелекту для виявлення загроз у реальному часі	Darktrace, IBM, CrowdStrike
Інтеграція безпеки у стратегію	Інформаційна безпека стає стратегічною частиною управління	Siemens, JPMorgan Chase
Кіберстійкість	Здатність швидко відновлюватися після атак	Cisco, IBM, Maersk
Кіберстрахування	Фінансове покриття збитків від кіберінцидентів	AIG, Allianz, Zurich Insurance
Дотримання стандартів	Виконання ISO/IEC 27001, GDPR, NIST та ін.	SAP, Oracle, Facebook
Security-as-a-Service	Аутсорсинг кібербезпеки як послуга	Palo Alto Networks, Fortinet, Arctic Wolf
Захист у ланцюгах постачання	Безпека партнерських систем і постачальників	Apple, Toyota, Unilever
Кіберзахист у геополітичних умовах	Зміцнення кібербезпеки на тлі геополітичних загроз	Lockheed Martin, Huawei, Raytheon

Джерело: систематизовано автором на основі [39].

Світові тренди в сфері інформаційної безпеки підприємств відображають глибокі трансформації в підходах до управління кіберзахистом в умовах глобалізації, цифровізації економіки та зростання кіберзагроз. Такі тенденції засвідчують перехід від реактивної моделі безпеки до проактивної, стратегічно орієнтованої парадигми, де інформаційна безпека інтегрується в усі рівні управління організацією. Такий підхід, відповідає концепції системного управління ризиками, в основі якого лежить захист інформаційних активів, цифрової стійкості, безперервності бізнесу та довгострокової конкурентоспроможності.

Одним із основних трендів є впровадження моделі «Zero Trust», яка змінює традиційне уявлення про периметральну безпеку, підкреслюючи необхідність безперервної перевірки кожного запиту на доступ. Крім того, активне

використання штучного інтелекту та машинного навчання в системах виявлення та реагування на загрози демонструє поступ до автоматизації функцій кіберзахисту, що підвищує його швидкість, адаптивність і ефективність. Упровадження хмарної безпеки відповідає загальносвітовій діджиталізації, створюючи потребу в надійному захисті даних у віртуальних середовищах. Така динаміка зумовлює зростання попиту на «Security-as-a-Service» та кіберстрахування, що особливо актуально для малого та середнього бізнесу, який не має змоги створити власну кіберінфраструктуру.

Крім технологічних аспектів, тренди стосуються і стратегічного рівня – зокрема, інтеграція кібербезпеки в корпоративну стратегію свідчить про усвідомлення її як основного бізнес-активу, а не лише технічної функції. Зростає значення дотримання міжнародних стандартів і нормативних актів, таких як ISO/IEC 27001, GDPR, NIST, що забезпечують уніфікований підхід до управління безпекою в міжнародному бізнес-середовищі. Крім того, геополітична нестабільність, активізація гібридних загроз та державного кібершпиунства обумовлюють необхідність посиленого захисту критичної інфраструктури, зокрема у великих транснаціональних корпораціях.

Аналіз досліджуваної проблеми засвідчує, що сучасні світові тренди кібербезпеки демонструють перехід до гнучких, адаптивних і орієнтованих на довгострокову стійкість моделей, у яких інформаційна безпека є інструментом захисту та фундаментальним елементом цифрової трансформації бізнесу і запорукою його стабільності в умовах глобальних ризиків. Аналіз світових трендів у сфері забезпечення інформаційної безпеки суб'єктів підприємництва свідчить про глибоку трансформацію ролі кіберзахисту. Визначені тренди демонструють, що інформаційна безпека є невід'ємною складовою цифрової трансформації бізнесу, а її інтеграція в корпоративну стратегію є важливою умовою конкурентоспроможності в глобалізованому економічному середовищі.

Європейська модель інформаційної безпеки вирізняється нормативною послідовністю, стратегічною інтеграцією безпеки в управління бізнесом та акцентом на захисті прав користувачів. Концепції «Security by Design», «Privacy

by Design», а також стандарти, закріплені у GDPR і NIS 2, стали орієнтирами для підприємств у розбудові систем кіберзахисту. Аналіз зазначених концепцій і стратегій, дозволяє зрозуміти зміст ефективної європейської практики та її потенціал до адаптації в інших регіонах. Європейський досвід застосування концепцій та стратегій в забезпеченні інформаційної безпеки підприємств систематизовано в таблиці 1.7.

Таблиця 1.7 – Концепції та стратегії забезпечення інформаційної безпеки підприємств: досвід Європи

Концепції	Зміст концепцій	Приклади реалізації
Security by Design, Privacy by Design	Інтеграція безпеки з етапу проектування IT-систем та процесів.	Німеччина, Швеція, Нідерланди – обов’язкова практика згідно з GDPR.
Європейська стратегія кібербезпеки	Стратегічний документ ЄС щодо кіберстійкості, обміну інформацією, захисту критичної інфраструктури.	Реалізується через Cyber Resilience Act, NIS 2.
GDPR як стандарт безпеки	Регламент захисту персональних даних – обов’язковий для всіх компаній, що працюють з даними громадян ЄС.	Вся Європа – стимул до впровадження контролю доступу, шифрування, аудитів.
NIS, NIS 2	Визначає вимоги до безпеки для цифрових послуг та важливої інфраструктури.	Франція, Нідерланди, Італія – імплементують NIS 2 на національному рівні.
Публічно-приватне партнерство	Співпраця бізнесу, держави й академічної спільноти у сфері кіберзахисту.	ECSO (European Cyber Security Organisation), Horizon Europe.
Інституціоналізація інформаційної безпеки у компаніях	Впровадження посад CISO, політик ІБ, корпоративного управління безпекою.	Фінляндія, Данія, Естонія – CISO як частина ESG-звітності.
Кібергігієна та навчання персоналу	Освітні програми, тренінги, фішинг-тестування для співробітників.	Франція, Велика Британія, Естонія – державні програми підтримки бізнесу.

Джерело: систематизовано автором на основі [40-47].

Аналіз європейського досвіду застосування концепцій та стратегій в забезпеченні інформаційної безпеки підприємств засвідчує, що інформаційна безпека більше розглядається як стратегічний елемент сталого розвитку підприємств. Представлені концепції охоплюють нормативно-правовий, організаційний, технічний та соціальний виміри захисту інформації, що є характерною рисою європейської моделі цифрової безпеки. Наприклад,

впровадження концепцій «Security by Design», «Privacy by Design» свідчить про пріоритет запобіжного підходу, коли захист даних інтегрується на всіх етапах життєвого циклу систем [44]. Такі принципи закріплені у GDPR, який задає чіткі регламенти щодо обробки персональних даних і підвищує відповідальність бізнесу. Крім того, Європейська стратегія кібербезпеки та директива NIS/NIS 2 є прикладами нормативної гармонізації та міждержавної координації дій у сфері кібербезпеки, що є важливою умовою безпеки цифрового ринку ЄС.

На нашу думку, окрему увагу доцільно приділити інституціоналізації інформаційної безпеки на рівні підприємств, зокрема створенню посад CISO, розробці корпоративних політик та впровадженню міжнародних стандартів (ISO, IEC 27001). Крім того, публічно-приватне партнерство та підвищення кіберосвіти персоналу свідчать про важливість соціального капіталу у забезпеченні стійкості підприємств до цифрових загроз [45].

Європейський досвід застосування концепцій та стратегій в забезпеченні інформаційної безпеки підприємств засвідчує високий рівень системності, превентивності та нормативної узгодженості у підходах до кіберзахисту. Впровадження таких механізмів, як GDPR, NIS 2, Security by Design, а також активне залучення бізнесу до публічно-приватного партнерства свідчать про інтеграцію інформаційної безпеки в усі рівні управління підприємствами, що дозволяє мінімізувати ризики кібератак та сприяє підвищенню довіри споживачів, збереженню репутації та забезпеченню сталого розвитку в умовах цифрової трансформації. Європейські практики можуть слугувати ефективною моделлю для адаптації у підходах до інформаційної безпеки бізнесу.

Зростання кіберзагроз, розвиток глобальної економіки та ускладнення інформаційних систем зумовили необхідність створення єдиних стандартів і нормативів інформаційної безпеки. Світові регламенти, такі як ISO/IEC 27001, GDPR, NIST CSF, PCI DSS та інші, слугують основою для формування системного, правового та технічного підходу до захисту інформації в корпоративному середовищі. Їхнє застосування дозволяє підприємствам

захищати свої активи та забезпечувати довіру партнерів, відповідність законодавству та конкурентоспроможність на міжнародному ринку (табл. 1.8).

Таблиця 1.8 – Світові регламенти інформаційної безпеки підприємств

Регламенти	Зміст та особливості регламентів	Застосування
ISO/IEC 27001	Міжнародний стандарт управління інформаційною безпекою, включає оцінку ризиків, політики, інциденти.	Організації всіх галузей, включно з фінансовим та виробничим сектором.
General Data Protection Regulation	Регламент ЄС щодо захисту персональних даних, вимагає прозорості обробки, прав суб'єктів, безпеки за замовчуванням.	Компанії, що працюють з громадянами ЄС.
NIST Cybersecurity Framework	Рамкова модель управління кібербезпекою: ідентифікація, захист, виявлення, реагування, відновлення.	США та міжнародні компанії, особливо критична інфраструктура.
COBIT	Фреймворк для управління ІТ і безпекою, орієнтований на досягнення бізнес-цілей через управління ІТ-процесами.	Великі корпорації, що інтегрують ІБ у загальне управління.
PCI DSS	Стандарт захисту даних платіжних карток: шифрування, автентифікація, контроль доступу.	Банки, платіжні системи, інтернет-магазини.
ITIL	Найкращі практики управління ІТ-послугами, містить модулі з інформаційної безпеки.	Організації, що впроваджують ITSM для покращення якості послуг.
Digital Operational Resilience Act	Регламент ЄС щодо кіберстійкості фінансових організацій, включає тестування, звітування, взаємодію з ІТ-постачальниками.	Банки, страхові компанії, фінансові установи в ЄС
CSA STAR	Сертифікація безпеки хмарних провайдерів: прозорість, управління ризиками, відповідність стандартам.	Хмарні сервіси (AWS, Azure, Google Cloud).
CIS Controls	Практичний список пріоритетних заходів кібербезпеки, що мінімізують ризики поширених атак.	Малий та середній бізнес, ІТ-команди.
NIS 2	Директива з кібербезпеки, яка встановлює єдині стандарти для всіх країн ЄС щодо забезпечення стійкості цифрової інфраструктури	Середній та великий бізнес.

Джерело: систематизовано автором на основі [40, 45, 48-54].

Визначені світові регламенти забезпечення інформаційної безпеки підприємств, є системним оглядом основних міжнародних нормативів, які формують сучасне уявлення про ефективне управління інформаційною безпекою у бізнес-середовищі. Такий підхід носить міждисциплінарний характер інформаційної безпеки, що поєднує технічні, управлінські, правові та стратегічні аспекти захисту інформаційних активів підприємств, а також охоплює як обов'язкові регламенти (наприклад, GDPR, DORA), так і добровільні стандарти

(ISO/IEC 27001, NIST CSF), які в сукупності формують уніфіковану нормативну базу для адаптації підприємств до глобальних кіберзагроз.

Кожен зі стандартів або регламентів виконує специфічну функцію в екосистемі інформаційної безпеки. Наприклад, ISO/IEC 27001 виступає як базовий інструмент створення та оцінки системи управління інформаційною безпекою, тоді як GDPR фокусується на захисті персональних даних і регламентує правові зобов'язання компаній щодо користувачів [45]. NIST CSF забезпечує модульний фреймворк, що дозволяє підприємствам ідентифікувати та усувати кіберризики на різних рівнях. COBIT і ITIL інтегрують інформаційної безпеки у загальну систему корпоративного управління, тоді як PCI DSS розроблений спеціально для забезпечення захисту фінансових транзакцій.

Особливу роль відіграють галузеві та новітні регламенти, наприклад, DORA, що визначає цифрову стійкість фінансового сектору, та CSA STAR, який стосується хмарних сервісів. Такі стандарти враховують специфіку сучасних технологічних середовищ, зокрема хмарних обчислень та децентралізованих платформ, і формують вимоги до прозорості, контролю доступу, інцидент-менеджменту та взаємодії з постачальниками IT-послуг. CIS Controls представляють практичну модель для малого та середнього бізнесу, надаючи набір першочергових дій з кіберзахисту.

Таким чином, визначені світові регламенти інформаційної безпеки підприємств, демонструють важливість гармонізації міжнародних підходів до інформаційної безпеки та забезпечення відповідності підприємств глобальним викликам. Регламенти є орієнтирами для імплементації конкретних вимог та обґрунтованою основою для формування дієвої політики інформаційної безпеки.

Зазначимо, що 18 жовтня 2024 року набула чинності директива з кібербезпеки NIS 2, яка встановлює єдині стандарти для всіх країн ЄС щодо забезпечення стійкості цифрової інфраструктури [46]. Цей нормативний акт значно розширює сферу дії попередньої директиви NIS 1, охоплюючи операторів критичної інфраструктури та широкий спектр суб'єктів у сферах енергетики,

транспорту, фінансів, охорони здоров'я, цифрових послуг, а також організації середнього бізнесу з основним впливом на ринок.

Відповідно до вимог NIS 2, компанії зобов'язані розробляти, документувати та підтримувати актуальні стратегії кібербезпеки, проводити регулярну оцінку ризиків, впроваджувати політики управління інцидентами та забезпечення безперервності діяльності. Однією з важливих вимог є обов'язкове повідомлення про значущі кіберінциденти національним органам кібербезпеки протягом 24 годин з моменту виявлення порушення. Директива передбачає посилення відповідальності керівництва компаній за дотримання норм безпеки, включаючи можливість адміністративних санкцій за неналежне реагування. NIS 2 має на меті створити єдиний кіберзахисний простір у ЄС, у якому компанії зобов'язані впроваджувати технічні заходи захисту та формувати культуру управління кіберризиками на всіх рівнях організації. Її імплементація є прикладом глобального підходу до інформаційної безпеки, де державне регулювання, обов'язкові стандарти та корпоративна відповідальність поєднуються в єдину систему, орієнтовану на довготривалу цифрову стійкість.

Також, відповідно до 12-го пакету санкцій ЄС, ухваленого у грудні 2023 року, забороняється продаж, постачання, передача, експорт або надання програмного забезпечення для управління бізнес-процесами (зокрема CRM, ERP, EDW, PLM тощо) російським компаніям, а також дочірнім структурам європейських підприємств, що діють на території росії. Україна активно рухається в напрямку євроінтеграції, тому українським суб'єктам підприємництва вже найближчим часом доведеться адаптуватися до міжнародних стандартів кібербезпеки для збереження своєї конкурентоспроможності на європейському ринку. Наразі чинне регуляторне середовище в Україні не створює достатніх умов для ефективного усунення ризиків, пов'язаних із широким використанням програмних продуктів ІС та BAS. Для багатьох підприємств і державних установ, які залишаються залежними від російського ПЗ, збереження існуючого стану речей здається

простішим шляхом, проте така зручність не гарантує безпеки – навпаки, вона створює серйозні вразливості в умовах гібридних загроз.

Українським суб'єктам підприємництва, доцільно орієнтуватися на світовий досвід інформаційної безпеки шляхом впровадження міжнародних стандартів (зокрема ISO/IEC 27001, GDPR, NIST), розробки внутрішніх політик безпеки, створення системи управління кіберризиками та підвищення цифрової грамотності персоналу.

Рекомендується впроваджувати концепції «Security by Design» та «Zero Trust», проводити регулярні аудити безпеки, використовувати хмарні технології з належним рівнем захисту, а також долучатися до публічно-приватних ініціатив у сфері кібербезпеки. Такий підхід сприятиме зниженню вразливості до кіберзагроз, забезпеченню стійкості бізнесу в умовах воєнного часу та інтеграції у глобальні цифрові ринки.

Стандартизація інформаційної безпеки згідно з вимогами міжнародних нормативних документів ISO є важливим інструментом у формуванні ефективної та уніфікованої системи захисту інформаційних ресурсів підприємства. Основним стандартом у цій сфері виступає ISO/IEC 27001, який встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою.

У доповнення до нього діють інші стандарти родини ISO 27000, зокрема ISO/IEC 27002 (практичні заходи захисту), ISO/IEC 27005 (керування ризиками), ISO/IEC 27017 (хмарна безпека) тощо. Впровадження цих стандартів забезпечує структуровану роботу з ризиками, політиками, інцидентами та персоналом, гарантує відповідність міжнародним вимогам, що є важливим для участі підприємств у глобальних ринках і забезпечення довіри з боку партнерів та клієнтів (табл. 1.9).

У сучасних умовах цифровізації економіки та активізації кіберзагроз питання нормативно-правового регулювання інформаційної безпеки набуває особливої актуальності для суб'єктів підприємництва.

Таблиця 1.9 – Стандартизація інформаційної безпеки згідно вимог нормативних документів ISO

Нормативні документи	Організаційні аспекти управління інформаційною безпекою		
	Інформація та документація	Інформаційні технології	Управління документами
ISO 16175. Інформація та документація	Принципи і функціональні вимоги до документів в електронному середовищі		Керівництво і функціональні вимоги до систем управління цифровими документами
Міжнародні стандарти ISO та ІЕС на інформаційні технології для забезпечення безпеки управління		Методи забезпечення безпеки, виявлення та розкриття електронної інформації, формат Office Open XML	Системи менеджменту інформаційної безпеки, принципи та методи управління документацією.
ISO 32000. Управління документами	Форма переносимого документа, формат портативного документа тощо		
Інші нормативні документи	ISO / TO 15801: 2009. Рекомендації щодо забезпечення достовірності і надійності документації	ISO 14641-1: 2012. Проектування та експлуатація інформаційних систем для забезпечення довготривалого збереження електронних документів	ISO / TO 18800: 2012. Керівництво із виконання, відбору і передачі документів
			ISO / TO 18492: 2005. Забезпечення довготривалого зберігання електронної документованої інформації
			ISO / TO 26122: 2008. Аналіз процесів роботи з точки зору управління документами

Джерело: систематизовано автором на підставі аналізу стандартів ISO [45, 47].

Надійний правовий фундамент є необхідною передумовою для ефективного управління інформаційними ризиками, забезпечення захисту даних і відповідності міжнародним стандартам. У зв'язку з інтеграційними процесами та потребою гармонізації українського законодавства з нормами ЄС, важливо дослідити структуру нормативно-правового забезпечення інформаційної безпеки, що охоплює міжнародний, національний, галузевий та внутрішньокорпоративний рівні (табл. 1.10).

Таблиця 1.10 – Структура нормативно-правового забезпечення інформаційної безпеки суб'єктів підприємництва

Рівні	Зміст рівнів	Приклади нормативно-правових актів
Міжнародно-правовий	Нормативні акти та стандарти, які регулюють ІБ на рівні ЄС та міжнародних організацій.	GDPR, NIS 2 Directive, ISO/IEC 27001, ISO/IEC 27002, NIST CSF, Конвенція про кіберзлочинність (Будапештська)
Національно-правовий (Україна)	Закони та нормативні документи, що встановлюють загальні засади інформаційної та кібербезпеки в Україні.	ЗУ «Про інформацію», ЗУ «Про кібербезпеку», ЗУ «Про захист персональних даних», нормативи Держспецзв'язку, НБУ, ККУ
Галузевий	Норми та інструкції, які регулюють ІБ у конкретних секторах економіки.	Регулювання НБУ, DORA, PCI DSS (фінанси), медичні стандарти конфіденційності, вимоги до критичної інфраструктури
Внутрішньо-корпоративний	Внутрішні політики та регламенти підприємств щодо управління інформаційною безпекою.	Політика ІБ, регламенти доступу, план реагування на інциденти, резервне копіювання, впровадження ISO 27001

Джерело: систематизовано автором на основі [45, 54-60].

Структура нормативно-правового забезпечення інформаційної безпеки суб'єктів підприємництва демонструє обґрунтовану системну модель регулювання інформаційних процесів у цифровому середовищі. Така багаторівнева ієрархія правових норм забезпечує комплексний підхід до формування стійкої системи кіберзахисту, де кожен рівень виконує свою специфічну функцію – від глобального регламентування до локального впровадження політик безпеки. Вона узгоджує загальносвітові стандарти з національними особливостями та специфікою окремих галузей, забезпечуючи правову цілісність системи інформаційної безпеки.

Міжнародний рівень, представлений такими актами, як GDPR (загальний регламент захисту персональних даних), NIS 2 Directive (директива про кіберстійкість критичної цифрової інфраструктури), ISO/IEC 27001 (міжнародні стандарти управління інформаційною безпекою), NIST (рамкова модель управління кіберризиками), Будапештська конвенція, задає уніфіковані вимоги до безпеки персональних даних, стійкості критичної інфраструктури та управління інформаційними ризиками [54-56]. Зазначені нормативні акти є

основою для гармонізації національного законодавства, виступають орієнтирами для країн, що прагнуть інтегруватися у глобальний цифровий простір.

Національний рівень, зокрема в Україні, визначає базові правові засади функціонування системи інформаційної безпеки. Закони України «Про інформацію», «Про захист персональних даних», «Про кібербезпеку», Закон України «Про персональні дані», Кримінальний кодекс України, Стратегії та концепції з кібербезпеки, інформаційного суверенітету тощо, нормативні акти Держспецзв'язку, НБУ, Кіберполіції. та інші нормативи створюють нормативне поле для практичної реалізації вимог безпеки на підприємствах [57-60].

Галузевий рівень доповнює це регулювання специфічними інструкціями для різних сфер – фінансової, медичної, транспортної, енергетичної – враховуючи характер оброблюваної інформації та потенційні ризики. Внутрішньокорпоративний рівень охоплює інклюзивні інституції підприємства (політики, інструкції та стандарти, розроблені на рівні окремого підприємства):

- політика інформаційної безпеки;
- регламент доступу до даних;
- план реагування на інциденти;
- протоколи резервного копіювання;
- кодекс поведінки працівника в цифровому середовищі;
- впровадження ISO 27001 на підприємстві;

Таким чином, структурований підхід до нормативно-правового регулювання інформаційної безпеки забезпечує відповідність підприємств законодавчим вимогам та сприяє побудові ефективної, адаптивної та довготривалої системи захисту в умовах постійної зміни кіберзагроз. Він формує основу для правової та організаційної стійкості суб'єктів підприємництва в цифрову епоху.

Впровадження та дотримання правових норм на всіх рівнях сприяє зміцненню цифрової стійкості підприємств, забезпечує правову визначеність їх діяльності в інформаційному середовищі.

Висновки до розділу 1

Доведено, що категоризація учасників інформаційної безпеки підприємства та систематизація їх на внутрішніх і зовнішніх забезпечує цілісне розуміння структури управління інформаційними ризиками. Такий поділ дозволяє ефективно розподілити функціональні обов'язки, оптимізувати взаємодію між усіма сторонами, а також враховувати як внутрішні організаційні процеси, так і зовнішні чинники впливу. Усвідомлення ролі кожного учасника сприяє підвищенню стійкості підприємства до інформаційних загроз, формуванню культури безпеки та забезпеченню відповідності нормативно-правовим вимогам у сфері інформаційної безпеки.

Застосовано функціонально-компонентний підхід, до аналізу інформаційної безпеки підприємств дозволяє системно охопити всі основні елементи, що формують ефективну політику захисту інформаційних ресурсів. Такий підхід забезпечує структурування внутрішніх та зовнішніх чинників впливу, дає змогу виявити функціональні зони відповідальності та інтегрувати заходи безпеки у загальну систему управління підприємством. Доведено подвійну природу інформації – об'єктивну та суб'єктивну, що зумовлює потребу одночасного впровадження технічних, організаційних і психологічних механізмів захисту. Такий підхід, формує умови для адаптивної, стійкої та економічно доцільної системи інформаційної безпеки, яка здатна ефективно реагувати на динамічні виклики цифрового середовища та сприяти довгостроковій конкурентоспроможності підприємства.

Запропоновано функціональну модель інформаційної безпеки підприємства, що забезпечує комплексний підхід до захисту інформаційних ресурсів. Її реалізація дозволяє запобігати загрозам та оперативно реагувати на інциденти і ефективно інтегрувати заходи безпеки в управлінські, економічні та освітні процеси підприємства. Такий підхід сприяє підвищенню адаптивності організації до сучасних викликів кіберсередовища та формує підґрунтя для

сталого функціонування і збереження конкурентоспроможності в умовах цифрової трансформації.

Визначено систему принципів інформаційної безпеки підприємства, що формується як багаторівнева концептуальна основа для побудови ефективної та стійкої політики захисту інформаційних ресурсів. Визначені принципи включають технічні, організаційні, управлінські та соціальні аспекти безпеки, забезпечуючи комплексний підхід до мінімізації ризиків. Важливу роль відіграє принцип інклюзивної інституційності, який акцентує на важливості залучення всіх зацікавлених сторін до процесів управління інформаційною безпекою, що, у свою чергу, підвищує прозорість, адаптивність і відповідальність усередині організації. Сукупне застосування цих принципів створює цілісну модель інформаційної безпеки, здатну ефективно функціонувати в умовах постійної зміни цифрового середовища та зростання інформаційних загроз.

Доведено, що рішення суб'єктів підприємництва щодо інвестування в інформаційну безпеку є результатом взаємодії зовнішніх загроз та внутрішніх ресурсів підприємства, що зумовлює необхідність системного підходу до управління ризиками. Зовнішні чинники, зокрема регуляторні вимоги, конкурентний тиск і загрози кіберзлочинності, формують зовнішній імператив дій, тоді як внутрішні чинники – фінансова спроможність, цифрова досконалість та стратегічні орієнтири – визначають реальні можливості впровадження ефективної системи захисту. Усвідомлення цінності даних, як стратегічного активу, стає основним мотиватором для створення інтегрованої системи інформаційної безпеки, що є передумовою сталого функціонування та конкурентоспроможності сучасного підприємства.

Визначено, що забезпечення інформаційної безпеки суб'єктів підприємництва є складним багатовимірним процесом, що залежить від поєднання глобальних викликів, специфіки розміру підприємства та наявних ресурсів. Система бар'єрів – фінансових, технічних та організаційних – ускладнює реалізацію заходів кіберзахисту, особливо для малого та середнього бізнесу, який має обмежені можливості адаптації до динамічних умов цифрового

середовища. Крім того, у великого бізнесу зростає складність управління ризиками через масштаб цифрової інфраструктури та необхідність дотримання міжнародних норм, що вимагає стратегічного підходу до інформаційної безпеки, орієнтованого на інституційне зміцнення, підвищення цифрової культури персоналу та інтеграцію безпеки у всі рівні управління підприємством.

Систематизовано стимули забезпечення інформаційної безпеки суб'єктів підприємництва, які мають багатовимірний характер та включають економічні, регуляторні, репутаційні та стратегічні аспекти, що свідчить про її інтегровану роль у сучасному бізнес-середовищі. Вони знижують ризики та втрати від потенційних кіберінцидентів і створюють передумови для сталого розвитку, посилення ринкових позицій та зміцнення довіри з боку зацікавлених сторін. Інформаційна безпека виступає як інструмент захисту та як драйвер цифрової трансформації, конкурентоспроможності та стратегічної стійкості підприємств.

Доведено, що ефективність забезпечення інформаційної безпеки суб'єктів підприємництва залежить від цілісної взаємодії фінансових, технологічних, організаційних та зовнішньополітичних чинників. Найбільш стійкі до кіберзагроз підприємства – це ті, які поєднують високий рівень цифрової досконалості, кваліфікований персонал, сучасну ІТ-інфраструктуру, чіткі внутрішні політики безпеки та здатність оперативно реагувати на інциденти. Зовнішні умови, такі як дотримання регуляторних вимог, врахування технологічних трендів та адаптація до глобальних викликів, суттєво впливають на стратегічну стійкість підприємства, що підтверджує необхідність комплексного, адаптивного підходу до формування системи інформаційної безпеки як важливої складової цифрового розвитку бізнесу.

Проаналізовано світові тренди у сфері забезпечення інформаційної безпеки суб'єктів підприємництва, що свідчать про глибоку трансформацію ролі кіберзахисту, від технічної підтримки до стратегічного активу бізнесу. Впровадження таких підходів, як «Zero Trust», AI-орієнтовані системи безпеки, хмарна безпека та кіберстійкість, дозволяє підприємствам ефективно протистояти сучасним загрозам та забезпечувати безперервність діяльності,

підвищувати довіру з боку партнерів та споживачів і дотримуватись міжнародних вимог. Визначені тренди демонструють, що інформаційна безпека є невід'ємною складовою цифрової трансформації бізнесу, а її інтеграція в корпоративну стратегію є важливою умовою конкурентоспроможності в глобалізованому економічному середовищі.

Охарактеризовано європейський досвід формування концепцій та стратегій інформаційної безпеки підприємств, що засвідчує високий рівень системності, превентивності та нормативної узгодженості у підходах до кіберзахисту. Впровадження таких механізмів, як GDPR, NIS 2, Security by Design, а також активне залучення бізнесу до публічно-приватного партнерства свідчать про інтеграцію інформаційної безпеки в усі рівні управління підприємствами, що дозволяє мінімізувати ризики кібератак та сприяє підвищенню довіри споживачів, збереженню репутації та забезпеченню сталого розвитку в умовах цифрової трансформації. Європейські практики можуть слугувати ефективною моделлю для адаптації у національних підходах до інформаційної безпеки бізнесу.

Визначено нормативно-правове забезпечення інформаційної безпеки суб'єктів підприємництва, яке є багаторівневою системою, що охоплює міжнародні стандарти, національні закони, галузеві нормативи та внутрішньокорпоративні документи. Така структурована модель дозволяє забезпечити комплексний підхід до захисту інформаційних ресурсів, адаптацію до сучасних кіберзагроз та гармонізацію з європейськими вимогами. Впровадження та дотримання правових норм на всіх рівнях сприяє зміцненню цифрової стійкості підприємств, забезпечує правову визначеність їх діяльності в інформаційному середовищі та підвищує довіру з боку партнерів, споживачів і державних інституцій.

РОЗДІЛ 2

ДІАГНОСТИКА СТАНУ ТА ПЕРСПЕКТИВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА

2.1 Методичні засади дослідження стану та перспектив забезпечення інформаційної безпеки суб'єктів підприємництва

У сучасних умовах стрімкої цифровізації бізнес-процесів, посилення кіберзагроз та зростання значущості інформаційних ресурсів, питання забезпечення інформаційної безпеки набуває пріоритетного значення для суб'єктів підприємництва. Інформація перетворилася на один із основних стратегічних активів, який безпосередньо впливає на конкурентоспроможність, репутацію, фінансову стабільність і життєздатність бізнес-структур. За цих умов потреба в системному підході до оцінки стану інформаційної безпеки та формування дієвих механізмів її забезпечення є надзвичайно актуальною. Проте ефективне управління інформаційною безпекою потребує як технічних рішень так і методологічно обґрунтованих підходів до її дослідження. Зокрема, необхідно враховувати специфіку суб'єктів підприємництва за масштабами, галузевими особливостями, рівнем цифрової досконалості, що вимагає гнучких та адаптивних методик аналізу. Методичне забезпечення дослідження інформаційної безпеки має включати інструменти для виявлення ризиків, оцінки вразливостей, визначення рівня захищеності, а також прогнозування можливих загроз і побудови сценаріїв розвитку ситуації [61].

У цьому контексті важливо ідентифікувати сучасні загрози інформаційній безпеці та оцінити перспективи та напрями вдосконалення системи її забезпечення з урахуванням глобальних тенденцій, державної політики, нормативно-правових вимог та інституційних можливостей самих суб'єктів підприємництва. Тому, актуальним є науковий пошук методичних засад, які дозволять здійснювати комплексне, об'єктивне та науково обґрунтоване

дослідження стану інформаційної безпеки суб'єктів підприємництва, а також визначати стратегічні орієнтири її розвитку в майбутньому.

Варто зауважити, що наразі існує ряд підходів, методик та систем показників щодо аналізу і оцінки процесу забезпечення інформаційної безпеки суб'єктів підприємництва. Зокрема, Рой Я.В., Мазур Н.П. та Складанний П.М. акцентують увагу на важливості проведення аудиту інформаційної безпеки як важливої умови для виявлення вразливостей і загроз, а також оцінки ефективності існуючих захисних заходів [62]. У роботах Тулуп'єва А.О. та Кваші С.В. розроблено методику оцінювання рівня захищеності інформації в автоматизованих системах, що ґрунтується на ієрархічному аналізі загроз, можливих втрат і частотності їх реалізації [63]. У своїх дослідженнях Мурашко О.В. підкреслює доцільність використання ризикоорієнтованого підходу до оцінювання стану інформаційної безпеки з урахуванням потенційних наслідків для бізнес-процесів підприємства [64]. Науковці Шевченко Л.І. та Ткачук Л.С. запропонували методику якісної оцінки ризиків в інформаційному середовищі малих підприємств із застосуванням бальних шкал, що забезпечує адаптацію оцінки до специфіки організацій малого бізнесу [65].

Цікавою з наукової точки зору є робота Велігури А.В., в якій представлено комплексну методику оцінювання стану інформаційної безпеки підприємства, що базується на системному підході та охоплює три основні блоки: програмно-технічну захищеність, інформаційну надійність персоналу та якість інформації, що використовується для прийняття управлінських рішень. Автор наголошує, що «ефективне функціонування системи інформаційної безпеки залежить від узгодженої роботи підсистем аналізу загроз, планування та реалізації заходів, спрямованих на забезпечення безпеки» [66]. Кожен із трьох напрямків включає набір кількісних індикаторів, що дозволяють об'єктивно виміряти рівень безпеки підприємства.

Перший блок оцінювання охоплює програмно-технічну захищеність. Тут застосовуються такі показники:

- коефіцієнт технічного захисту інформації

$$K_{3T} = 1 / IA \quad (2.1),$$

де IA – кількість не відвернутих атак;

- коефіцієнт програмної захищеності

$$K_{3.П} = Ч_{фб} / Ч_{фн} \quad (2.2),$$

де $Ч_{фб}$ – час безперебійного функціонування корпоративної інформаційної системи, год.,

$Ч_{фн}$ – нормативний час функціонування корпоративної інформаційної системи, год.;

- коефіцієнт фінансового захисту

$$K_{3.ф} = B_{з.ін} / B_{пр.ін}, 0,15, \text{ зростання} \quad (2.3),$$

де $B_{з.ін}$ – витрати на захист інформаційних ресурсів, грн.,

$B_{пр.ін}$ – витрати на придбання інформаційних ресурсів, грн.;

- коефіцієнт фінансування ІТ-служб

$$K_{фін} = B_{фін} / B_{заг}, 0,5-0,15, \text{ зростання} \quad (2.4),$$

Де $B_{заг}$ – загальні витрати підприємства,

$B_{фін}$ – витрати на фінансування інформаційних служб підприємства, грн.

Другий блок методики передбачає оцінювання надійності персоналу, який забезпечує інформаційну безпеку. Зокрема,

- коефіцієнт правової захищеності інформації

$$K_{з.пр} = I_{з.юр} / I, 1, \text{ зменшення} \quad (2.5),$$

де $I_{з.юр}$ – загальний обсяг юридично захищеної інформації, %,

I – обсяг інформації, розголошення якої може спричинити негативні наслідки для підприємства, %;

- коефіцієнт досвіду роботи персоналу

$$K_{р.д} = ЧП_1 / ЧП_{заг}, 1, \text{ зростання} \quad (2.6),$$

де $ЧП_1$ – чисельність працівників, які мають доступ до комерційної таємниці, що працюють на підприємстві більше одного року, ос.,

$ЧП_{заг}$ – загальна чисельність працівників, що мають доступ до комерційної таємниці, ос;

- коефіцієнт надійності персоналу

$$(ЧП_{зв.} - ЧП_{вип}) / ЧП_{зв} \quad (2.7),$$

де $ЧП_{вип}$ – чисельність працівників, звільнених за причиною витоку інформації, ос.,

$ЧП_{зв.}$ – загальна чисельність звільнених працівників, ос.;

- коефіцієнт підготовленості персоналу

$$(ЧП_{з.} - ЧП_{п}) / ЧП_{з} \quad (2.8),$$

де $ЧП_{п}$ – чисельність працівників, ненавмисні дії яких призвели до витоку інформації завдяки низькому рівню підготовки персоналу до розпізнавання загроз безпеки, ос.

$ЧП_{з.}$ – загальна чисельність працівників, що мають доступ до закритої інформації, ос.

Третій блок зосереджено на оцінці якості інформації, яка використовується для управлінських рішень. Визначаються такі коефіцієнти:

- коефіцієнт повноти інформації

$$K_{ін.п} = I_n / I_{необ} \quad (2.9),$$

де I_n – обсяг інформації, що є в розпорядженні ОПР, %,

$I_{необ.}$ – обсяг інформації, необхідної для ухвалення рішення, %;

- коефіцієнт точності інформації

$$K_{ін.т} = I_p / I_n \quad (2.10),$$

де I_p – обсяг релевантної інформації, %,

I_n – загальний обсяг наявної в розпорядженні ОПР інформації, %;

- коефіцієнт суперечливості інформації

$$K_{\text{ін.с}} = I_{\text{ухв}} / I_3 \quad (2.11),$$

де $I_{\text{ухв}}$ – кількість незалежних свідчень на користь ухвалення рішення, %,

I_3 – загальна кількість незалежних свідчень у сумарному обсязі релевантної інформації, %;

- коефіцієнт своєчасності надання інформації

$$K_{\text{ін.н.с}} = I_{\text{н.с}} / I_{\text{необ}}, 1, \text{ зростання} \quad (2.12),$$

де $I_{\text{н.с.}}$ – обсяг своєчасно наданої ОПР інформації, %,

$I_{\text{необ.}}$ – обсяг інформації, необхідної для ухвалення рішення, %;

- коефіцієнт надійності джерел інформації

$$K_{\text{ін.н}} = I_{\text{д.н}} / I_{\text{н.з}} \quad (2.13),$$

де $I_{\text{н.д.}}$ – обсяг інформації, наданої ОПР з надійних джерел, %,

$I_{\text{н.з.}}$ – загальний обсяг наданої ОПР інформації, %.

Таким чином, методика Велігури надає формалізовані підходи до обчислення рівня ІБ та дозволяє виявляти «вузькі місця» у функціонуванні ІТ-інфраструктури, кадровій політиці та інформаційних потоках підприємства, що робить її ефективним інструментом як для моніторингу, так і для стратегічного управління інформаційною безпекою в умовах зростання кіберризиків.

На думку Живко З.Б., «рівень інформаційної безпеки суб'єкта підприємництва можна оцінювати за допомогою спеціалізованих коефіцієнтів, які відображають якісні характеристики інформаційного забезпечення управлінських рішень» [67]. Зокрема, коефіцієнт повноти інформації ($K_{\text{пі}}$) визначається як співвідношення між фактичним обсягом інформації, доступної керівнику, і тією кількістю даних, яка є необхідною для прийняття обґрунтованого рішення. Коефіцієнт точності інформації ($K_{\text{ті}}$) характеризує частку достовірної інформації серед усієї наявної, що дозволяє оцінити рівень шумів і спотворень у комунікаційному середовищі. У свою чергу, коефіцієнт

суперечливості інформації (K_{ci}) визначається як співвідношення кількості незалежних свідчень, які підтримують прийняття певного рішення, до інших свідчень у загальному обсязі достовірної інформації.

Інтегральний рівень інформаційної безпеки (K_{i6}) Живко З.Б. пропонує визначати шляхом обчислення добутку трьох зазначених коефіцієнтів:

$$K_{i6} = K_{pi} \times K_{ti} \times K_{ci} \quad (2.14),$$

що дозволяє отримати узагальнену кількісну оцінку ступеня безпеки інформаційного середовища підприємства. Відповідно до шкали оцінювання, розрізняють три рівні інформаційної безпеки: високий ($K_{i6} > 0,7$), середній ($0,3 < K_{i6} < 0,7$) та низький ($K_{i6} < 0,3$). Такий підхід забезпечує можливість оцінити фактичний стан захищеності інформаційної системи та виявити її слабкі місця, що потребують посиленої уваги в процесі стратегічного управління. Застосування цих коефіцієнтів є корисним інструментом для системного аналізу ефективності прийняття рішень та формування адекватних механізмів інформаційного контролю.

В своїх дослідженнях Бегун А.В. пропонує аспектноорієнтовану технологію моделювання, що дозволяє оцінити ефективність захисту інформаційних ресурсів на основі сценарного аналізу і техніко-економічних показників [69]. На думку автора, відвернутий збиток – це не єдиний результат діяльності системи безпеки, з огляду на те, що 100 % повного захисту неможливо досягти, а тому існує залишковий ризик виникнення загрози, який прогнозує можливість виникнення збитку – від’ємного результату. Відповідно, оцінювання ефективності системи інформаційної безпеки має враховувати кількісні параметри зменшення втрат та здатність системи до адаптації, своєчасного реагування та мінімізації негативних наслідків при настанні інцидентів. Як підкреслює Бегун А.В., «доцільно застосовувати аспектноорієнтовані технології, які дозволяють оптимізувати захист із урахуванням особливостей інформаційного середовища та пріоритетності захисту окремих компонентів системи» [69]. Зокрема, в контексті банківських установ або web-орієнтованих структур, де високий рівень загроз поєднується з критичністю інформаційних

ресурсів, автор пропонує моделювання сценаріїв впливу на безпеку та визначення інтегрального показника ефективності захисту. Таким чином, ефективність системи повинна оцінюватись за фактом уникнення збитків та за здатністю знижувати ймовірність реалізації загроз у майбутньому та підвищувати загальну інформаційну стійкість підприємства.

Таким чином, за твердженням Бегуна А.В., результативність заходів із забезпечення інформаційної безпеки може бути виражена у формі вартості відвернених та фактично понесених збитків. Виходячи з цього, автором запропоновано відповідну формулу для розрахунку ефекту інформаційної безпеки:

$$E = (U_1 - U_2) / Z_0 \quad (2.15),$$

де: U_1 – відвернутий збиток (можливий збиток у результаті атаки на інформаційну систему);

U_2 – збиток від впливу атаки на інформаційну систему;

Z_0 – витрати на забезпечення інформаційної безпеки.

Враховуючи вираз: $U_2 = U_{2.1} + U_{2.2}$, де $U_{2.1}$ – прямі збитки, $U_{2.2}$ – непрямі збитки, обчислення показника ефекту (E) доцільно здійснювати за наступною формулою:

$$E = (U_1 - U_2) / (Z_1 + Z_2 + Z_3) \quad (2.16),$$

де Z_1 – витрати на формування політики інформаційної безпеки;

Z_2 – витрати на реалізацію політики інформаційної безпеки;

Z_3 – витрати, які пов'язані з наслідками порушення політики інформаційної безпеки

Зазначимо, що автор акцентує увагу на доцільності врахування страхування залишкового інформаційного ризику, за якого величина страхового внеску (s) збільшує загальні витрати (Z), тоді як страхове відшкодування у разі настання страхової події (S) зменшує розмір потенційних збитків (U):

$$E = (U_1 - U_2 + S) / (Z_0 + s) \quad (2.17),$$

На думку Бегуна А.В., максимізація загального економічного ефекту від впровадження заходів інформаційної безпеки можлива за дотримання таких умов:

$$\left\{ \begin{array}{l} U_1 \rightarrow \max \\ U_2 \rightarrow \min \\ Z_0 \rightarrow \min \end{array} \right.$$

При цьому автор обґрунтовано підкреслює, що процес максимізації відвернутого ризику та мінімізації залишкового ризику має здійснюватися комплексно, тоді як зниження витрат на забезпечення інформаційної безпеки повинно бути економічно доцільним і збалансованим.

Поряд із визначенням абсолютного економічного ефекту, автор також пропонує здійснювати оцінку вартості збереженого та примноженого інформаційного ресурсу (C), співвідносячи її із витратами, понесеними на забезпечення інформаційної безпеки. З цією метою запропоновано наступну формулу:

$$E^* = C / Z_0 \quad (2.18),$$

З метою узагальненої оцінки ефективності заходів інформаційної безпеки, автором запропоновано використання показника рентабельності витрат на забезпечення інформаційної безпеки. При цьому наголошується, що обсяг надлишкового інформаційного ресурсу має демонструвати певний рівень кореляційного зв'язку з показниками чистого прибутку підприємства або його потенціалом до формування такого прибутку [69].

Зазначені підходи суттєво різняться за глибиною аналізу, охопленням аспектів захисту, методами збору та обробки даних, проте вказують на необхідність комплексного, системного та адаптивного методологічного забезпечення дослідження стану інформаційної безпеки. У зв'язку з цим актуальним є подальше удосконалення існуючих підходів з метою їх адаптації

до нових умов ведення підприємницької діяльності, цифрової трансформації та підвищення кіберзагроз в умовах гібридних загроз і воєнних ризиків.

У сучасних умовах зростаюча інтенсивність використання інформаційно-комунікаційних технологій, з одного боку, розширює можливості для підвищення ефективності бізнес-процесів, а з іншого – загострює проблематику інформаційної безпеки через кіберзагрози, втрат конфіденційної інформації, порушення цілісності даних і функціонування інформаційних систем. У зв'язку з цим особливої ваги набуває завдання формалізованого оцінювання рівня інформаційної безпеки, що вимагає визначення чітких порогових значень для класифікації її стану.

Порогові значення виступають критеріями, які дозволяють ідентифікувати межі допустимого ризику, виявляти відхилення від нормативного рівня захищеності та приймати своєчасні управлінські рішення щодо запобігання загрозам. Їх застосування у практиці інформаційного аудиту та моніторингу безпеки створює підґрунтя для об'єктивного аналізу поточного стану інформаційної безпеки, побудови сценаріїв розвитку ситуації та підвищення адаптивності систем управління ризиками.

У літературі запропоновано низку методичних підходів до визначення таких порогових значень, від простих шкал бального оцінювання до багаторівневих моделей з використанням вагових коефіцієнтів, індикаторів критичності активів та ризикоорієнтованих параметрів [70]. Комплексне дослідження існуючих підходів, їхніх переваг, обмежень та можливостей адаптації до умов конкретного підприємства є важливим кроком на шляху до вдосконалення системи забезпечення інформаційної безпеки в цілому.

У дослідженні стану інформаційної безпеки суб'єктів підприємництва, важливу роль відіграє вибір адекватного методичного підходу до визначення порогових значень захищеності. Так, Рой Я.В., Мазур Н.П. та Складанний П.М. запропонували комплексну методику, яка базується на використанні вагових коефіцієнтів для різних індикаторів ризику. Їхній підхід дозволяє адаптувати модель до різних типів підприємств, передбачає інтеграцію з аудитом

інформаційної безпеки та класифікує рівень захищеності за чотирма пороговими станами – від критичного до безпечного.

Таблиця 2.1 – Характеристика методичних підходів до визначення порогових значень стану інформаційної безпеки підприємств

Джерело	Методичний підхід	Порогові рівні	Особливості
Рой Я.В., Мазур Н.П., Складанний П.М.	Комплексна оцінка з використанням вагових коефіцієнтів і ризик-орієнтованих індикаторів	4 рівні (критичний, передкризовий, допустимий, безпечний)	Інтеграція з системою аудиту ІБ, можливість адаптації до різних типів підприємств
Бегун А.В.	Аспектноорієнтоване моделювання рівнів ІБ з деталізованою шкалою (0-10 балів)	5 рівнів (критичний – оптимальний), % або бали	Застосовується як для банківських, так і для загальноекономічних систем
Мурашко О.В.	Системний підхід до управління ризиками з розрахунком рівня безпеки на основі вартості збитків	Визначення меж безпечного рівня за співвідношенням витрати/збитки	Оцінює економічний ефект від впровадження заходів ІБ
Тулуп'єв А.О., Кваша С.В.	Ієрархічна оцінка рівня захищеності за типами загроз і втрат	3 рівні (низький, середній, високий захист)	Підходить для технічного аналізу інформаційної інфраструктури
Шевченко Л.І., Ткачук Л.С.	Якісна оцінка ризиків для малих підприємств з використанням бальної шкали (0-5)	Шкала 0-5 балів з описом критичних відхилень	Придатна для малого бізнесу, проста в застосуванні
ISO/IEC 27001	Стандартизована система класифікації рівнів контролю та заходів ІБ (Annex A, control sets)	Визначення рівнів відповідності вимогам стандарту (низький – високий)	Міжнародна уніфікація, можливість сертифікації підприємства

Джерело: узагальнено автором на основі [45, 62-65, 69].

Автором аспектноорієнтованої моделі оцінювання інформаційної безпеки, яка передбачає використання бальної шкали від 0 до 10, є Бегун А.В. Такий підхід надає гнучкі можливості для кількісного оцінювання окремих аспектів інформаційної системи та дозволяє чітко ідентифікувати проміжні рівні безпеки. Використання детальної шкали оцінювання сприяє більш точному визначенню слабких місць у системі захисту інформації, а також забезпечує можливість проведення порівняльного аналізу між різними елементами інформаційної інфраструктури підприємства. Мурашко О.В. акцентував увагу на економічному ефекті від упровадження заходів інформаційної безпеки. Його системний підхід пов'язує рівень інформаційної безпеки із витратами підприємства та можливими

збитками, що дозволяє обґрунтувати доцільність інвестицій у сферу кіберзахисту.

Методика Тулуп'єва А.О. та Кваші С.В. базується на ієрархічному аналізі загроз, що передбачає три порогові рівні захищеності: низький, середній і високий. Такий підхід орієнтований переважно на технічну складову інформаційної інфраструктури підприємства. Шевченко Л.І. та Ткачук Л.С. розробили просту та доступну шкалу оцінювання ризиків для малих підприємств, яка базується на якісному експертному аналізі з використанням п'ятибальної шкали. Такий підхід, особливо ефективний для компаній з обмеженими ресурсами та відсутністю складних систем моніторингу.

На нашу, важливим у даному випадку є міжнародний стандарт ISO/IEC 27001:2022, який визначає вимоги до системи управління інформаційною безпекою та містить набір контрольних заходів. Хоча він не встановлює конкретних порогових значень у вигляді бальної шкали, стандарт дозволяє підприємствам оцінити рівень відповідності системи управління інформаційною безпекою за категоріями: низький, середній або високий рівень контролю. Перевагою такого підходу є можливість сертифікації та міжнародного визнання. Таким чином, представлені методичні підходи різняться за складністю, обсягом застосування та ступенем формалізації, однак усі вони спрямовані на виявлення критичних меж безпеки та обґрунтування заходів щодо її зміцнення в умовах зростання цифрових загроз.

Узагальнений аналіз наукових підходів до визначення порогових значень стану інформаційної безпеки підприємств засвідчив, що ефективне управління інформаційними ризиками потребує методологічно обґрунтованої системи оцінювання, яка враховує як кількісні, так і якісні параметри захищеності. Представлені у літературі підходи, зокрема ризикоорієнтовані моделі, бальні шкали та стандартизовані системи контролю (ISO/IEC 27001), дозволяють ідентифікувати критичні рівні інформаційної вразливості, забезпечити порівнянність результатів моніторингу у часовому та організаційному розрізі, а також адаптувати заходи інформаційної безпеки до специфіки суб'єкта

господарювання. Важливість таких підходів, відповідно до мети нашого дослідження, полягає у їх здатності формалізувати оцінку стану інформаційної безпеки та забезпечити інтеграцію такої оцінки в загальну систему управління підприємницькими ризиками та стратегічного розвитку організацій в умовах цифрових трансформацій і зростаючих кіберзагроз для суб'єктів підприємництва.

Аналіз методичних підходів до визначення порогових значень стану та рівнів інформаційної безпеки суб'єктів підприємництва засвідчує їх широкий спектр та різноманітність. Зважаючи на мету нашого дослідження, пропонуємо визначити 4 рівні інформаційної безпеки суб'єктів малого підприємництва: низький, середній, достатній та високий. Кожен із запропонованих рівнів характеризує певний стан готовності підприємства до протидії інформаційним загрозам, ступінь захищеності інформаційних ресурсів, наявність політик та процедур безпеки, а також рівень обізнаності персоналу. Низький рівень відповідає ситуації, коли заходи з інформаційної безпеки носять формальний характер або повністю відсутні, технічна інфраструктура застаріла, а ризики не ідентифікуються та не контролюються. Середній рівень передбачає наявність окремих заходів захисту, використання базових ІТ-рішень, проведення епізодичних навчань персоналу, проте відсутня цілісна система управління інформаційною безпекою. Достатній рівень характеризується структурованою політикою безпеки, регулярними аудитами, активним управлінням ризиками, а також наявністю окремого відповідального за інформаційну безпеку. Високий рівень передбачає інтеграцію інформаційної безпеки у всі бізнес-процеси, високий рівень технічного оснащення, автоматизовану систему моніторингу подій безпеки, а також постійне вдосконалення засобів захисту відповідно до змін у зовнішньому середовищі.

Врахування у дослідженні такої градації дозволяє створити уніфіковану основу для порівняльного аналізу підприємств, діагностики критичних зон ризику та формування пріоритетних напрямів підвищення інформаційної стійкості суб'єктів підприємництва, що відкриває можливості для розроблення

цілових програм підтримки малих підприємств у сфері інформаційної безпеки, адаптованих до їхнього поточного рівня розвитку та реальних ресурсних можливостей. У науковій площині, сформувався широкий спектр методик оцінювання інформаційної безпеки суб'єктів підприємництва, які відрізняються за ступенем деталізації, складністю реалізації та орієнтацією на конкретні види ризиків. Вибір відповідного підходу залежить від розміру підприємства, його специфіки діяльності, наявності інформаційних активів і цілей управління. Важливо, що більшість сучасних методик ґрунтуються на використанні системи показників – кількісних або якісних критеріїв, що дають змогу об'єктивно оцінити стан інформаційної безпеки, визначити критичні зони та пріоритети для вдосконалення захисних заходів [71]. Існуючі методичні підходи до оцінки стану забезпечення інформаційної безпеки суб'єктів підприємництва систематизовано в таблиці 2.3.

Таблиця 2.3 – Характеристики існуючих методичних підходів до оцінки стану забезпечення інформаційної безпеки суб'єктів підприємництва

Назва підходу	Автори	Методи оцінки	Система показників	Переваги	Недоліки
Методика комплексного оцінювання стану ІБ підприємства	А. В. Велігура	Індикаторний аналіз, порівняльний аналіз	Показники рівня захисту, політик безпеки, інцидентів	Комплексність, виявлення слабких місць	Потребує багато ресурсів, складна для МСП
Методика оцінки ризиків OCTAVE	CERT Coordination Center (США)	Аналіз загроз, оцінка вразливостей, класифікація активів	Критичність активів, ймовірність загроз, вразливість	Орієнтація на організаційні потреби, залучення персоналу	Трудомістка, складна для новачків
Методика оцінки ризиків CRAMM	ССТА (Велика Британія)	Ідентифікація активів, оцінка загроз, розрахунок ризиків, контрзаходи	Цінність активів, рівень загроз, ефективність контрзаходів	Детальність, підтримка ПЗ	Складна у впровадженні, перевантаженість для МСП
Факторний аналіз з байєсівськими мережами	І. Добринін, Т. Радивілова, Н. Мальцева, Д. Агєєв	Факторний аналіз, байєсівські мережі	Ймовірність настання події, вплив на активи, фактори ризику	Кількісна оцінка на основі якісних даних, врахування взаємозв'язків	Потребує спеціального математичного апарату

Джерело: узагальнено автором на основі [66, 70, 72, 73]

У сучасних умовах цифрової трансформації бізнесу забезпечення інформаційної безпеки суб'єктів підприємництва є критично важливим завданням, що потребує науково обґрунтованих методичних підходів до оцінювання її стану. Відповідна оцінка має базуватися на фактичному аналізі технічного стану інформаційної інфраструктури та на врахуванні організаційних, економічних, правових і поведінкових чинників. У науковій літературі існує кілька визнаних підходів до оцінки інформаційної безпеки, що суттєво різняться за методологією, інструментарієм і сферою застосування.

Комплексна методика, запропонована Велігурою А.В., базується на використанні індикаторного та порівняльного аналізу [66]. Такий підхід дозволяє оцінити рівень інформаційної безпеки підприємства за сукупністю важливих показників, включаючи ефективність політик безпеки, частоту інцидентів, рівень впровадження стандартів. Методика є універсальною, проте потребує значних ресурсів і є складною для малих підприємств, що обмежує її масштабованість. Її перевагою є можливість адаптації до різних галузей шляхом розширення системи оцінних індикаторів.

Міжнародні методики, зокрема OCTAVE (CERT, США) та CRAMM (ССТА, Велика Британія), орієнтовані переважно на управління ризиками. Вони включають ідентифікацію активів, аналіз загроз і вразливостей, визначення критичності ресурсів і розробку відповідних контрзаходів [72, 73]. У межах цих підходів формується система показників, яка враховує ймовірність загроз, вартість активів, ступінь уразливості, що дозволяє реалізувати ефективну пріоритизацію заходів безпеки. Основною перешкодою для використання цих методик є їхня складність та потреба в спеціалізованому програмному забезпеченні.

Сучасні дослідження у сфері інформаційної безпеки також акцентують увагу на використанні математичних моделей, зокрема байєсівських мереж, для переходу від якісного до кількісного аналізу ризиків. Такий підхід дозволяє враховувати багатофакторність впливу на інформаційну безпеку, моделювати причинно-наслідкові зв'язки, а також оцінювати ймовірність настання

інцидентів. Система показників у цьому випадку включає оцінку ймовірностей, взаємозалежність загроз і потенційні наслідки, що підвищує точність аналітики. Модель вимагає високого рівня кваліфікації спеціалістів і наявності достовірних даних для коректного застосування.

З огляду на багатовимірність та міждисциплінарний характер проблеми, методологічний інструментарій дослідження інформаційної безпеки має включати як загальнонаукові, так і спеціалізовані емпіричні та прикладні методи. Важливим є поєднання теоретичного аналізу із практичними підходами до збору та інтерпретації даних, що дозволяє виявляти існуючі загрози та моделювати потенційні ризики та обґрунтовувати управлінські рішення. Вибір методів дослідження повинен відповідати цілям та завданням дослідження, забезпечуючи комплексну оцінку як технічного стану системи захисту, так і організаційно-економічних аспектів управління інформаційною безпекою на підприємстві. Методологічний інструментарій дослідження проблеми забезпечення інформаційної безпеки підприємств систематизовано на рис. 2.1.

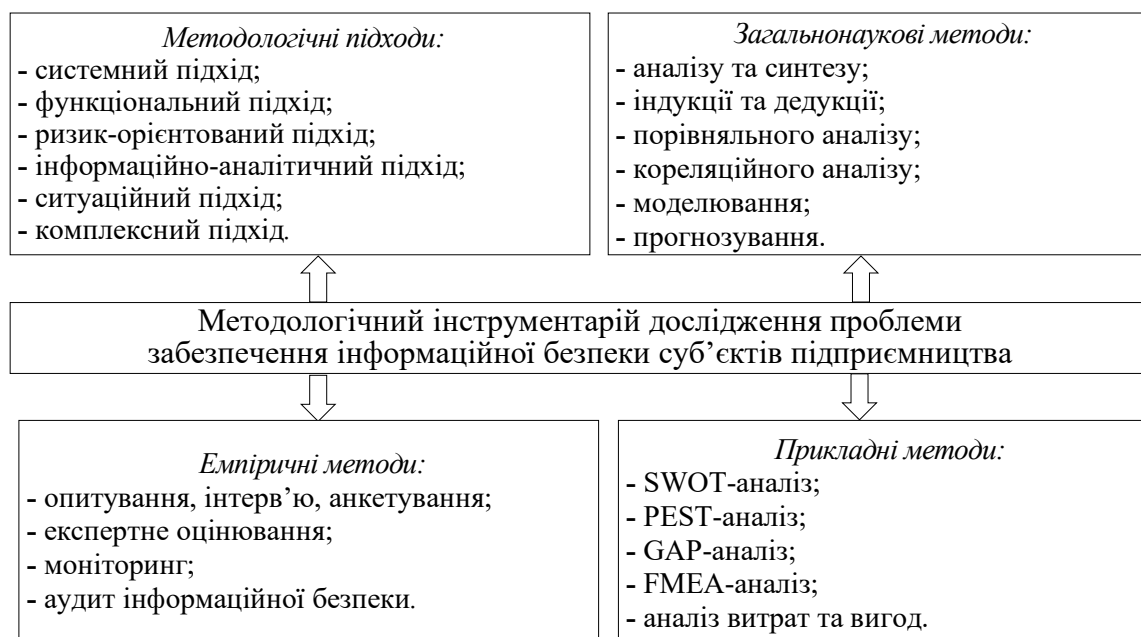


Рис. 2.1. Методологічний інструментарій дослідження проблеми забезпечення інформаційної безпеки підприємств.

Джерело: розроблено автором

Основою методології, відповідно до мети нашого дослідження, виступають підходи, які дозволяють сформувати комплексне бачення досліджуваної проблематики. Зокрема, системний підхід забезпечує цілісне уявлення про інформаційну безпеку як взаємозалежну систему елементів, функціональний підхід дає змогу вивчити роль та взаємодію компонентів захисту, ризик-орієнтований підхід дозволяє акцентувати увагу на пріоритетних загрозах, інформаційно-аналітичний – використовує обробку даних для прийняття рішень, ситуаційний забезпечує адаптацію до змінних умов, а комплексний підхід інтегрує зазначені підходи у єдину дослідницьку стратегію.

На етапі наукового пізнання використовуються загальнонаукові методи, які формують логічну та аналітичну базу дослідження, так методи аналізу і синтезу дозволяють складні системи, поділяти на елементи і знову їх об'єднувати в одну картину, індукція та дедукція забезпечують формування гіпотез та їх перевірку, порівняльний аналіз допомагає зіставляти рівень інформаційної безпеки підприємствах, кореляційний аналіз виступає ефективним інструментом виявлення взаємозв'язків між чинниками ризику та рівнем безпеки, моделювання та прогнозування дають можливість створювати сценарії розвитку подій і визначати оптимальні шляхи реагування на потенційні загрози.

Важливим компонентом дослідження є емпіричні методи, які забезпечують отримання достовірних первинних даних. Методики опитування, інтерв'ю та анкетування дозволяють вивчити думки і поведінкові особливості персоналу щодо практик інформаційної безпеки, експертне оцінювання дає змогу залучити до аналізу фахівців з відповідної галузі з метою підвищення обґрунтованості висновків, моніторинг та аудит інформаційної безпеки дозволяють відстежувати стан інформаційних систем, виявляти загрози в режимі реального часу та оцінювати ефективність діючих заходів захисту.

Важливу роль у дослідженні відіграють прикладні методи, які дають змогу здійснити структурований аналіз внутрішніх та зовнішніх чинників впливу на інформаційну безпеку. SWOT-аналіз визначає сильні та слабкі сторони, можливості і загрози в системі захисту, PEST-аналіз дозволяє оцінити політичні,

економічні, соціальні та технологічні чинники, GAP-аналіз ідентифікує розриви між бажаним і реальним станом безпеки, FMEA-аналіз фокусується на виявленні потенційних відмов систем і їх наслідків, тоді як аналіз витрат і вигод допомагає обґрунтувати економічну доцільність впровадження захисних заходів. Тож, однією з проблем забезпечення інформаційної безпеки є відсутність уніфікованого підходу до визначення допустимих меж стану безпеки [74].

Проведений аналіз методологічного інструментарію забезпечення інформаційної безпеки підприємств дозволяє розробити алгоритм дослідження зазначеного процесу.

Пропонуємо дослідження поділити на послідовні етапи, які охоплюють шлях від визначення мети дослідження до оцінки ефективності реалізації стратегій інформаційної безпеки. Кожен етап має містити логіку, поєднуючи аналітичні дії (збір та аналіз даних, оцінювання стану безпеки) зі стратегічними кроками (формування рішень, впровадження заходів та коригування стратегії), що представлено на рис. 2.2.

Алгоритм дослідження процесу забезпечення інформаційної безпеки суб'єктів підприємництва структуровано у вигляді послідовних дев'яти логічно взаємопов'язаних етапів, кожен з яких спрямований на досягнення визначеної дослідницької мети та забезпечення ефективного управління інформаційною безпекою суб'єктів підприємництва. Запропонована структура поєднує як діагностичні, так і стратегічні компоненти, що дозволяє здійснити кількісну та якісну оцінку рівня інформаційної безпеки і окреслити напрями її вдосконалення.

На першому етапі формулюється мета дослідження – кінцевий результат, якого планується досягти у забезпеченні інформаційної безпеки підприємств. Визначаються конкретні завдання, об'єкт і предмет дослідження, а також обираються методи та підходи, що будуть використані для аналізу (аналітичний зміст) та розробки рекомендацій (стратегічний зміст). На цьому етапі доцільно чітко окреслити, які аспекти процесу забезпечення інформаційної безпеки підприємства будуть вивчатися (наприклад, стан захищеності даних, вплив інвестицій на діяльність тощо) і якими методами (опитування, аудит,

статистичний аналіз, економіко-математичне моделювання тощо) будуть отримані необхідні дані.

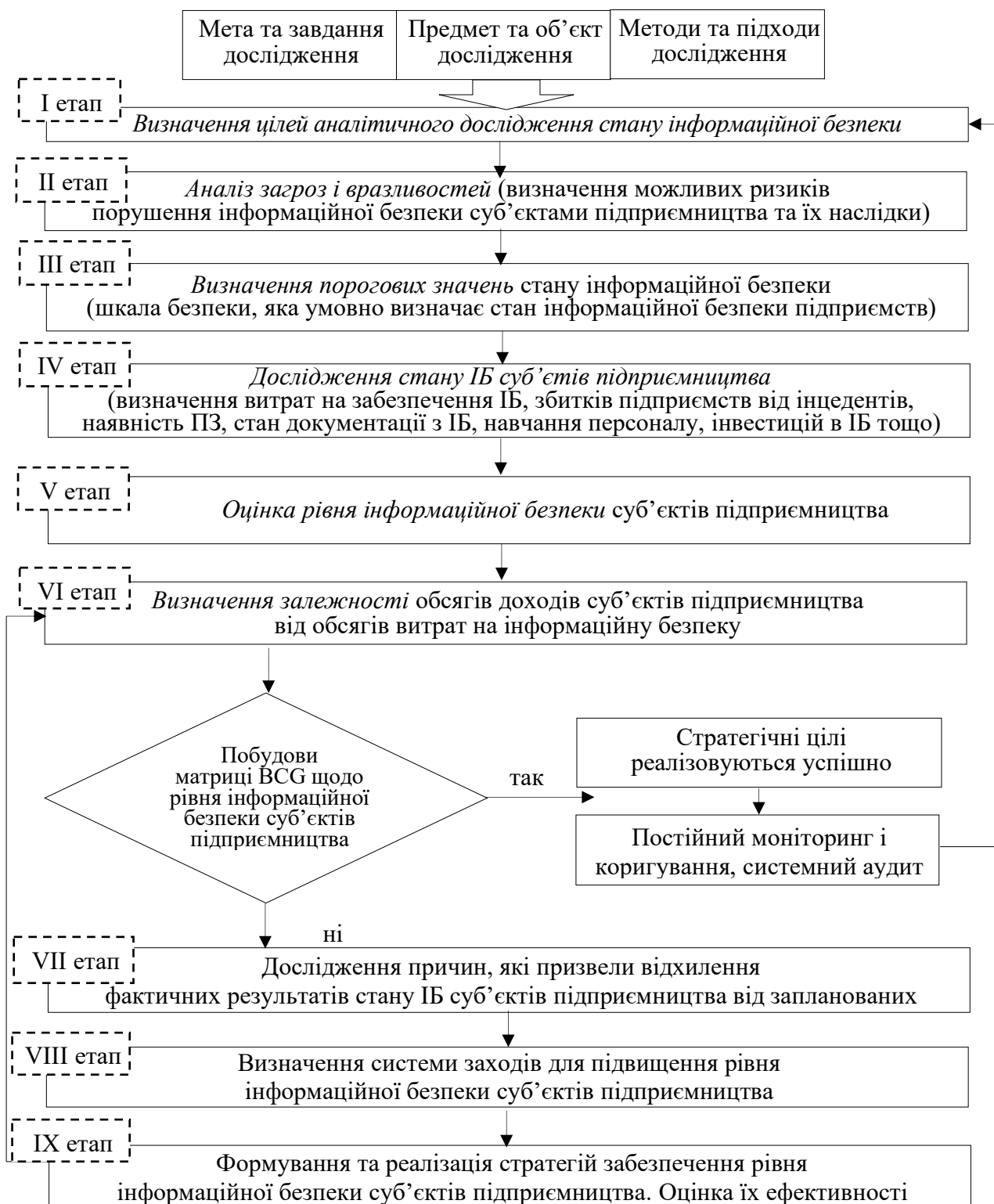


Рис. 2.2. Алгоритм дослідження процесу забезпечення інформаційної безпеки суб'єктів підприємництва

Джерело: розроблено автором

Очікуваним результатом є сформований план дослідження: чітко сфокусована мета, перелік дослідницьких питань і методологія їх вирішення. Практична значущість етапу, наприклад для суб'єктів малого підприємництва полягає в тому, що правильно визначена мета та завдання гарантують орієнтацію дослідження на реальні потреби бізнесу. Такий підхід забезпечує, що подальші результати будуть актуальними та корисними для підвищення рівня інформаційної безпеки в умовах малого підприємництва.

Другий етап передбачає ідентифікацію актуальних загроз та вразливостей інформаційних систем суб'єктів підприємництва. Аналітична складова етапу полягає у виявленні джерел загроз (технічних, організаційних, людських, зовнішніх) та у класифікації можливих вразливостей, які можуть бути використані зловмисниками. Це може включати недосконалості в ІТ-інфраструктурі, відсутність політик безпеки, ненавчений персонал, відкриті мережеві порти або застаріле програмне забезпечення. Стратегічна складова – у прогнозуванні наслідків реалізації ризиків: фінансових втрат, зупинки діяльності, витоку конфіденційних даних тощо. На основі цього формуються матриці ризиків або таблиці ймовірності та наслідків, що дозволяють ранжувати загрози за рівнем критичності. Очікуваний результат – структурований опис потенційних загроз, типових вразливостей та їхніх можливих наслідків для підприємств. Практична значущість – дозволяє усвідомити, які саме ризики є найбільш імовірними та шкідливими, і зосередити ресурси на попередженні цих загроз.

На третьому етапі встановлюються критерії та порогові значення для оцінювання стану інформаційної безпеки підприємств. По суті, формується «шкала безпеки» – система показників або бальна шкала, що умовно розподіляє рівень інформаційної безпеки на категорії. Аналітичний зміст цього етапу полягає у вивченні стандартів, нормативів та найкращих практик, щоб визначити, які саме показники (кількість інцидентів, наявність політик безпеки, обсяг інвестицій тощо) слід враховувати і які граничні значення свідчать про належний чи критичний стан безпеки. Стратегічний зміст полягає у встановленні

бенчмарків, підприємство отримує орієнтири, з якими можна порівнювати фактичний стан інформаційної безпеки і на основі яких формуватимуться цілі покращення. Очікуваний результат – розроблена шкала або модель оцінки рівня інформаційної безпеки, що дозволяє класифікувати кожне підприємство за рівнем захищеності. Практична значущість – малі підприємства отримують зрозумілий інструмент діагностики своєї безпеки. Знаючи порогові значення, керівники при проведенні аудиту можуть визначити, чи відповідає стан захищеності мінімально прийнятним вимогам, і вчасно реагувати, якщо рівень інформаційної безпеки занадто низький.

Четвертий етап передбачає емпіричне дослідження фактичного стану інформаційної безпеки суб'єктів підприємництва з урахуванням основних показників, що відображають рівень захищеності організації. Аналітична частина зосереджується на зборі, систематизації та аналізі даних за такими напрямками: обсяги витрат на забезпечення інформаційної безпеки у структурі загальних витрат, розмір збитків, яких зазнали підприємства внаслідок інцидентів, обсяги інвестицій тощо. Стратегічна значущість етапу полягає в ідентифікації сильних та слабких місць у системах інформаційної безпеки підприємств, що дає змогу в подальшому обґрунтовано формувати напрями поліпшення. Такий підхід забезпечує керівників підприємств фактичними даними для об'єктивної оцінки рівня безпеки, дозволяє визначити зони ризику та виявити критичні аспекти, що потребують негайного реагування, що формує основу для подальших стратегічних рішень у сфері інформаційної безпеки.

На п'ятому етапі проводиться оцінка фактичного рівня інформаційної безпеки конкретних підприємств – об'єктів дослідження. В результаті формується кількісно-якісний портрет поточного стану інформаційної безпеки кожного підприємства за релевантними індикаторами. Завдяки цьому, суб'єкти підприємництва отримують об'єктивну оцінку своєї безпеки. Таке «діагностування» дозволяє управлінцям усвідомити реальну картину – наприклад, чи є їхній бізнес вразливим до кіберзагроз, які слабкі місця

потребують уваги – що є необхідною передумовою для прийняття обґрунтованих рішень щодо вдосконалення інформаційної безпеки.

Шостий етап має на меті дослідження взаємозв'язку між інвестиціями в інформаційну безпеку та фінансовими результатами підприємства (зокрема, обсягами його доходів або прибутків). Аналітичний зміст етапу полягає у зборі та статистичному аналізі даних, порівнянні витрати на заходи інформаційної безпеки (наприклад, частка бюджету, спрямована на інформаційну безпеку) з економічними показниками діяльності малого підприємства, що може включати кореляційний аналіз або побудову економетричних моделей, що дозволяють виявити, чи існує позитивна віддача від вкладень у безпеку – наприклад, зменшення втрат від інцидентів, уникнення простоїв, збереження довіри споживачів, що врешті відображається на доходах. Стратегічний аспект проявляється в інтерпретації отриманих залежностей, якщо виявлено сильний позитивний ефект, це аргументує необхідність стратегічних інвестицій в інформаційну безпеку, якщо зв'язок слабкий або негативний, можливо, підприємству слід оптимізувати витрати чи перерозподілити ресурси. В результаті реалізації цього етапу визначається кількісна оцінка взаємозв'язку між рівнем витрат на інформаційну безпеку та економічною ефективністю підприємств (наприклад, коефіцієнт кореляції, графічна залежність або формула), що дає підприємствам відповідь на питання – «Чи окупаються вкладення в інформаційну безпеку?». Багато невеликих компаній побоюються витратити кошти на захист, вважаючи це тягарем. Аналіз залежності витрат і доходів допомагає обґрунтувати такі витрати мовою бізнесу, а саме показати, що недофінансування безпеки може призводити до серйозних фінансових втрат, тоді як розумні інвестиції здатні захистити дохід і репутацію компанії.

На сьомому етапі результати попередніх аналізів узагальнюються шляхом побудови матриці BCG у розрізі рівня інформаційної безпеки досліджуваних підприємств. Класична матриця BCG використовується для стратегічного аналізу бізнес-портфеля, поділяючи об'єкти на чотири категорії. У нашому випадку матрицю доцільно адаптувати до сфери інформаційної безпеки суб'єктів

підприємництва. Аналітичний зміст етапу полягає у виборі двох показників для матриці: одним виміром є рівень інформаційної безпеки підприємства (високий чи низький відносно інших, за результатами етапу IV), іншим – показник бізнес-успішності. Стратегічний зміст матриці BCG-ІБ полягає в тому, що кожна категорія підприємств потребує різних підходів до забезпечення безпеки. Матриця BCG спрощує ухвалення рішень, підказуючи, чи слід агресивніше інвестувати в інформаційну безпеку, підтримувати поточний рівень, чи мінімізувати витрати (залежно від категорії).

Восьмий етап присвячений виявленню та аналізу причин, через які фактичний стан інформаційної безпеки малих підприємств може не відповідати бажаному або запланованому рівню. Під запланованим рівнем розуміють орієнтир або цільові значення інформаційної безпеки. Аналітичний зміст етапу – провести причинно-наслідковий аналіз: з'ясувати, чому виникли виявлені прогалини. Стратегічний зміст етапу полягає у використанні цієї інформації для коригування підходів: розуміння причин дозволяє розробити адекватні рекомендації, які адресують корінні проблеми, а не лише їх симптоми. Цей етап дає підприємствам розуміння «що саме пішло не так». Виявивши першопричини слабого захисту (скажімо, недоліки в навчанні персоналу чи помилки у виборі засобів безпеки), компанія може спрямувати зусилля на ці проблемні місця. На даному етапі, закладається основа для ефективнішого планування наступних кроків – стратегій, які враховують реальні обмеження і можливості підприємства.

На восьмому етапі відбувається формування та впровадження стратегії інформаційної безпеки для підприємств. Спираючись на всі попередні аналітичні напрацювання, розробляється комплексна стратегія забезпечення інформаційної безпеки. Аналітична складова етапу включає вибір оптимального набору заходів з урахуванням специфіки кожного підприємства та категорії, до якої воно належить. Для підприємств різних типів будуть доречні різні стратегії: наприклад, суб'єктам з низьким рівнем інформаційної безпеки і високим бізнес-потенціалом слід реалізувати стратегію інтенсивного посилення безпеки (значні інвестиції в критичні заходи, швидке усунення вразливостей), тоді як компанії з

високим рівнем інформаційної безпеки може підійти стратегія підтримання (удосконалення існуючих систем та точкове поліпшення). Наявність стратегії забезпечує системність у захисті інформації – всі важливі напрями (техніка, люди, процеси) охоплені і взаємоузгоджені. Впровадження стратегічних заходів безпосередньо підвищує рівень безпеки. скорочується кількість інцидентів, зменшується ризик успішних атак, підвищується готовність до надзвичайних ситуацій. Крім того, стратегія враховує можливості бізнесу – оптимізує витрати на інформаційну безпеку, розставляючи пріоритети так, щоб безпека досягалася економічно ефективно, без надмірного навантаження на бюджет підприємства. Таким чином, підприємство переходить у режим безперервного вдосконалення процесу інформаційної безпеки. Подібний циклічний підхід відповідає принципам управління інформаційною безпекою, зокрема моделі «PDCA» (Plan-Do-Check-Act – плануй, виконуй, перевіряй, дій), що гарантує підтримання високого рівня захищеності в довгостроковій перспективі.

Високий рівень інтеграції інформаційно-комунікаційних технологій у бізнес-процеси зумовлює зростання залежності від надійності, конфіденційності та доступності інформаційних ресурсів. Постійне зростання кількості та складності кіберзагроз вимагає системного підходу до моніторингу та оцінювання рівня захищеності підприємства. Вирішення цього завдання потребує чітко сформованої системи показників, що дозволяє здійснювати комплексну діагностику інформаційної безпеки.

Такі показники мають відображати технічний стан систем захисту та ефективність організаційних механізмів, поведінкові аспекти персоналу, рівень інформаційної досконалості підприємства та здатність протидіяти як внутрішнім, так і зовнішнім загрозам. Структурування показників за окремими напрямками дозволяє забезпечити цілісність оцінки та приймати обґрунтовані управлінські рішення.

Показники, що характеризують інформаційне забезпечення виробничих або сервісних процесів, дають змогу оцінити ступінь інтегрованості інформаційних технологій у основні бізнес-функції підприємства.

Таблиця 2.4 – Система показників для оцінки рівня інформаційної безпеки підприємства

Група показників, що характеризують	Показники
Інформаційне забезпечення виробничих або сервісних процесів (ступінь автоматизації інформаційних процесів)	Доступність інформаційних систем для користувачів. Наявність регламентів інформаційної підтримки. Частота оновлення інформаційних баз даних. Відмовостійкість основного ПЗ та систем управління виробництвом.
Захист інформаційних ресурсів підприємства (наявність політики інформаційної безпеки)	Частота оновлення антивірусного програмного забезпечення. Кількість виявлених інцидентів ІБ за певний період. Ступінь захисту мережевого периметра. Рівень резервного копіювання та збереження критичних даних.
Протидію негативного впливу зовнішнього потоку інформації (кількість заблокованих зовнішніх атак)	Рівень впровадження систем фільтрації. Наявність захисту від фішингових і соціотехнічних атак. Частота навчання персоналу щодо протидії зовнішнім загрозам. Ступінь дотримання вимог кібергігієни у взаємодії із зовнішніми партнерами.

Джерело: узагальнено автором на основі [61-70, 72, 73].

До таких можливих показників пропонуємо віднести рівень автоматизації інформаційних процесів, доступність інформаційних систем для персоналу, наявність чітких регламентів інформаційної підтримки, регулярність оновлення баз даних і відмовостійкості програмного забезпечення. Зазначені показники визначають, наскільки стабільною та ефективною є система передачі, обробки й збереження інформації в межах операційної діяльності.

До групи показників захисту інформаційних ресурсів підприємства відносять ті, що дозволяють оцінити ступінь впровадження внутрішніх заходів інформаційної безпеки, а саме: наявність політики інформаційної безпеки, що регламентує стандарти захисту; частота оновлення антивірусного програмного забезпечення; кількість зареєстрованих інцидентів порушення безпеки; рівень захищеності мережевого периметра та ефективність систем резервного копіювання. Визначені показники є важливими для підтримання контролю над конфіденційною інформацією та забезпечення безперервності бізнес-процесів.

До показників протидії негативному впливу зовнішнього інформаційного середовища, які спрямовані на оцінку здатності підприємства захищатися від

зовнішніх кіберзагроз, пропонуємо віднести кількість відвернених або заблокованих атак, рівень впровадження систем фільтрації, наявність механізмів захисту від фішингу, регулярність навчання працівників основам інформаційної гігієни, а також дотримання норм безпеки при взаємодії з партнерами та постачальниками. Застосування системи показників, структурованих за трьома основними напрямками, забезпечує комплексне оцінювання стану інформаційної безпеки підприємства, дозволяє виявити слабкі місця та сформулювати обґрунтовані рекомендації для її вдосконалення.

Структуризація системи показників за трьома основними напрямками (інформаційне забезпечення бізнес-процесів, захист внутрішніх ресурсів та протидія зовнішнім загрозам), дозволяє здійснювати всебічну та об'єктивну діагностику стану інформаційної безпеки. Такий підхід забезпечує комплексне охоплення технічних, організаційних і поведінкових аспектів безпеки та створює основу для порівняльного аналізу динаміки ризиків, виявлення критичних вразливостей і формування ефективної політики інформаційного захисту.

2.2 Детермінанти розвитку суб'єктів малого підприємництва України

У сучасних умовах трансформації цифрового середовища розвиток суб'єктів малого підприємництва в Україні набуває особливого значення, зважаючи на його роль у забезпеченні економічної стійкості, створенні робочих місць та стимулюванні інновацій. Проте поряд із потенціалом зростає і вразливість малого бізнесу до інформаційних загроз, що зумовлює необхідність вивчення економічних, соціальних та регуляторних чинників впливу та засад інформаційної безпеки [75]. Інформаційна безпека для суб'єктів малого підприємництва є стратегічною передумовою сталого розвитку. Загрози кібератак, витоку комерційно чутливої інформації, фішинг, шахрайство з використанням ІТ-технологій можуть мати катастрофічні наслідки для малого бізнесу, який, як правило, має обмежені ресурси для побудови повноцінних систем захисту, що зумовлює потребу дослідження тих детермінант, які

стимулюють розвиток підприємництва та сприяють підвищенню його інформаційної захищеності.

Для коректної оцінки поточного рівня інформаційної безпеки суб'єктів малого підприємництва та визначення стратегічних орієнтирів забезпечення досліджуваних процесів, доцільно здійснити дослідження ситуації розвитку зазначених суб'єктів на ринку України. Такий підхід є основою для розуміння того, як інформаційна безпека може вплинути на діяльність суб'єктів малого підприємництва. Так, інформаційне середовище та цифровізація є важливим чинником трансформації малого та середнього бізнесу в Україні, особливо в умовах викликів останнього десятиліття. Економічна турбулентність, геополітична нестабільність, пандемічні обмеження та повномасштабна війна стали каталізаторами структурних змін у підприємницькому секторі. Крім того, стрімкий розвиток цифрових технологій, доступ до онлайн-сервісів та інтеграція інструментів електронного урядування створили нові можливості для розвитку МСБ, зокрема шляхом спрощення процедур ведення бізнесу, розширення доступу до ринків і підвищення адаптивності.

Для аналізу стану розвитку суб'єктів малого підприємництва, необхідно володіти достовірною статистичною інформацією, зокрема щодо загальної кількості суб'єктів такого бізнесу та основних показників їх діяльності. Так, дослідження динаміки суб'єктів підприємницької діяльності в контексті інформаційної безпеки дозволяє виявити основні тенденції трансформації підприємницького ландшафту України, оцінити ефективність реалізованих цифрових рішень та окреслити подальші напрями розвитку інформаційної екосистеми малого бізнесу (рис. 2.3).

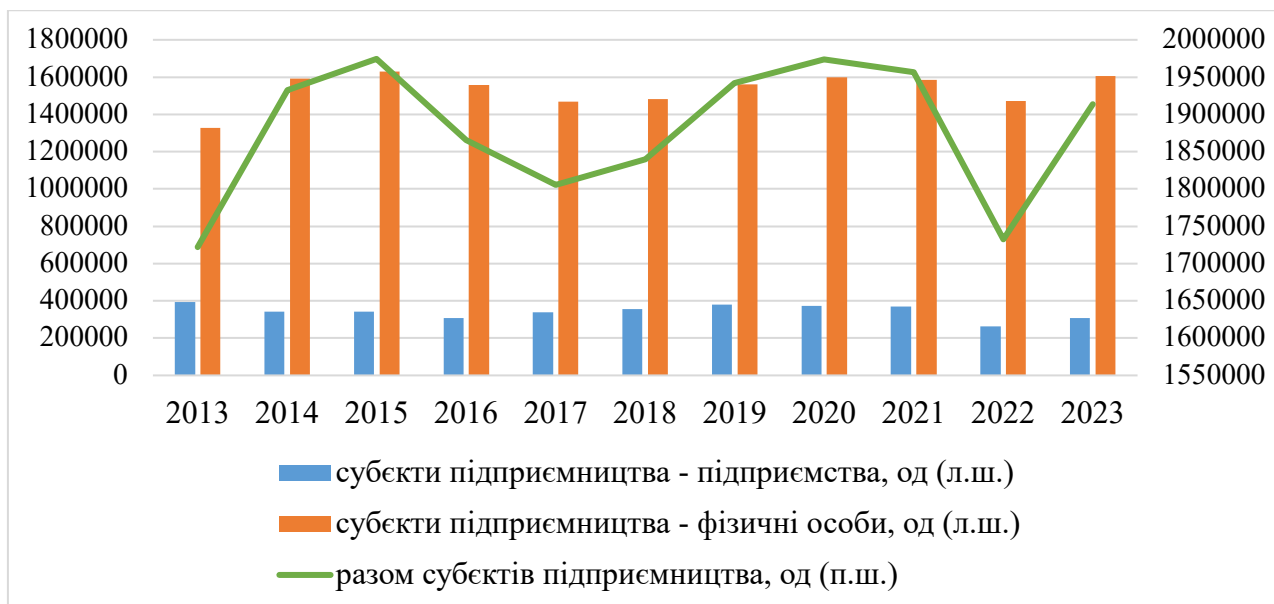


Рис. 2.3. Динаміка кількості суб'єктів підприємництва України у розрізі різновидів суб'єктів господарювання протягом 2013-2023 роках.

Джерело: побудовано автором на основі [76, 77].

У період з 2013 по 2023 рік спостерігається суттєва трансформація структури суб'єктів підприємницької діяльності в Україні. Зокрема, кількість фізичних осіб-підприємців демонструє тенденцію до зниження в період 2013-2016 рр., що пов'язано із впровадженням нових правил оподаткування, а також загальною макроекономічною нестабільністю, викликаною збройною агресією росії. Проте, починаючи з 2017 року, кількість ФОП знову зростає, що свідчить про активізацію самозайнятості, поліпшення цифрової інфраструктури для реєстрації бізнесу та розвиток онлайн-сервісів.

Малі та середні підприємства, демонструють порівняно стабільні, проте більш помірні темпи приросту, що може свідчити про більшу вразливість даної форми господарювання до змін у законодавстві, регуляторному середовищі та фінансовому тиску. Особливо помітним є зменшення кількості юридичних осіб у 2020 році, що корелює з наслідками пандемії COVID-19, яка істотно вплинула на фінансову стійкість бізнесу, особливо в секторах послуг, роздрібної торгівлі та транспорту. Період з 2021 року демонструє певне відновлення, однак загальна структура залишається стабільною: частка ФОП продовжує переважати, що свідчить про гнучкість і адаптивність цієї форми ведення бізнесу в умовах криз.

Динаміка також відображає зростання цифрової активності підприємців, зокрема, спрощення доступу до адміністративних послуг через цифрові платформи на зразок «Дія» [78], розширення можливостей для дистанційного ведення бізнесу, електронного документообігу та онлайн-торгівлі.

Отже, аналіз динаміки кількості суб'єктів підприємництва за 2013-2023 роки дозволяє зробити висновок про позитивний вплив цифровізації на підтримку і розвиток підприємницької активності, особливо у секторі мікро- та малого бізнесу. Цифрове середовище стає важливим чинником підтримки життєздатності бізнесу в умовах нестабільності та каталізатором для його структурної еволюції. Аналіз динаміки кількості суб'єктів підприємництва у розрізі різновидів суб'єктів господарювання протягом 2013-2023 рр. засвідчує глибокі трансформації підприємницького середовища в Україні, зумовлені як зовнішніми викликами (економічна криза, пандемія, війсьні дії), так і внутрішніми чинниками цифровізації. Спостерігається зростання ролі фізичних осіб-підприємців як найбільш адаптивної форми ведення бізнесу в умовах нестабільності. Цифрові інструменти, платформи електронного урядування та спрощені процедури реєстрації і адміністрування підприємницької діяльності стали важливими чинниками підтримки та стимулювання самозайнятості. Таким чином, цифровізація дедалі більше виконує роль драйвера розвитку малого та середнього бізнесу, посилюючи його стійкість, мобільність і конкурентоспроможність.

Зважаючи євроінтеграційні процеси України та мету нашого дослідження, пропонуємо визначити чітку класифікацію суб'єктів господарювання за критеріями, які використовуються в країнах ЄС та в Україні, що представлено в таблиці 2.5. Класифікацію суб'єктів господарювання за критеріями, які використовуються в країнах ЄС та в Україні базується на трьох основних показниках: річному обороті, кількості працівників і річному балансі. Поділ підприємств за розміром є важливою умовою для обґрунтування економічної політики, спрямованої на підтримку різних груп підприємств відповідно до

їхнього потенціалу та відповідно до цього – залежність рівня інформаційної безпеки від зазначених показників.

Таблиця 2.5 – Класифікація суб'єктів господарювання

Види бізнесу	Критерії	ЄС	Україна
Мікро- суб'єкти бізнесу	Річний оборот, млн євро	< 2	< 2
	Кількість працівників	< 10	< 10
	Річний баланс, млн євро	< 2	не визначено
Суб'єкти малого бізнесу	Річний оборот, млн євро	< 10	< 10
	Кількість працівників	< 50	< 50
	Річний баланс, млн євро	< 10	не визначено
Суб'єкти середнього бізнесу	Річний оборот, млн євро	< 50	< 50
	Кількість працівників	< 250	< 250
	Річний баланс, млн євро	< 43	не визначено

Джерело: узагальнено на основі [79].

Мікропідприємства в обох системах класифікації визначаються як такі, що мають річний оборот менше 2 мільйонів євро та кількість працівників менше 10 осіб, що узгоджується з підходами ЄС і відображає прагнення України до гармонізації національного законодавства з європейськими стандартами. Однак у показнику річного балансу спостерігається відмінність, у ЄС він обмежений рівнем до 2 мільйонів євро, тоді як в українській класифікації цей критерій формально не визначений. Відсутність чітких параметрів річного балансу в Україні ускладнює проведення повноцінного фінансового аналізу та зіставлення підприємств за однаковими ознаками.

Для суб'єктів малого підприємництва, поріг річного обороту встановлений на рівні до 10 мільйонів євро, а кількість працівників – до 50 осіб. Як і у випадку з мікропідприємствами, в Україні не встановлено межі для річного балансу, що свідчить про певну спрощеність підходу до класифікації і може створювати бар'єри для застосування єдиних норм податкового або фінансового регулювання. Щодо середнього бізнесу – в обох системах встановлено обмеження річного обороту на рівні до 50 мільйонів євро і чисельність працівників – до 250 осіб. У ЄС додатково враховується баланс у розмірі до 43 мільйонів євро, що дозволяє точніше визначати фінансову вагу підприємства. Така комплексна модель дає змогу краще диференціювати економічну

активність суб'єктів господарювання, забезпечуючи ґрунтоване прийняття рішень щодо їх підтримки, доступу до фінансування або участі в пільгових програмах. Такий підхід до групування суб'єктів підприємництва є необхідною умовою для ефективного управління економікою, формування сприятливого бізнес-середовища та розробки цільових стратегій підтримки мікро-, малого та середнього бізнесу, а також визначення стратегічних засад забезпечення інформаційної безпеки досліджуваних суб'єктів. Гармонізація української системи з європейськими стандартами є важливим кроком у напрямі інтеграції до єдиного економічного простору ЄС.

Сьогодні суб'єкти малого підприємництва відіграють важливу роль у соціально-економічному розвитку країни. В умовах глобалізації, цифрової трансформації та викликів, пов'язаних із воєнним станом, інформаційна безпека та цифровізація стає важливою умовою підвищення ефективності, адаптивності та конкурентоспроможності МСП [80]. У цьому контексті аналіз інформаційного середовища, у якому функціонують підприємства, набуває особливого значення, адже саме інформаційна інфраструктура забезпечує доступ до технологій, ринків, інновацій та управлінських рішень.

Інформаційне середовище малого бізнесу в Україні охоплює сукупність цифрових, комунікаційних, аналітичних та інфраструктурних елементів, які впливають на здатність підприємств здійснювати бізнес-процеси, взаємодіяти зі споживачами, партнерами та органами самоврядування. На сучасному етапі основними викликами для українських суб'єктів малого підприємництва залишаються недостатній рівень доступу до цифрових рішень, обмежені ресурси для модернізації, низький рівень цифрової грамотності серед підприємців.

Попри це, спостерігається позитивна динаміка в частині інтеграції цифрових технологій такими суб'єктами. Зокрема, підприємства активно впроваджують онлайн-продажі, CRM-системи, хмарні сервіси, системи електронного документообігу, використовують платформи для аналітики даних та автоматизації бізнес-процесів. Важливим стимулом для цифровізації стали реформи у сфері цифрового врядування, зокрема електронні сервіси «Дія»,

цифрові податкові інструменти, а також міжнародна технічна допомога, спрямована на відновлення бізнесу під час війни [81]. Проте рівень цифрової інтенсивності та інформаційної безпеки залишається нерівномірним. За оцінками, понад 65% МСП мають низький або дуже низький рівень цифровізації та відповідно інформаційної безпеки, тоді як лише 10-15% демонструють високі показники впровадження сучасних ІКТ. Такі підприємства переважно зосереджені у великих містах або працюють в ІТ, фінансах, логістиці, торгівлі чи сервісі. У регіонах та серед виробничих підприємств процес цифрової трансформації часто гальмується через брак ресурсів та кваліфікованих кадрів.

Цифрова трансформація МСП в Україні є інструментом технологічного оновлення та стратегічною передумовою для підвищення економічної стійкості, розширення доступу до міжнародних ринків, інноваційної діяльності та підвищення продуктивності праці та забезпечення інформаційної безпеки суб'єктів господарювання. Вона сприяє прозорості бізнесу, зменшенню транзакційних витрат, швидшому прийняттю управлінських рішень, покращенню пропонованого сервісу, а саме основне – зменшенню ризиків пов'язаних з інформаційною безпекою та можливістю кібератак [82]. Таким чином, створення сприятливого інформаційного середовища та підтримка цифровізації малого бізнесу має стати пріоритетом економічної політики держави. Важливими кроками в цьому напрямі є розвиток цифрової інфраструктури, підтримка цифрової освіти підприємців, надання фінансових стимулів для впровадження ІКТ, а також посилення інституційної взаємодії між державою, бізнесом та освітнім середовищем. Лише за умови системного підходу цифровізація, високого рівня інформаційної та як наслідок економічної безпеки, суб'єкти малого підприємництва зможуть стати фундаментом відновлення та модернізації економіки України сьогодні та у повоєнний період.

Структурні показники суб'єктів господарювання є важливим індикатором економічного розвитку територій, оскільки вони відображають кількісний та якісний стан підприємницького середовища, рівень ділової активності, а також вплив бізнесу на формування валового внутрішнього продукту. Особливої ваги

набуває аналіз цих показників у розрізі розміру підприємств, адже суб'єкти малого підприємництва сьогодні на тлі війни росії проти України, виступають рушійною силою інновацій, зайнятості та економічної гнучкості. В умовах цифрової трансформації та глобальних викликів, структурні показники дозволяють оцінити поточний стан бізнес-середовища (таблиця 2.6).

Таблиця 2.6 – Основні структурні показники суб'єктів господарювання країн ЄС та України з розподілом за розмірами

Території	Територія, тис. км ²	Населення, млн. осіб	Загальна кількість підприємств, млн. одиниць	МСП частка, у загальній кількості підприємств, %	МСП, частка у ВВП, %
2022					
ЄС	4234,0	446,8	23,2	99,8	58,0
Україна	603,6	41,2	2,0	99,9	55,0
2023					
ЄС	4234,0	448,2	24,0	99,8	58,4
Україна	603,6	40,4	1,85	99,9	56,2
2024					
ЄС	4234,0	449,3	24,8	99,8	59,0
Україна	603,6	39,8	1,75	99,9	57,5

Джерело: узагальнено на основі [83-88].

Аналіз структурних показників суб'єктів господарювання в ЄС та Україні дозволяє виявити загальні тенденції економічного розвитку, ефективності бізнес-середовища та ролі малого підприємництва в загальній структурі економіки. ЄС має площу 4234 тис. км² з населенням у 2002 року близько 446,8 млн осіб. Загальна кількість зареєстрованих підприємств сягала 23,2 млн, з яких 99,8% становили малі та середні підприємства. Частка МСП у формуванні валового внутрішнього продукту ЄС становила 58,0%. Зазначені показники підтверджують, що мале та середнє підприємництво є основним структуроутворюючим елементом економіки ЄС, створюючи більшість робочих місць та забезпечуючи гнучкість економіки. В Україні ситуація є дещо подібною за структурою, хоча й відрізняється за абсолютними значеннями. Територія України має площу 603,6 тис. км². У 2022 в Україні проживало 41,2 млн осіб, а кількість підприємств становила близько 2 млн. При цьому частка МСП сягала 99,9% у загальному обсязі суб'єктів господарювання, що свідчить про

переважання малого бізнесу. Частка МСП у ВВП України становила 55,0%, що є високим показником і підтверджує важливість цього сектора для національної економіки, особливо в умовах воєнного стану та економічної нестабільності.

У 2023 році в ЄС спостерігалось незначне зростання за всіма основними показниками, кількість підприємств зростає до 24 млн, чисельність населення – до 448,2 млн осіб, а внесок МСП у ВВП – до 58,4%. Таке зростання обумовлено стабільною економічною політикою, цифровою трансформацією та послідовною підтримкою підприємництва в рамках Європейського зеленого курсу та програми індустрії 4.0. В Україні відбувалося скорочення загальної кількості підприємств до 1,85 млн, що пов'язано з наслідками війни, міграційними процесами та тимчасовим припиненням діяльності частини бізнесу. Проте частка МСП у ВВП навіть зростає до 56,2%, що свідчить про адаптивність та стійкість малого бізнесу в кризових умовах.

У 2024 році у ЄС продовжилася позитивна динаміка: кількість підприємств збільшилась до 24,8 млн, населення – до 449,3 млн осіб, а частка МСП у ВВП досягла 59,0%, що є наслідком значного рівня інформаційної безпеки як наслідку системної цифровізації, активного залучення до глобальних ланцюгів постачання та впровадження інновацій. В Україні ж, попри подальше зменшення кількості підприємств до 1,75 млн та зниження чисельності населення до 39,8 млн, спостерігається підвищення частки МСП у ВВП до 57,5%. Така тенденція демонструє високий рівень гнучкості та здатності МСП забезпечувати економічну підтримку навіть у надзвичайно складних умовах.

Суб'єкти малого підприємництва залишаються основою економічної структури як країн ЄС, так і України. Проте, для України характерні виклики, пов'язані з війною, інфраструктурними обмеженнями та проблемами інвестиційного клімату. Незважаючи на це, зростаюча роль МСП у ВВП свідчить про стратегічну важливість розвитку цього сектору, особливо з урахуванням потенціалу цифровізації, інновацій та інтеграції у міжнародні економічні процеси. Так, рівень цифрової трансформації та інформаційної безпеки є одним із основних чинників успішного функціонування суб'єктів малого

підприємництва в країнах Європи, оскільки цифрові інструменти надають підприємствам можливість оперативно реагувати на зміни ринкової ситуації, впроваджувати інновації та оптимізовувати внутрішні процеси. Завдяки використанню сучасних ІТ-рішень компанії можуть забезпечити ефективну взаємодію зі споживачами, автоматизувати операційну діяльність, вийти на нові ринки та знизити витрати. У результаті, такий підхід підвищує їхню стійкість до кризових явищ і забезпечує довгострокове зростання в умовах глобальної конкуренції. Цифровізація виступає технологічною модернізацією та стратегічним чинником трансформації бізнес-моделей, що є визначальним для інтеграції в цифрову економіку майбутнього.

Кадрова політика є одним із основних елементів ефективного функціонування підприємств будь-якого масштабу, оскільки витрати на персонал безпосередньо впливають на фінансову стабільність, продуктивність праці, конкурентоспроможність бізнесу та рівень інформаційної безпеки. В умовах трансформації економіки України, спричиненої зовнішніми шоками, змінами регуляторного середовища та активним впровадженням цифрових технологій, відбувається суттєве переосмислення підходів до управління трудовими ресурсами [89]. Особливо це актуально для малого та середнього підприємництва, яке, з одного боку, демонструє гнучкість у прийнятті управлінських рішень, а з іншого – стикається з обмеженими фінансовими ресурсами для повноцінного забезпечення витрат на персонал. Аналіз динаміки витрат на персонал у розрізі видів економічної діяльності та форм господарювання за період 2013-2023 років дозволяє виявити основні тенденції у розвитку трудового потенціалу, оцінити ступінь цифровізації кадрових процесів та зробити висновки щодо зміни соціально-економічної поведінки бізнесу в умовах постійних викликів (рис. 2.4).

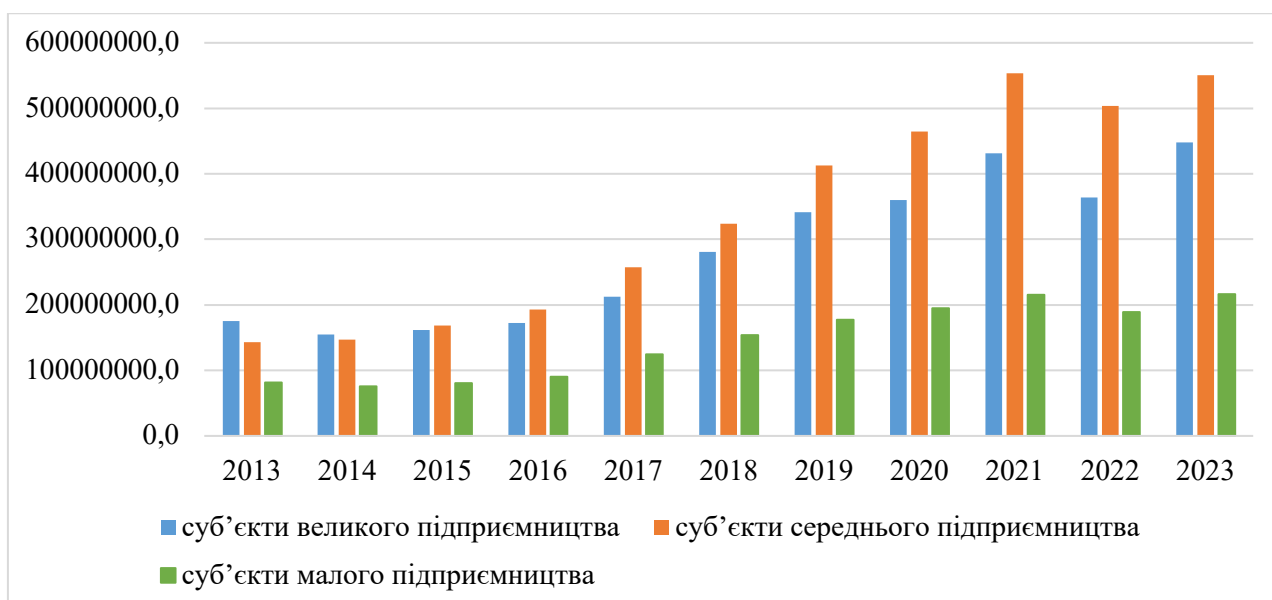


Рис. 2.4 Витрати на персонал суб'єктів великого, середнього та малого підприємництва за видами економічної діяльності у 2013-2023 роках.

Джерело: побудовано автором на основі [76, 77].

Протягом 2013-2023 років витрати на персонал у суб'єктів підприємництва різного масштабу демонстрували суттєві відмінності, що відображає неоднорідність економічної активності за видами господарювання та рівнем фінансової спроможності підприємств. Загальна динаміка засвідчує, що найбільші обсяги витрат на персонал традиційно припадають на великі підприємства, що зумовлено їхньою більшою чисельністю персоналу, вищим рівнем оплати праці, соціальними гарантіями та стабільнішими умовами зайнятості. Середні підприємства демонструють помірну, але поступову динаміку зростання витрат на персонал, що свідчить про їхню адаптацію до вимог ринку праці, підвищення кваліфікаційних вимог до працівників та впровадження елементів корпоративної культури. Крім того, малі підприємства характеризуються більш стриманими темпами приросту таких витрат, що пов'язано з їхньою обмеженою фінансовою базою, високою залежністю від зовнішніх чинників і частою орієнтацією на самозайнятість або неформальні трудові відносини.

Розподіл витрат на персонал за видами економічної діяльності також вказує на домінування галузей із високою часткою людських ресурсів – таких як

промисловість, торгівля, транспорт і послуги. У цих секторах витрати великих підприємств значно перевищують аналогічні показники малого і середнього бізнесу, що свідчить про масштабність операцій та системність кадрової політики. Зростання витрат у період після 2020 року частково зумовлене інфляційними процесами, змінами у законодавстві щодо оплати праці та адаптацією до нових реалій, спричинених пандемією COVID-19 та подальшою економічною нестабільністю [90]. Також цифровізація, зокрема автоматизація обліку заробітної плати, кадрового менеджменту та використання хмарних сервісів, стала важливим інструментом оптимізації витрат на персонал для МСП.

Таким чином, аналіз витрат на персонал суб'єктів великого, середнього та малого підприємництва за видами економічної діяльності у 2013-2023 роках свідчить про суттєву диференціацію в кадровій політиці та фінансових можливостях різних форм бізнесу. Великі підприємства залишаються лідерами за обсягами витрат, що пояснюється масштабом діяльності, розгалуженими структурами управління та високими соціальними стандартами [91]. Середні підприємства демонструють стабільне зростання витрат, що вказує на їхню поступову інтеграцію до сучасних практик управління персоналом. Проте, малі підприємства залишаються вразливими до економічних коливань, що обмежує їхню здатність інвестувати у трудові ресурси. Розвиток цифрових технологій створює умови для оптимізації витрат і підвищення ефективності управління персоналом навіть у малому бізнесі. У цілому, динаміка витрат на персонал відображає економічний стан підприємств та рівень їх цифрової трансформації та адаптації до сучасних вимог ринку праці.

Обсяг виробленої продукції є важливим показником економічної активності підприємницького сектора (рис. 2.5). Зокрема важливим є цей показник, в умовах трансформації економіки України, посиленої зовнішніми викликами, такими як пандемія, повномасштабна війна та зміна на світових ринках [92]. Такий підхід, дозволяє оцінити внесок кожної групи підприємств та виявити потенціал до стійкого розвитку, інноваційної активності, цифрової трансформації та забезпечення інформаційної безпеки. Співставлення обсягів

виробництва у часовому та галузевому вимірі сприяє формуванню обґрунтованих управлінських рішень щодо забезпечення інформаційної безпеки зокрема та підтримки підприємництва загалом.

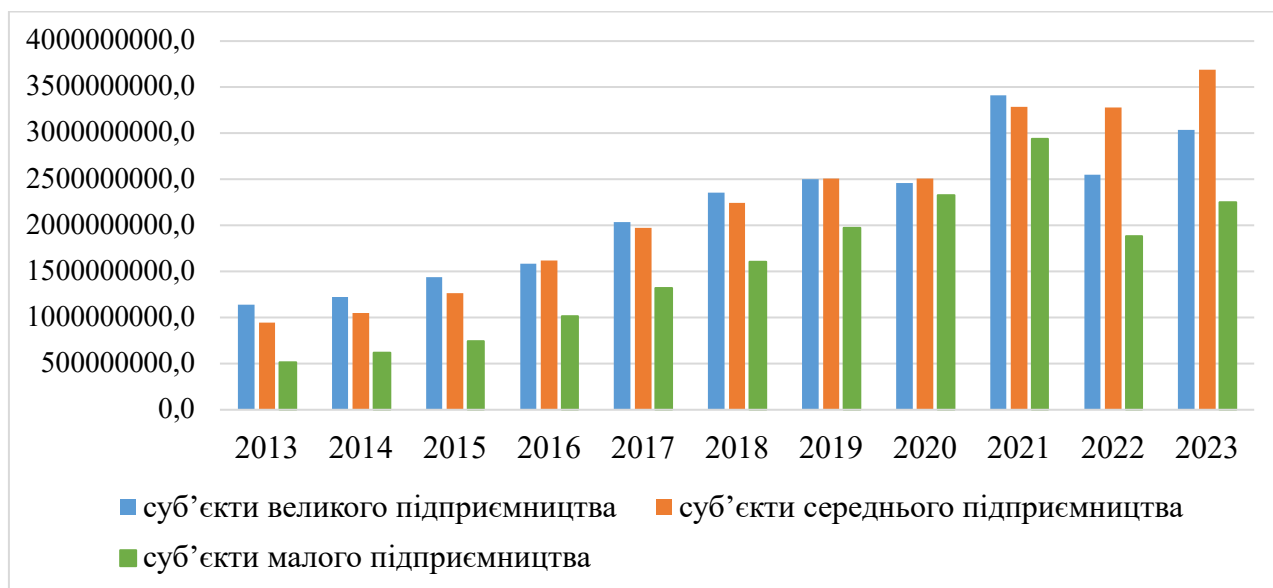


Рис. 2.5 Обсяг виробленої продукції (товарів, послуг) суб'єктів підприємництва за видами економічної діяльності у 2013-2023 роках.

Джерело: побудовано автором на основі [76, 77].

Протягом 2013-2023 років структура обсягу виробленої продукції (товарів і послуг) суб'єктами підприємництва демонструє відчутну асиметрію, що відображає різний рівень ресурсного забезпечення, доступу до інфраструктури, ринкової сили та інноваційного потенціалу підприємств різних масштабів. Як свідчать дані, переважну частину продукції в абсолютному вимірі стабільно формують великі підприємства. Їхня домінуюча позиція пояснюється значними виробничими потужностями, диверсифікацією видів діяльності, високою капіталізацією та налагодженими ланцюгами поставок. Середні підприємства посідають проміжне положення, забезпечуючи значний, але помітно менший обсяг продукції порівняно з великим бізнесом. Вони демонструють поступове зростання обсягів виробництва, що свідчить про адаптивність до ринкових змін, здатність до технологічного оновлення та гнучкі стратегії розвитку. Цей сегмент є важливим для розширення внутрішнього ринку та забезпечення регіонального економічного зростання.

Малі підприємства, незважаючи на чисельну перевагу серед суб'єктів господарювання, генерують найменший обсяг продукції, що зумовлено як обмеженими фінансовими та виробничими ресурсами, так і специфікою діяльності, орієнтованої переважно на локальні ринки та послуги. Разом із тим, у низці сфер, зокрема в сфері ІТ, креативних індустрій і торгівлі, малі підприємства демонструють зростання за рахунок цифровізації, розвитку електронної комерції, нішевої спеціалізації та достатньої інформаційної безпеки.

Період з 2020 року ознаменувався сповільненням темпів зростання обсягу виробництва через вплив пандемії COVID-19, деструкцію логістичних ланцюгів і коливання попиту. Крім того, з 2022 року почали проявлятися нові виклики, пов'язані з війною, які суттєво вдарили по великому виробництву в окремих галузях, що дало можливість деяким малим і середнім підприємствам проявити гнучкість, оперативно адаптуватися до нових умов, переорієнтуватися на внутрішній ринок або цифрові формати діяльності.

Таким чином, аналіз обсягу виробленої продукції (товарів, послуг) суб'єктами підприємництва у 2013-2023 роках засвідчив домінування великих підприємств у національній виробничій структурі, що обумовлено їх масштабністю, ресурсною базою та стабільними виробничими процесами. Крім того, зростання ролі середнього і частково малого бізнесу у формуванні обсягів продукції свідчить про підвищення їх адаптивності до викликів, орієнтацію на нові ринки та впровадження цифрових інструментів [93]. Особливо важливою стала роль МСП у кризові періоди, коли їх гнучкість і здатність до швидкої трансформації виявилися необхідними. Таким чином, структура виробництва поступово змінюється в бік диверсифікації, що створює передумови для стійкішого розвитку економіки за умови належної державної підтримки цифрової модернізації малого і середнього бізнесу.

З огляду на розвиток малого, середнього та великого підприємництва в Україні, показник кількості відпрацьованих годин найманими працівниками дає змогу оцінити масштаби залучення робочої сили, стабільність функціонування суб'єктів господарювання та їхню спроможність реагувати на зовнішні виклики

(рис. 2.6). Особливо актуальний такий аналіз, зважаючи на події останніх років, що охоплює періоди соціально-економічних потрясінь, пандемії COVID-19, а також повномасштабної війни росії проти України. У таких умовах кількість відпрацьованих годин виступає статистичним показником та маркером стійкості бізнесу, рівня цифровізації процесів, трансформації моделей зайнятості та рівня інформаційної безпеки.

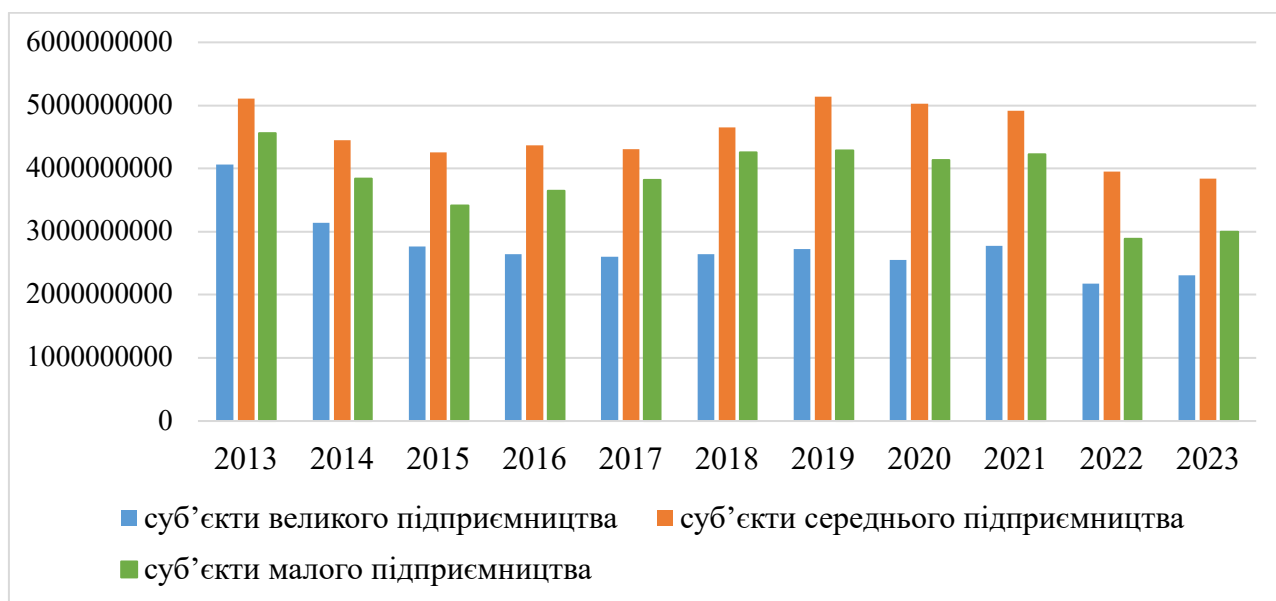


Рис. 2.6. Кількість відпрацьованих годин найманими працівниками суб'єктами підприємництва за видами економічної діяльності у 2013-2023 роках.

Джерело: побудовано автором на основі [76, 77].

За аналізований період спостерігається закономірна перевага великих підприємств за обсягом відпрацьованих годин, що зумовлено значною кількістю найманого персоналу, повною зайнятістю та стабільністю виробничих циклів, що підтверджує їх провідну роль у формуванні офіційного ринку праці. Середні підприємства демонструють більш помірні показники, однак відзначаються стабільністю, що свідчить про їх адаптивність до економічних викликів та збереження робочих місць навіть в умовах кризи. Крім того, малі підприємства характеризуються нижчим рівнем загальної кількості відпрацьованих годин, що відображає менший масштаб операцій, часткову зайнятість працівників та ширше використання гнучких або неформальних форм праці.

Значні коливання в структурі відпрацьованих годин спостерігаються у 2014-2015 та 2022-2023 роках – періоди, пов’язані з геополітичною нестабільністю та воєнною агресією росії, що призвели до зниження зайнятості, скорочення тривалості робочого часу або повного припинення діяльності окремих суб’єктів господарювання. Крім того, пандемія COVID-19 у 2020-2021 роках суттєво вплинула на сектор послуг та торгівлі, що спричинило гнучкий перерозподіл трудових ресурсів. Цифровізація бізнес-процесів, впровадження дистанційної праці та автоматизація окремих функцій призвели до зміни структури трудової участі [94]. Особливо це помітно в малому та середньому бізнесі, де ІТ-рішення дозволили оптимізувати навантаження на персонал без суттєвого зменшення ефективності праці.

Таким чином, кількість відпрацьованих годин є чутливим індикатором соціально-економічної ситуації, рівня цифрової трансформації бізнесу та рівня інформаційної безпеки. Визначальну роль у забезпеченні зайнятості стабільно відіграють великі підприємства, які генерують найбільший обсяг відпрацьованого часу завдяки масштабності та стабільності виробничих процесів. Середній бізнес демонструє адаптивність і стійкість, тоді як малий – більшу гнучкість, проте вразливість до економічних шоків. Пандемія, війна та цифрова трансформація помітно вплинули на динаміку трудової участі, стимулюючи розвиток дистанційної праці, гнучких графіків і нових форматів зайнятості.

Додана вартість є важливим показником, що характеризує економічну ефективність підприємницької діяльності та рівень її внеску у валовий внутрішній продукт країни (рис. 2.7) та дозволяє оцінити реальну цінність, створену в процесі виробництва, служить індикатором продуктивності, інноваційності та конкурентоспроможності бізнесу. Дослідження динаміки зазначених показників, дозволяє простежити трансформаційні процеси в економіці України, визначити сфери з високою доданою вартістю та виявити роль цифровізації у зростанні продуктивності різних форм бізнесу.

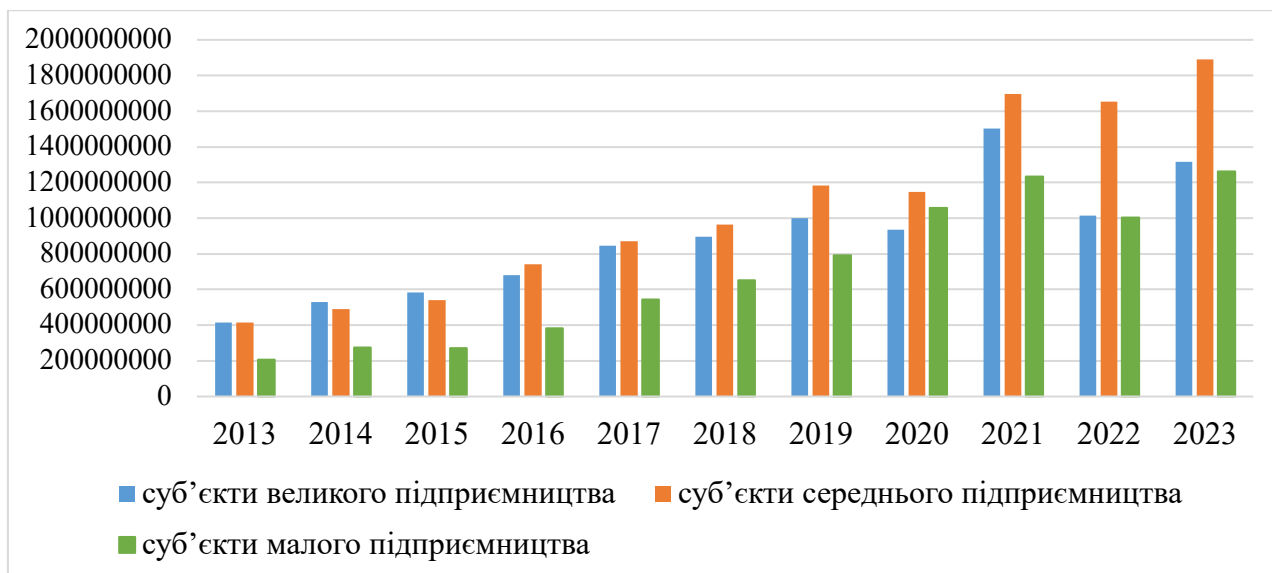


Рис. 2.7 Додана вартість за витратами виробництва суб'єктів підприємництва за видами економічної діяльності у 2013-2023 роках.

Джерело: побудовано автором на основі [76, 77].

У динаміці за 2013-2023 роки спостерігається чітка диференціація між великими, середніми та малими суб'єктами підприємництва за обсягами створеної доданої вартості. Великі підприємства традиційно забезпечують найбільшу частку доданої вартості у загальному обсязі, що зумовлено значними обсягами виробництва, високою капіталоємністю, а також широкою участю у зовнішньоекономічній діяльності. Їх продукція має вищу частку переробленої вартості, що свідчить про глибшу технологічну переробку, вищу кваліфікацію персоналу та активне впровадження інновацій. Середні підприємства демонструють стійке, хоча й дещо обмежене зростання обсягів доданої вартості. Їх внесок особливо важливий у секторах, що забезпечують внутрішній ринок – будівництві, переробній промисловості, транспорті та сфері послуг. Зазначений сегмент відіграє роль зв'язуючої ланки між великим капіталом і дрібним підприємництвом, поєднуючи гнучкість із поступовою цифровізацією виробництва.

Малі підприємства, попри свою чисельну перевагу, формують найменшу частку доданої вартості, що пояснюється меншими обсягами виробництва та нижчим рівнем інвестицій у технології, обмеженим доступом до кредитних

ресурсів і вузькою спеціалізацією. Проте в окремих секторах (зокрема у сфері послуг, ІТ, креативних індустріях) малі підприємства демонструють зростання обсягів доданої вартості завдяки цифровізації та високій інноваційній динаміці.

Таким чином, аналіз доданої вартості за витратами виробництва суб'єктів підприємництва у 2013-2023 роках свідчить про структурну нерівномірність у формуванні економічної цінності між різними формами господарювання. Великі підприємства стабільно генерують основну частину доданої вартості, що підтверджує їхню важливу роль у національній економіці. Крім того, середній бізнес демонструє позитивну динаміку зростання, зміцнюючи свої позиції в окремих секторах внутрішнього ринку. Найменший внесок забезпечують малі підприємства, проте їхня гнучкість, інноваційний потенціал і здатність до цифрової трансформації відкривають нові можливості для підвищення ефективності та участі у створенні доданої вартості. За умов цілеспрямованої державної підтримки та розвитку цифрової інфраструктури, МСП можуть стати катализатором стійкого економічного зростання в регіонах України [95].

Зайнятість населення є одним із важливих показників соціально-економічного розвитку територій та визначальним чинником добробуту громадян (рис 2.8). У структурі національної економіки підприємницький сектор, великий, середній і малий, відіграє провідну роль у створенні робочих місць, формуванні ринку праці та забезпеченні динаміки трудової мобільності. Аналіз кількості зайнятих працівників у підприємствах різного масштабу дозволяє виявити зміни у структурі зайнятості та особливості реагування бізнесу на зовнішні виклики – економічну кризу, пандемію COVID-19, повномасштабну війну, а також на процеси цифрової трансформації [96]. Вивчення динаміки цього показника є важливим для розуміння ролі кожної категорії підприємств у формуванні трудового потенціалу країни та визначення напрямів подальшого розвитку політики зайнятості в умовах нестабільного середовища.

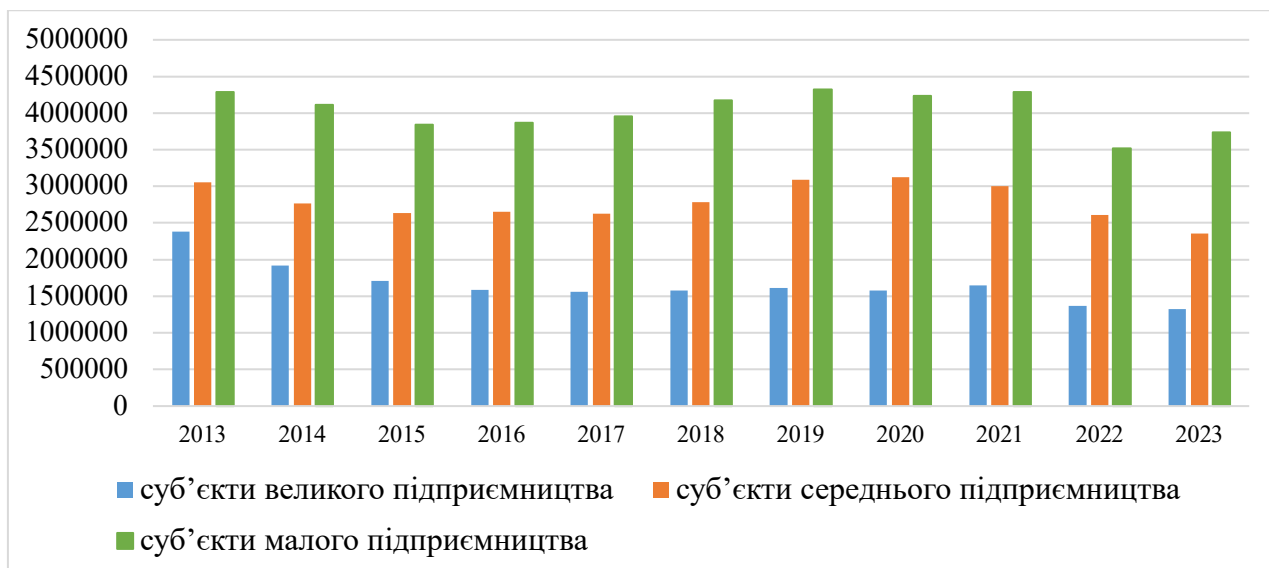


Рис. 2.8 Кількість зайнятих працівників у суб'єктів великого, середнього та малого підприємництва за видами економічної діяльності у 2013-2023 роках.

Джерело: побудовано автором на основі [76, 77].

Протягом 2013-2023 років кількість зайнятих працівників у суб'єктів великого, середнього та малого підприємництва демонструє динаміку, яка відображає структурні зрушення на ринку праці, трансформації у сфері зайнятості та адаптацію бізнесу до кризових умов. Як свідчать дані, найбільшу кількість зайнятих стабільно забезпечують великі підприємства. Їхній значний кадровий потенціал пояснюється масштабістю виробництва, необхідністю обслуговування складних організаційних структур, а також стабільністю зайнятості в умовах розвиненої системи трудових гарантій. Середні підприємства демонструють відносну стабільність показників зайнятості, а в окремі роки навіть зростання, що свідчить про їхню адаптивність, здатність до збереження трудових ресурсів та ефективне управління персоналом. Цей сегмент виконує важливу функцію підтримки регіонального ринку праці, особливо у виробничо-сервісних секторах.

Малі підприємства, попри свою чисельну перевагу в структурі суб'єктів господарювання, забезпечують найменшу кількість зайнятих, що пов'язано як з обмеженістю масштабів їх діяльності, так і з широким використанням самозайнятості, гнучких форм праці та часткової зайнятості. Також у ряді сфер,

таких як сервіс, ІТ, роздрібна торгівля, малий бізнес демонструє тенденцію до зростання кількості працівників, що зумовлено розвитком цифрової економіки, електронної комерції та відносною мобільністю цього сектору.

Періоди економічної нестабільності, зокрема 2014-2015, 2020-2021 та 2022-2023 роки, мали суттєвий вплив на рівень зайнятості у всіх категоріях підприємств. Особливо вразливими виявилися малі підприємства, тоді як великі мали більше ресурсів для збереження персоналу. Цифровізація бізнесу, автоматизація процесів та розвиток дистанційних форм зайнятості сприяли частковій стабілізації трудового ринку в умовах кризи.

Таким чином, аналіз кількості зайнятих працівників у суб'єктів великого, середнього та малого підприємництва за видами економічної діяльності у 2013-2023 роках свідчить про стійку домінантну роль великих підприємств у забезпеченні формальної зайнятості. Також середній бізнес демонструє стабільність і гнучкість у реагуванні на кризові виклики, зберігаючи робочі місця та поступово нарощуючи кадровий потенціал. Малі підприємства, хоч і менш чисельні за показником зайнятості, залишаються важливим джерелом гнучких форм праці, самозайнятості та трудової мобільності, особливо в галузях, де цифрові технології відіграють провідну роль. Зміни у структурі зайнятості, зумовлені зовнішніми кризами та внутрішніми реформами, засвідчують потребу в адаптивній політиці підтримки зайнятості з урахуванням масштабу та специфіки підприємницької діяльності [97].

Мале підприємництво відіграє важливу роль у структурі національної економіки, забезпечуючи створення робочих місць, стимулювання конкуренції, розвиток регіонів і формування середовища для інновацій. Динаміка кількості діючих суб'єктів малого бізнесу є індикатором економічної активності та адаптивності підприємницького середовища до зовнішніх викликів, політичних, соціальних, фінансових (рис. 2.9). Важливим є аналіз зазначених показників в довгостроковій ретроспективі, що охоплює періоди глибоких криз та паралельного розвитку цифрової інфраструктури.

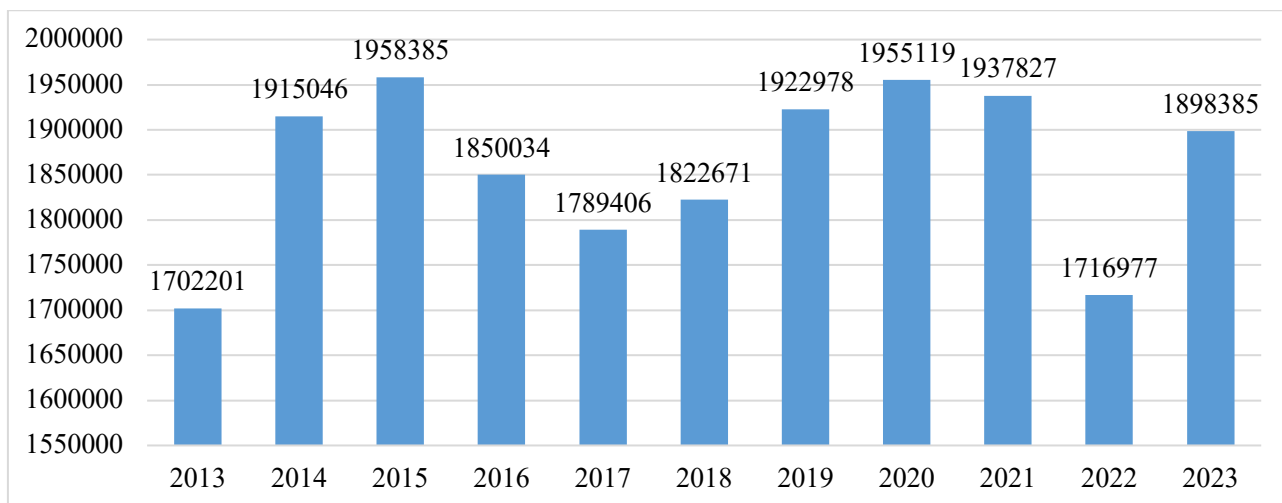


Рис. 2.9 Кількість діючих суб'єктів малого підприємництва за видами економічної діяльності у 2013-2023 роках.

Джерело: побудовано автором на основі [76, 77].

Протягом 2013-2023 років динаміка кількості діючих суб'єктів малого підприємництва в Україні відображає як загальноекономічні тенденції, так і галузеві трансформації в умовах постійної адаптації до внутрішніх і зовнішніх викликів. Динаміка засвідчує значні коливання у кількості малих підприємств, які безпосередньо корелюють із фазами економічної нестабільності, зокрема з подіями 2014-2015 років, пандемією COVID-19 у 2020-2021 роках та повномасштабною війною, що розпочалася у 2022 році.

Найбільше зменшення кількості малих підприємств фіксується у періоди глибоких криз, що зумовлено зниженням купівельної спроможності населення, перебоями у логістиці, зростанням вартості ресурсів та загальним зниженням економічної активності. Також, спостерігається і зворотна тенденція, відновлення активності малого бізнесу в міжкризові роки, що свідчить про його високу гнучкість, швидке пристосування до нових умов ведення господарської діяльності та спроможність ефективно використовувати цифрові інструменти.

За видами економічної діяльності помітне лідерство секторів роздрібної торгівлі, послуг та харчування, де малі підприємства мають найвищу концентрацію. Зазначені сфери характеризуються відносно невеликими стартовими інвестиціями, коротким циклом окупності та високою адаптивністю до споживчих трендів. У той час як у промисловості, сільському господарстві та

будівництві спостерігається більш стримана динаміка зростання кількості суб'єктів малого бізнесу, що зумовлено високими бар'єрами входу, капіталомісткістю та залежністю від інфраструктурних умов [81].

Цифровізація, розвиток електронної комерції, платіжних систем, CRM-рішень і державних онлайн-сервісів (зокрема «Дія») сприяли зростанню кількості зареєстрованих малих підприємств у сферах, орієнтованих на технології та дистанційне обслуговування, що вказує на зміну структурних пріоритетів у малому підприємстві на користь інноваційних і менш затратних за ресурсами моделей бізнесу.

Отже, аналіз кількості діючих суб'єктів малого підприємництва за видами економічної діяльності у 2013-2023 роках виявив високий рівень чутливості цього сегмента до зовнішніх економічних і соціальних потрясінь, а також його здатність до швидкої адаптації. Незважаючи на скорочення кількості малих підприємств у періоди криз, спостерігається стійка тенденція до відновлення та зростання в міжкризові роки, що свідчить про гнучкість бізнес-моделей та здатність підприємців оперативно реагувати на зміну умов. Лідируючі позиції малих підприємств у торгівлі, послугах і харчуванні зумовлені їх меншою капіталоемністю та швидшою окупністю. Крім того, цифровізація виступає вагомим чинником стимулювання розвитку малого бізнесу, відкриваючи нові можливості для реєстрації, обліку, обслуговування споживачів та просування продукції. Підтримка малого підприємництва через цифрові інструменти та цільові державні програми є важливою умовою формування стійкої, інклюзивної економіки в Україні [98].

Мале підприємництво є фундаментальним елементом сучасної економіки, що забезпечує динамічний розвиток регіонів, створення робочих місць, формування конкурентного середовища та впровадження інновацій. У контексті численних внутрішніх і зовнішніх викликів, які пережила Україна протягом 2013-2023 років, саме малий бізнес продемонстрував здатність до гнучкого реагування на зміни та збереження економічної активності навіть у найскладніших умовах. Аналіз основних показників діяльності суб'єктів малого

підприємництва, таких як кількість підприємств, обсяги реалізованої продукції, рівень зайнятості, витрати на персонал та створення доданої вартості, дозволяє комплексно оцінити їхній стан, виклики та перспективи розвитку (рис. 2.10).

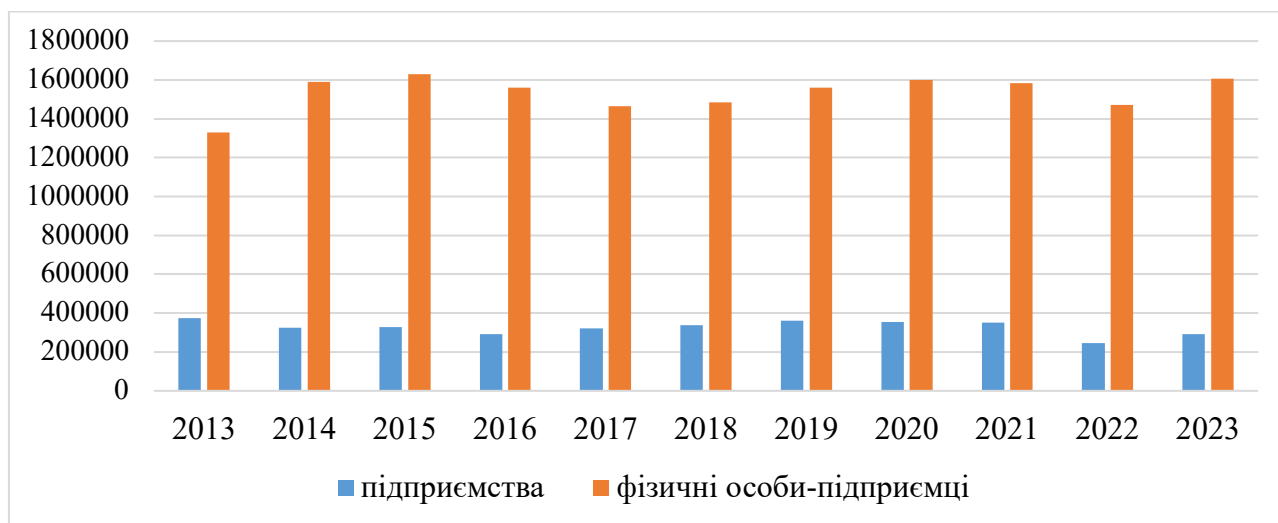


Рис. 2.10 Показники діяльності суб'єктів малого підприємництва у 2013-2023 роках.

Джерело: побудовано автором на основі [76-77].

Показники діяльності суб'єктів малого підприємництва за 2013-2023 роки відображають еволюцію цього сектору в умовах глибоких соціально-економічних змін та переходу до цифрової економіки. Загальна динаміка основних індикаторів – кількості підприємств, обсягів реалізованої продукції (товарів, послуг), доданої вартості, витрат на персонал та чисельності зайнятих, засвідчує високий рівень чутливості малого бізнесу до кризових явищ і, його здатність до оперативного відновлення.

У 2014-2015 роках на фоні політичної нестабільності та економічного спаду спостерігається зниження більшості показників діяльності. Подібна ситуація повторюється у 2020-2021 роках внаслідок пандемії COVID-19, яка особливо вдарила по секторах торгівлі, громадського харчування та послуг. Найбільш критичним виявився період 2022-2023 років, коли у зв'язку з повномасштабною війною частина малих підприємств припинила діяльність, зменшилися обсяги реалізації та зросли витрати на забезпечення базових операційних потреб.

Разом з тим, динаміка демонструє, що після кожного спаду спостерігається тенденція до відновлення, особливо у сферах, де активно впроваджуються цифрові технології, електронна комерція та дистанційні форми взаємодії з клієнтами. Обсяг доданої вартості та кількість зайнятих у малому бізнесі зростають у міжкризові періоди, що свідчить про накопичення підприємницького досвіду, пошук нових моделей ведення бізнесу та поступову модернізацію. Цифровізація стала важливим чинником підтримки життєздатності малого підприємництва. Онлайн-платформи, електронні сервіси державного управління, автоматизовані CRM-системи та платіжні рішення дали змогу значній частині підприємств продовжити роботу навіть в умовах фізичних обмежень або переміщення бізнесу. Аналіз показників діяльності малого підприємництва у 2013-2023 роках свідчить про наявність як вразливих місць (низька капіталізація, залежність від попиту, обмеженість ринків), так і сильних сторін (гнучкість, адаптивність, цифрова трансформація), які визначають потенціал цього сектору як основи для розвитку сталого, інноваційного економічного середовища.

Аналіз показників діяльності суб'єктів малого підприємництва у 2013-2023 роках засвідчив, що цей сектор є чутливим до зовнішніх економічних шоків і надзвичайно адаптивним до змін. У періоди криз, зокрема під час політичної нестабільності, пандемії та воєнного стану, малі підприємства зазнавали скорочення обсягів виробництва, зменшення кількості зайнятих та обмеження фінансових ресурсів. Проте в міжкризові роки вони демонстрували відновлення, використовуючи переваги гнучкості, локальної орієнтації, інноваційності та цифровізації бізнес-процесів. Розвиток цифрових інструментів став одним із основних чинників підтримки життєздатності малих підприємств, дозволивши їм зберегти економічну активність і підвищити ефективність [99].

Значним кроком на шляху до забезпечення інформаційної безпеки суб'єктів підприємництва та впровадження цифрових технологій у малий і середній бізнес стала міжнародна ініціатива «Digital for SMEs (D4SME)» [100], заснована 2018 року за участю країн-членів ОЕСР. Основна метою цієї ініціативи

є підтримка урядів, бізнес-структур та відповідних інституцій у створенні партнерських зв'язків, обміні досвідом, знаннями та цифровими компетенціями з метою сприяння активній і результативній цифровій трансформації малого та середнього бізнесу. Такий підхід сприяє формуванню дієвих політик, стимулюванню інноваційних процесів і підвищенню технологічної спроможності підприємств в умовах глобальних змін.

Стан інформаційної безпеки українських суб'єктів малого підприємництва значно відрізняється від глобальних тенденцій, що обумовлено низкою деструктивних чинників (недостатній рівень цифрової обізнаності суб'єктів господарювання та споживачів). У зв'язку з цим застосування європейської методики оцінювання індексу цифрової інтенсивності з усталеними показниками не завжди є релевантним для українських умов. Україна часто відсутня у провідних міжнародних рейтингах цифрового розвитку, що ускладнює об'єктивне розуміння змін, які відбуваються в національній цифровій інфраструктурі, та визначення її місця у глобальному цифровому просторі.

Відсутність належно сформованого інформаційного середовища для бізнесу, сьогодні є значною проблемою. спостерігається дефіцит чітких стратегічних орієнтирів, дорожніх карт і практичних рекомендацій, які б сприяли поширенню знань про інформаційну безпеку, цифрові технології, їхні переваги та шляхи впровадження. Також, наявна система збору статистичних даних щодо інформаційної безпеки суб'єктів підприємництва та їх цифрової трансформації залишається обмеженою за охопленням і технічно застарілою. В Україні основним джерелом такої інформації сьогодні виступає Державна служба статистики, яка проводить моніторинг через уніфіковану форму № 1-ІКТ (річна) «Використання інформаційно-комунікаційних технологій на підприємствах» [101]. Проте, такий формат не забезпечує повного врахування особливостей і динаміки цифрового розвитку малого підприємництва, що значно звужує можливості аналітики для формування ефективних управлінських рішень щодо забезпечення інформаційної безпеки.

Відповідно до положень національної програми «Цифровізація для відновлення в Україні», у довгостроковій перспективі на період 2026-2032 років [102], передбачено якісну розбудову інфраструктури даних, що буде забезпечувати систематичне вимірювання цифрової економіки країни. Такий показник базується на основі зібраних статистичних показників суб'єктів господарювання. Зазначимо, що одним з важливих напрямів є інтеграція України до європейської методології The Digital Economy and Society Index [103]. Такий підхід дозволить отримати доступ до єдиної бази цифрових даних ЄС. Проте, незважаючи на перспективність зазначених дій, вже сьогодні доцільно здійснювати аналіз та оцінку локальних процесів забезпечення інформаційної безпеки суб'єктів підприємництва, адаптуючи принципи DESI на мікрорівень із подальшим масштабуванням.

Враховуючи важливість інформаційної безпеки суб'єктів, саме малого підприємництва та доцільність цифрового розвитку для економічного відновлення, у червні 2023 року. Організація економічного співробітництва та розвитку спільно з Урядом України ініціювали чотирирічну програму [104], спрямовану на підтримку майбутніх реформ, а також процесів модернізації та повоєнної відбудови, а також наближення України до членства в ЄС та ОЕСР. Відповідно до цієї програми передбачено вдосконалення державної політики щодо МСП за дванадцятьма тематичними напрямками, передбачених актом про малий бізнес для Європи (SBA).

Зазначимо, що ОЕСР сьогодні тісно співпрацює з Україною у сфері цифрової трансформації МСП, що передбачає посилення потенціалу інституційної підтримки бізнесу, створення інструментів для діагностики цифрової досконалості підприємств, а також розробку механізмів просування цифрових навичок та формування цифрової культури серед керівників МСП і фізичних осіб-підприємців. Такий підхід спрямований на підвищення спроможності українських малих та середніх підприємств до інтеграції в цифрову економіку Європи.

У цьому контексті важливим кроком стало ухвалення ЄС у березні 2022 року Закону про цифрові ринки (DMA) [105], що є частиною ширшої стратегії підтримки цифрового розвитку. Закон покликаний регламентувати діяльність великих цифрових платформ, так званих «вартових», з метою забезпечення рівних умов конкуренції та створення відкритого, прозорого та справедливого цифрового ринку в межах ЄС. Такий нормативний підхід є зразком для країн-кандидатів, зокрема України, які прагнуть гармонізувати свою цифрову політику з європейськими стандартами.

Зазначимо, що у квітні 2022 року було досягнуто ще одного важливого кроку в сфері цифрового регулювання – укладено угоду щодо впровадження Закону про цифрові послуги [106], який став першим у світі комплексним нормативно-правовим документом, що регламентує діяльність онлайн-середовища. Цей закон ґрунтується на основному принципі, усе що є незаконним у реальному (офлайн) середовищі, має залишатися незаконним і в цифровому (онлайн) просторі. Згідно з положеннями DSA, онлайн-платформи та пошукові системи зобов'язані вживати заходів для захисту користувачів від незаконного контенту, небезпечних товарів і послуг, що розповсюджуються в Інтернеті. Крім того, на ці платформи покладається обов'язок проводити систематичну оцінку ризиків, які можуть виникати внаслідок функціонування їхніх алгоритмів – зокрема у контексті захисту основоположних прав людини, безпеки дітей та підтримання якісного публічного діалогу. Як і закон про цифрові ринки, DSA набув чинності у 2022 році та офіційно почав застосовуватись з 2023 року. У сукупності ці два нормативні акти формують основу нового цифрового правового поля в ЄС, спрямованого на забезпечення прозорості, відповідальності та справедливості у сфері цифрових послуг.

Сучасні цифрові технології відкривають суб'єктам малого підприємництва нові можливості для виходу за межі локальних ринків, сприяючи їхній експансії на національному та міжнародному рівнях, що особливо актуально для країн ЄС, де функціонує єдиний внутрішній ринок, що полегшує доступ до нових партнерів і споживачів. Завдяки онлайн-платформам, інструментам електронної

комерції та цифрового маркетингу, малі та середні підприємства отримують змогу активніше долучатися до глобальних торговельних процесів і розширювати базу споживачів [107]. Крім того, цифрові технології сприяють впровадженню інноваційних рішень, що є важливим для підвищення адаптивності, конкурентоспроможності та сталого розвитку МСП в умовах динамічного економічного середовища.

Аналіз стану інформаційної безпеки суб'єктів малого підприємництва в Україні засвідчує значну кількість загроз, пов'язаних із активним поширенням цифрових технологій та недостатнім рівнем захищеності інформаційних систем. У сучасних умовах господарювання малі підприємства дедалі частіше стають об'єктами кібератак, несанкціонованого доступу до даних, фішингових схем, зараження шкідливим програмним забезпеченням та інших форм інформаційного впливу. Як засвідчив проведений аналіз, вразливість таких суб'єктів пояснюється обмеженими фінансовими можливостями, відсутністю спеціалізованих підрозділів із кіберзахисту та недостатнім рівнем обізнаності персоналу щодо правил інформаційної безпеки. Значною проблемою є також використання застарілого програмного забезпечення та ненадійних технічних рішень, що підвищує ризик витоку конфіденційної інформації та втрати важливих даних. Значна кількість суб'єктів малого підприємництва не мають чітко визначених політик інформаційної безпеки, систем резервного копіювання даних та механізмів оперативного реагування на кіберінциденти. Унаслідок цього навіть незначні порушення можуть призводити до серйозних фінансових збитків, зупинки бізнес-процесів і погіршення репутації підприємства.

Порушення інформаційної безпеки може спричиняти значні фінансові втрати, негативно впливати на репутацію підприємства, знижувати рівень довіри з боку споживачів, а також ускладнювати подальший розвиток бізнесу. У зв'язку з цим, доцільним є визначення основних проблем, характерних проявів порушення інформаційної безпеки та їх наслідки для суб'єктів малого підприємництва, що представлено на рис. 2.11.

Можливі ризики порушення інформаційної безпеки суб'єктами малого підприємництва та їх наслідки систематизовано на рис. 2.11.

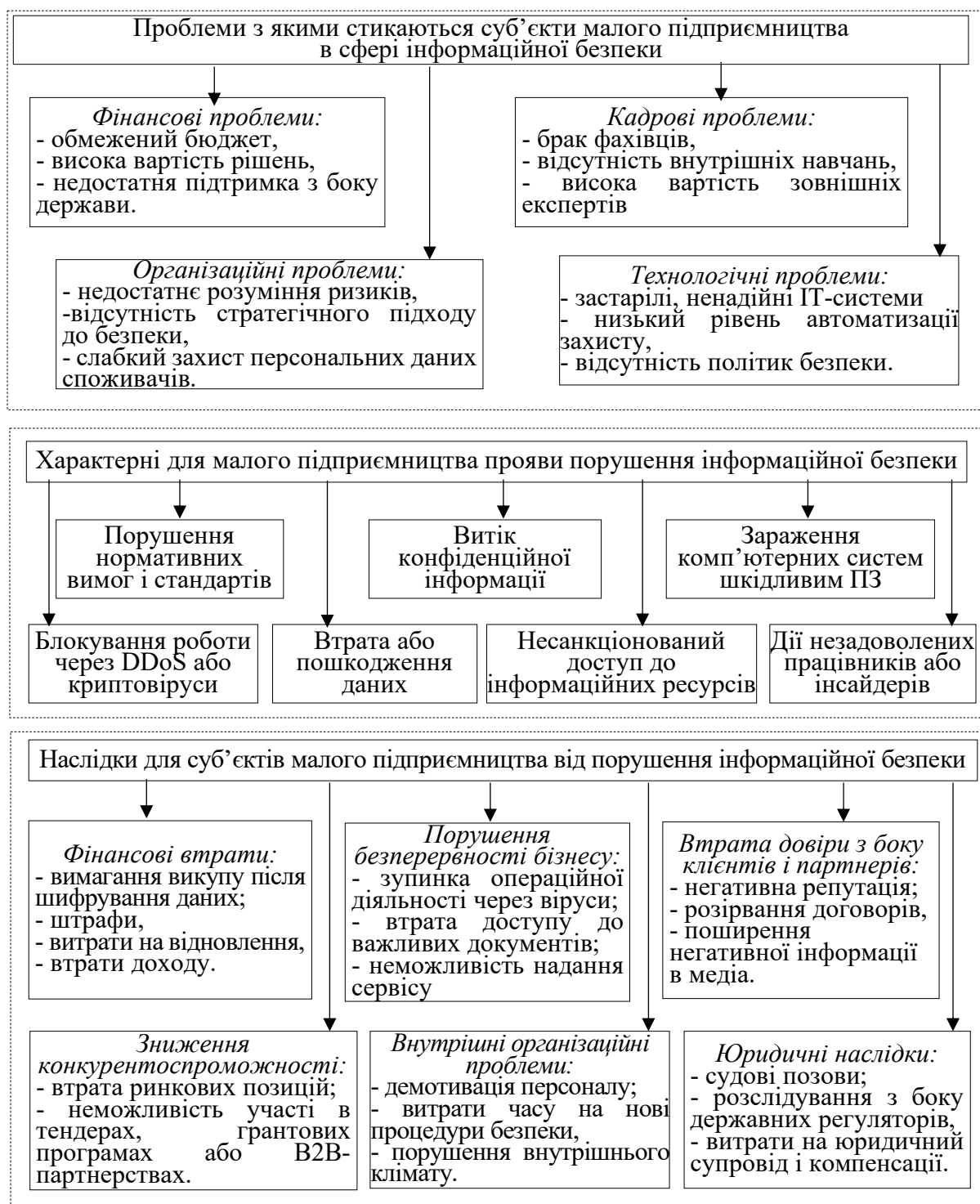


Рис. 2.11. Можливі ризики порушення інформаційної безпеки суб'єктами малого підприємництва та їх наслідки.

Джерело: розроблено автором.

Суб'єкти малого підприємництва у процесі здійснення господарської діяльності дедалі частіше стикаються з ризиками порушення інформаційної безпеки, що обумовлено активною цифровізацією бізнес-процесів, використанням електронного документообігу та залежністю від інформаційно-комунікаційних технологій. Основними проблемами у сфері інформаційної безпеки для малого бізнесу є фінансові, кадрові, організаційні та технологічні обмеження. Недостатній рівень фінансового забезпечення унеможливорює впровадження сучасних систем захисту інформації, а висока вартість спеціалізованих рішень та нестача державної підтримки значно ускладнюють процес формування ефективної системи кіберзахисту [108].

Вираженим деструктивним чинником підвищення вразливості суб'єктів малого підприємництва є кадрові проблеми, що проявляються у нестачі кваліфікованих фахівців з інформаційної безпеки, відсутності внутрішніх програм навчання персоналу та високій вартості зовнішніх експертних послуг. Також, значна кількість підприємств не приділяє належної уваги формуванню стратегічного підходу до управління інформаційною безпекою, що супроводжується недостатнім розумінням інформаційних ризиків, відсутністю внутрішніх політик безпеки та слабким захистом персональних даних споживачів. Технологічні проблеми також залишаються актуальними, оскільки багато підприємств використовують застарілі та ненадійні ІТ-системи з низьким рівнем автоматизації захисних механізмів.

Крім того, характерними проявами порушення інформаційної безпеки у сфері малого підприємництва є несанкціонований доступ до інформаційних ресурсів, витік конфіденційної інформації, зараження комп'ютерних систем шкідливим програмним забезпеченням, блокування роботи підприємства через DDoS-атаки або криптовіруси, а також втрата чи пошкодження даних. Додаткову загрозу становлять дії незадоволених працівників або інсайдерів, які можуть свідомо здійснювати витік інформації чи порушувати функціонування інформаційної системи підприємства. Такі ризики призводять до порушення нормативних вимог і стандартів у сфері захисту інформації.

Наслідки порушення інформаційної безпеки для суб'єктів малого підприємництва можуть мати комплексний характер та суттєво впливати на результати господарської діяльності, що проявляється у фінансових втратах, пов'язаних із необхідністю сплати штрафів, витратами на відновлення інформаційних систем, втратою доходів та можливими вимогами викупу після шифрування даних. Порушення безперервності бізнесу може спричинити зупинку операційної діяльності, втрату доступу до важливих документів та неможливість надання послуг споживачам. Крім того, у внутрішньому середовищі підприємства можуть виникати демотивація персоналу, порушення психологічного клімату та додаткові витрати часу на впровадження нових процедур безпеки. Також порушення інформаційної безпеки нерідко супроводжується юридичними наслідками у вигляді судових позовів, перевірок державних регуляторів і витрат на юридичний супровід та компенсаційні виплати.

Отже, сучасні умови функціонування суб'єктів малого підприємництва характеризуються зростанням кількості інформаційних загроз та підвищенням рівня залежності бізнес-процесів від цифрових технологій. Наявність фінансових, організаційних, кадрових і технологічних проблем значно ускладнює процес забезпечення належного рівня інформаційної безпеки та підвищує вразливість підприємств до кіберризиків. У результаті порушення інформаційної безпеки можуть виникати значні фінансові втрати, порушення безперервності діяльності, погіршення репутації та зниження конкурентоспроможності суб'єктів малого підприємництва.

За таких умов, доцільно провести комплексну оцінку рівня інформаційної безпеки підприємств, що дозволить визначити ступінь їх захищеності, виявити слабкі місця у системі інформаційного захисту та сформулювати ефективні напрями мінімізації ризиків.

2.3 Оцінка рівня інформаційної безпеки суб'єктів малого підприємництва

Суб'єкти малого підприємництва виступають рушійною силою економіки будь-якої країни, забезпечуючи гнучкість, інноваційність і створення робочих місць. В умовах стрімкого розвитку цифрових технологій та зростання ролі інформації як стратегічного ресурсу, інформаційне середовище стає визначальним чинником успішного функціонування бізнесу. Цифровізація відкриває нові можливості для підвищення ефективності управління інформаційною безпекою, оптимізації бізнес-процесів, розширення ринків збуту та посилення конкурентоспроможності підприємств. У цьому контексті особливої актуальності набуває аналіз поточного стану інформаційної безпеки та інформаційного середовища суб'єктів малого підприємництва. У реаліях повномасштабної війни забезпечення інформаційної безпеки суб'єктів підприємництва та їх цифрова трансформація набуває особливої ваги як важливий інструмент збереження їхньої життєздатності та адаптації до нових економічних викликів [109]. Цифрові рішення дозволяють бізнесу оперативно реагувати на зміни, забезпечувати достатній рівень інформаційної безпеки, виходити на нові ринки та підтримувати безпечну комунікацію зі споживачами в умовах нестабільності.

Для визначення рівня інформаційної безпеки суб'єктів малого підприємництва в дослідженні використано структурований підхід із залученням кількісного методу – опитування на основі розробленої анкети (Додаток Б1). Опитувальник охоплює основні аспекти організації системи інформаційної безпеки, зокрема: рівень фінансування інформаційної безпеки, наявність політик та процедур, кадрове забезпечення, використання технічних засобів захисту, частоту аудитів, рівень цифрової обізнаності персоналу, інцидент-менеджмент, резервне копіювання, застосування шифрування, взаємодії з постачальниками та готовність до інвестицій у забезпечення інформаційної безпеки.

Середньостатистична вибірка була сформована за методом повторного випадкового відбору, що дало змогу забезпечити репрезентативність даних у межах цільової сукупності малих підприємств. Перевага такого підходу полягає у забезпеченні статистичної стійкості результатів та можливості оцінки різних рівнів інформаційної безпеки за групами критеріїв. Аналіз результатів опитування дозволяє виявити найтипівіші практики та проблеми малого бізнесу в сфері інформаційної безпеки, зокрема: нерегулярне оновлення програмного забезпечення, недостатній рівень шифрування даних, обмежене резервне копіювання, відсутність тестованого плану реагування на інциденти, слабка інтеграція принципу найменших привілеїв, а також низький рівень готовності до впровадження багатофакторної автентифікації. Частина підприємств демонструє готовність до поступового збільшення інвестицій у кібербезпеку, що свідчить про зростання усвідомлення ризиків цифрового середовища. Узагальнення отриманих даних буде використано для побудови структурно-компонентної моделі формування системи інформаційної безпеки підприємства та формування відповідних рекомендацій щодо удосконалення політик безпеки, адаптованих до обмежених ресурсних можливостей малого бізнесу.

Важливим аспектом визначення достовірності результатів опитування є репрезентативність наявної вибірки, що характеризується розміром, структурою, рівнем відгуку, порівнянням вибірки із основною сукупністю. Для забезпечення достатнього рівня репрезентативності було здійснено попередній аналіз розподілу суб'єктів малого підприємництва Волинської області за видами діяльності, чисельністю персоналу та локалізацією. При формуванні вибірки враховувались основні статистичні параметри, що дозволяють мінімізувати похибки вибіркового спостереження. Структура вибірки забезпечила відображення основного сектору малого підприємництва Волинської області, яким є сервісний сектор, а саме: торгівля та послуги.

Розмір вибірки. Для точності дослідження та визначення розміру вибірки доцільно чітко знати обсяги генеральної сукупності. За даними Головного управління статистики у Волинській області, станом на кінець 2023 року на

території регіону діяло близько 4,8 тис. суб'єктів малого підприємництва [76]. Таким чином, для забезпечення базового рівня репрезентативності вибірка мала б становити щонайменше 10%, проте для дослідницьких цілей достатньо забезпечити охоплення, що дозволяє виявити типові характеристики і тенденції в межах цільової групи.

Структура вибірки відображає її репрезентативність, оскільки серед опитаних, саме суб'єкти малого підприємництва. Так, вибірка включала суб'єкти підприємництва Волинської області, які здійснюють діяльність у сферах виробництва, торгівлі та сервісу. Досліджувані суб'єкти підприємництва забезпечують різноманіття бізнес-моделей і цифрової зрілості. Врахування таких критеріїв дозволить зробити висновок про репрезентативність дослідження в межах малих типів виробничо-орієнтованих підприємств Волині.

Рівень відгуку – було розіслано 100 анкет. У нашому дослідженні, 20 підприємств надали повні відповіді, що відповідає рівню відгуку в 20%, що відповідає середньостатистичному рівню відгуку для анкетного опитування у сфері підприємництва, особливо в умовах обмеженого доступу до компаній, брак часу у респондентів і обмежена мотивація участі в дослідженнях. Це достовірний рівень опитування, оскільки він вищий нормативу, що складає 4,0%

Порівнянням вибірки із основною сукупністю об'єктів, стосується подібного розподілу, характеристики вибірки, подібності суб'єктів підприємництва у вибірці загальній структурі малого бізнесу Волинської області. Порівняльний аналіз соціально-економічних характеристик респондентів з даними Державної служби статистики України, відкритих даних в «Дія бізнес» та платформі «kompass.ua», підтвердив відповідність вибірки основним параметрам основної сукупності підприємств, зокрема за видом економічної діяльності та чисельністю працівників.

Репрезентативність наявної вибірки також доцільно обґрунтувати на основі довірчого інтервалу, який відображає, наскільки наявні результати можуть бути застосовані до усієї генеральної сукупності. Іншими словами, довірчий інтервал показує діапазон, у якому з високою ймовірністю знаходиться

справжнє значення для всієї групи підприємств малого бізнесу Волинської області.

Розрахунок довірчого інтервалу здійснюється за класичною формулою:

$$CI = p \pm Z \frac{\sqrt{p(1-p)}}{n} \quad (2.19),$$

де CI – довірчий інтервал, p – вибіркова частка, Z – критичне значення для відповідного рівня довіри, наприклад для 95% рівня довіри (1,96), n – розмір вибірки.

У нашому дослідженні, згідно з результатами опитування, 55% респондентів зазначили, що витрачають менше 10 000 грн на рік на забезпечення інформаційної безпеки. Таким чином, вибіркова частка становить $p = 0,55$, обсяг вибірки $n = 20$, а критичне значення $Z = 1,96$. Підставивши значення у формулу, отримаємо:

$$CI = 0,55 \pm 1,96 \frac{\sqrt{0,55(1-0,55)}}{20} = 33,2 - 76,8 \quad (2.20)$$

Отже, відповідно до розрахунків, довірчий інтервал становить від 33,2% до 76,8%, що означає: з ймовірністю 95%, реальна частка суб'єктів малого підприємництва, які витрачають менше 10 000 грн на рік на ІБ, перебуває в цьому діапазоні для всієї генеральної сукупності суб'єктів малого бізнесу Волинської області. Незважаючи на доволі широкий інтервал, це свідчить про домінування моделі мінімізації витрат на інформаційну безпеку у малому бізнесі. Враховуючи труднощі збору інформації в умовах війни росії проти України, така вибірка є максимально можливою в реалістичних умовах та може дати корисні результати і відобразити наявні тенденції щодо рівня інформаційної безпеки досліджуваних суб'єктів.

Таким чином, опитування проведено за допомогою технології «Google forms» (додаток Б1). В анкетуванні було визначено запитання щодо:

- фінансування інформаційної безпеки, включаючи обсяги річних витрат, готовність до збільшення інвестицій та наявність виділеного бюджету;

- оцінки завданих збитків внаслідок інформаційних атак за останні п'ять років;
- наявність політик та процедур інформаційної безпеки, включаючи формалізацію документації, частоту оновлення політик, наявність відповідальних осіб;
- практики проведення аудитів та перевірок, зокрема регулярність внутрішнього контролю інформаційної безпеки;
- рівня технічної оснащеності, включаючи використання фаєрволів, VPN, антивірусів, засобів шифрування та багатофакторної автентифікації;
- організації резервного копіювання та місце зберігання критичних даних;
- часу виявлення інцидентів, що дозволяє оцінити оперативність реагування на загрози;
- оновлення програмного забезпечення, як показник цифрової гігієни;
- оцінки постачальників та використання кіберстрахування;
- рівня обізнаності співробітників щодо фішингових атак, соціальної інженерії та дотримання принципу найменших привілеїв.

Анкети було розіслано у 100 суб'єктів малого підприємництва Волинської області, відповіді отримано 20 з них, інформація про які відображена у додатку Б2. Усі запитання мали чітку структуру, були як закритими так і напівзакритими (з варіантами відповідей), що забезпечило зручність обробки даних та стандартизованість аналітичних висновків. Зібрана інформація дозволяє діагностувати поточний стан інформаційної безпеки суб'єктів малого підприємництва та сформулювати підґрунтя для розробки практичних рекомендацій щодо її вдосконалення.

Проведений аналіз засвідчив, що незважаючи на зростаючу кількість кіберінцидентів, значна частина суб'єктів малого підприємництва не усвідомлює реального рівня ризиків або вважає інформаційну безпеку другорядним напрямом, що не потребує окремого бюджету. Як наслідок, витрати на інформаційну безпеку залишаються на мінімальному рівні або подекуди відсутні взагалі. Такий підхід створює значні ризики для функціонування самих

підприємств та для їхніх споживачів, партнерів і цифрових ланцюгів постачання загалом. Проведення дослідження дає можливість краще зрозуміти мотиваційні та організаційні особливості захисту суб'єктів малого підприємництва та сформулювати практичні рекомендації для підвищення їх цифрової стійкості.

Результати анкетування суб'єктів малого підприємництва щодо рівня витрат на інформаційну безпеку представлено на рис. 2.12.

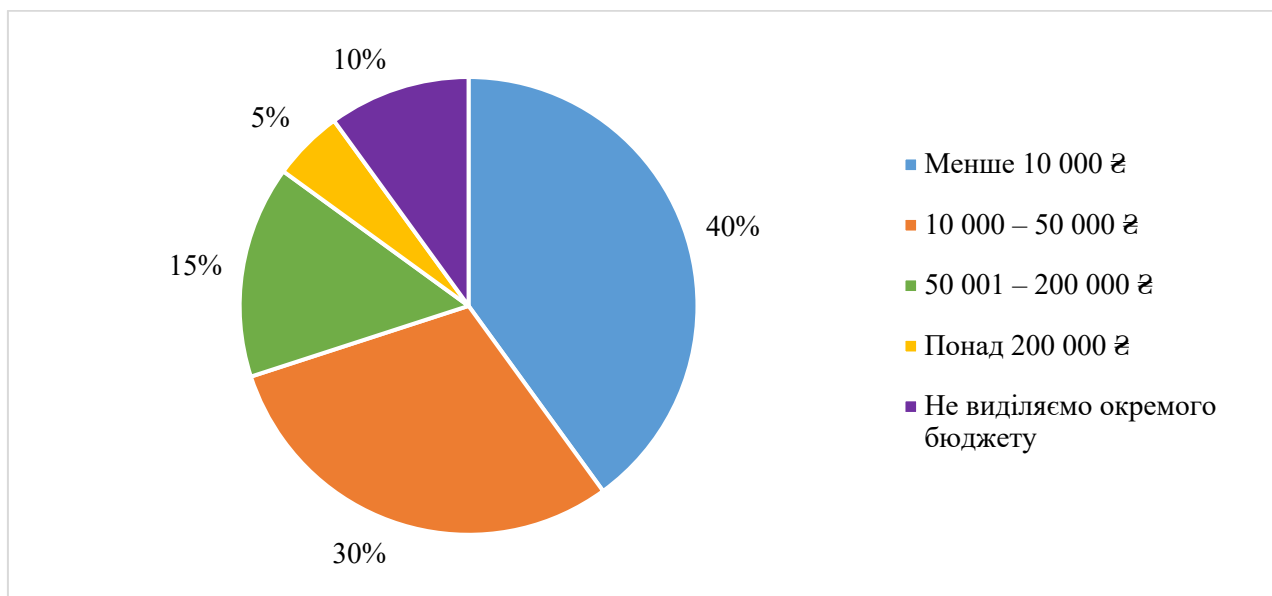


Рис. 2.12. Результати анкетування суб'єктів малого підприємництва щодо рівня витрат на інформаційну безпеку.

Джерело: побудовано автором за результатами опитування.

На основі аналізу результатів опитування, можна зробити висновки про характер та обсяги щорічних витрат малого бізнесу на забезпечення інформаційної безпеки. Представлені дані є репрезентативними для оцінки фінансової спроможності підприємств у сфері інформаційної безпеки, а також слугують індикатором їхньої цифрової зрілості та пріоритетності безпекових заходів у загальній бізнес-стратегії. Більшість суб'єктів малого підприємництва (40 %), за результатами опитування, витрачають на інформаційну безпеку менше 10 000 гривень на рік, що свідчить про загальну тенденцію до мінімізації витрат у цій сфері. Такий підхід зумовлений низьким рівнем усвідомлення ризиків, обмеженими ресурсами та відсутністю кваліфікованого персоналу. Значна частка респондентів зазначила, що взагалі не мають визначеного бюджету на

інформаційну безпеку, або витрати відбуваються нерегулярно та ситуативно – у разі настання інцидентів.

Незначна частка підприємств витрачає понад 5 000 гривень на рік, що, як правило, характерно для компаній із високою часткою цифрових процесів, наявністю інтернет-магазинів, віддаленого доступу до корпоративної інфраструктури або роботи з конфіденційними персональними даними споживачів. У таких підприємствах спостерігається вищий рівень формалізації системи інформаційної безпеки, включаючи політики, внутрішні регламенти, закупівлю програмного забезпечення для захисту кінцевих точок, резервне копіювання та аудит безпеки.

Загалом отримані результати вказують на недостатній рівень інвестування, серед більшості суб'єктів малого підприємництва, що створює потенційно вразливе середовище для цифрових інцидентів. Недофінансування інформаційної безпеки у малому підприємстві є чинником, що посилює їхню економічну нестійкість в умовах зростаючої кількості кіберзагроз. У цьому контексті актуальним є формування спрощених, але системних стратегій безпеки, які не потребують надмірних витрат, проте дозволяють суттєво знизити рівень ризиків [110]. Також доцільно впроваджувати механізми підтримки з боку інклюзивних інституцій, галузевих асоціацій, локальних кластерів, центрів цифрової грамотності, які можуть надати малому бізнесу доступ до типових інструментів, навчання та консультацій у сфері інформаційної безпеки. Таким чином, результати опитування є важливою емпіричною основою для подальшої розробки стратегій підвищення інвестиційної привабливості ІБ-рішень для суб'єктів малого підприємництва та свідчать про необхідність активізації державної політики підтримки інформаційної безпеки малого бізнесу на місцевому та національному рівнях.

Отримані результати опитування свідчать про низький рівень інвестицій суб'єктів малого підприємництва у сферу інформаційної безпеки, що вказує на необхідність формування доступних, ресурсоефективних стратегій інформаційної безпеки та посилення інституційної підтримки. В умовах

цифровізації та зростання кіберзагроз, системне недофінансування безпекових заходів становить суттєву загрозу для стабільності малого бізнесу, а тому потребує комплексної реакції з боку держави, місцевих органів влади та галузевих об'єднань.

Результати опитування суб'єктів малого підприємництва щодо суми збитків бізнесу, спричинених інформаційними атаками, за останні 5 років, представлено на рис. 2.13.

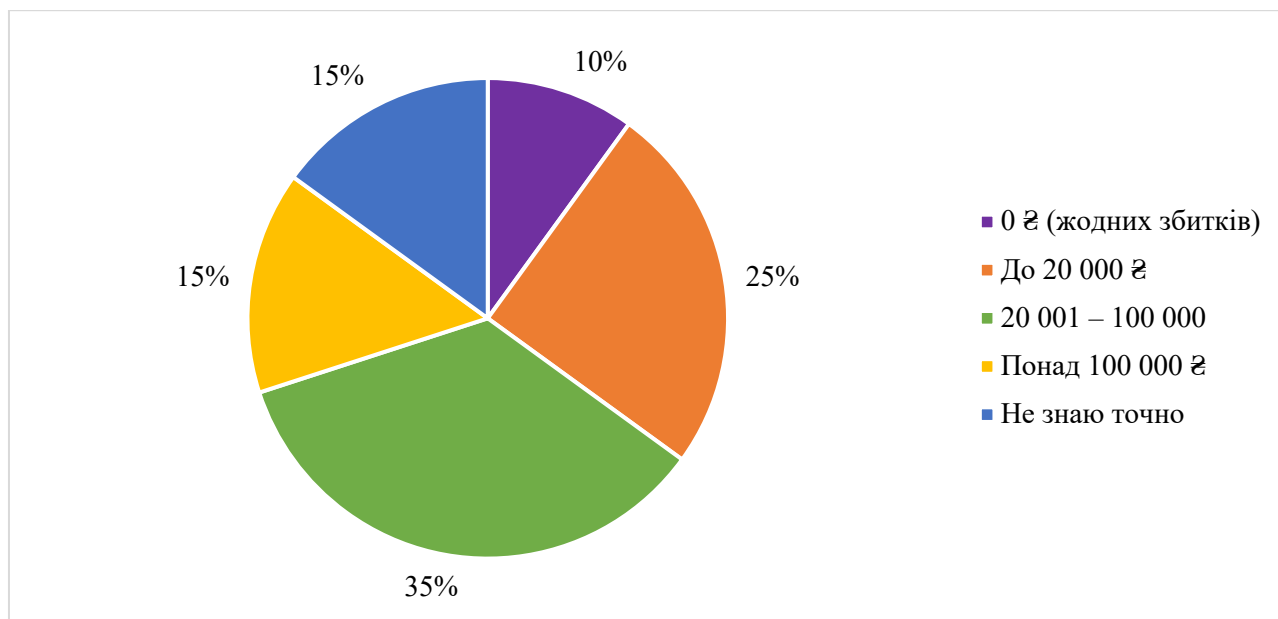


Рис. 2.13. Результати опитування суб'єктів малого підприємництва щодо суми збитків бізнесу, спричинених інформаційними атаками, за останні 5 років

Джерело: побудовано автором за результатами опитування

У результаті аналізу графічного відображення відповідей респондентів на питання «Яка сума збитків вашого бізнесу, спричинена інформаційними атаками, за останні 5 років?», виявлено низку тенденцій, які характеризують сучасний стан вразливості малого підприємництва до інформаційних загроз. Отримані результати дозволяють оцінити масштаби завданої шкоди та рівень обізнаності та готовності підприємств до протидії таким атакам.

Згідно з результатами опитування, переважна більшість досліджуваних підприємств (35 %), зазнала збитків у межах до 100 000 гривень внаслідок інформаційних інцидентів. Цей показник може свідчити про незначні фінансові

втрати, але вказує на обмежений рівень цифрової інтегрованості бізнесу або недостатню обізнаність про реальні масштаби пошкоджень. Часто малі підприємства не фіксують усіх втрат, пов'язаних з атаками (зупинка діяльності, втрата клієнтів, репутаційні наслідки), що занижує загальну оцінку шкоди.

Крім того, від 10 до 15% підприємств заявили про збитки понад 5 000 гривень, що вказує на наявність серйозних інцидентів, які мали прямий вплив на бізнес-операції. Досліджувані підприємства, як правило, мають вищу частку цифрової взаємодії зі споживачами або зберігають значний обсяг конфіденційної інформації. Частина респондентів (15%) також зафіксувала збитки понад 100 000 гривень, що є значним показником для більшості малих підприємств і часто супроводжується необхідністю тимчасового зупинення діяльності, втрати даних або юридичних наслідків. Особливо показовим є той факт, що певна частина респондентів не змогла оцінити обсяг збитків, що свідчить про відсутність систем моніторингу та обліку інцидентів, а також є тривожним сигналом, який свідчить про низький рівень зрілості систем управління інформаційною безпекою та відсутність внутрішньої політики реагування на кіберінциденти.

Загалом результати свідчать про суттєвий рівень економічної вразливості малого підприємництва перед кіберзагрозами, а також про відсутність належної фінансової оцінки наслідків атак. У довгостроковій перспективі це може призводити до хронічної недооцінки важливості інформаційної безпеки, невиправданих витрат у разі інцидентів та втрати конкурентоспроможності. Отже, актуальним завданням є впровадження механізмів навчання підприємців базовим принципам оцінки збитків та створення національної системи індикативного обліку кіберінцидентів у малому бізнесі. Представлені результати можуть лягти в основу формування політики підтримки малого бізнесу в напрямі підвищення цифрової грамотності, стандартизації звітності про кіберзбитки та розробки типових сценаріїв реагування на інформаційні атаки для сектору МСП.

Результати опитування засвідчують, що значна суб'єктів малого підприємництва зазнала фінансових втрат унаслідок інформаційних атак, проте здебільшого ці збитки не оцінюються належним чином або залишаються

незафіксованими, що свідчить про потребу у впровадженні систем моніторингу інцидентів, підвищенні рівня обізнаності керівників малого бізнесу щодо економічних наслідків кіберзагроз і створенні інституційної підтримки, яка дозволить мінімізувати втрати та посилити загальну стійкість суб'єктів малого підприємництва до інформаційних атак.

Результати опитування суб'єктів малого підприємництва щодо частоти проведення внутрішнього аудиту чи перевірки стану інформаційної безпеки, представлено на рис. 2.14.

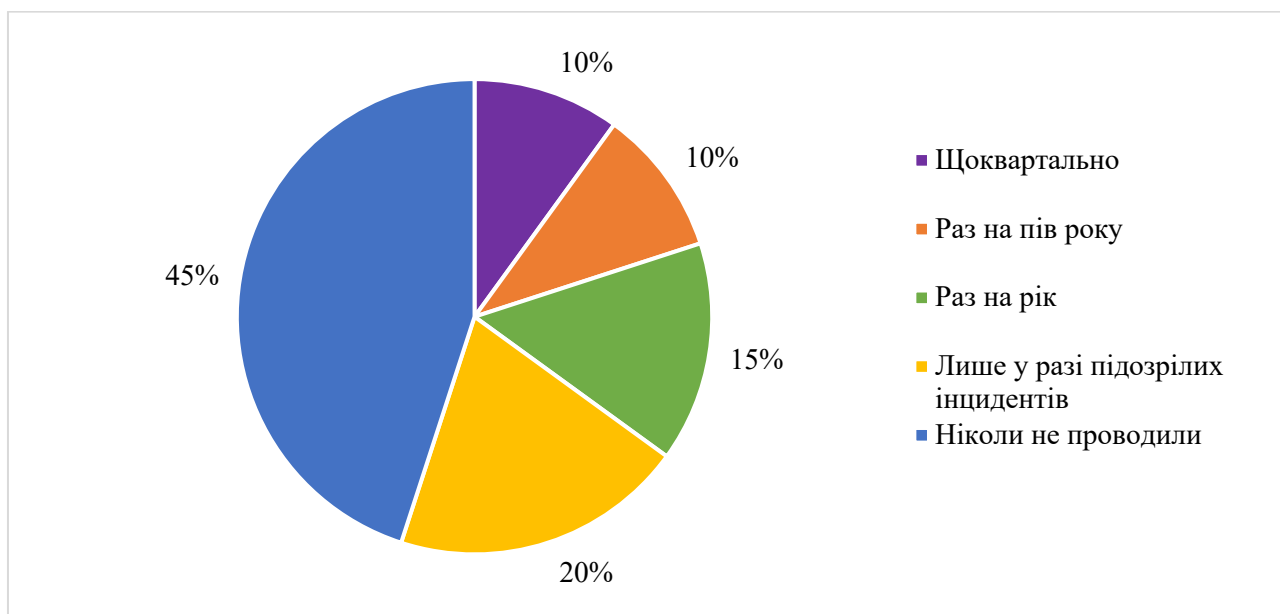


Рис. 2.14. Результати опитування суб'єктів малого підприємництва щодо частоти проведення внутрішнього аудиту щодо стану інформаційної безпеки.

Джерело: побудовано автором за результатами опитування

Найбільша частка респондентів (45 %) зазначила, що аудити інформаційної безпеки не проводяться взагалі або здійснюються «за потреби», що свідчить про відсутність внутрішніх регламентів, методик самооцінювання стану інформаційної безпеки та неформалізоване ставлення до контролю безпекових ризиків. Такий підхід знижує здатність суб'єктів малого підприємництва вчасно виявляти вразливості та запобігати інцидентам, що потенційно посилює економічну та репутаційну нестійкість бізнесу. Лише невеликий відсоток підприємств (до 10%) вказали на щоквартальне або щорічне проведення аудитів, що відповідає загальноприйнятим рекомендаціям

міжнародних стандартів, таких як ISO/IEC 27001. Зазначені підприємства, як правило, мають вищу цифрову зрілість, кращу фінансову спроможність і розуміння ролі інформаційної безпеки у забезпеченні довіри з боку клієнтів і партнерів. Їхній досвід може бути використаний як зразок для формування типових практик перевірок інформаційної безпеки для решти малого бізнесу.

Частина респондентів повідомила, що перевірки здійснюються нерегулярно або раз на кілька років, що формально створює ілюзію контролю, але не дозволяє оперативно реагувати на нові виклики та зміни в цифровому середовищі. У таких випадках основна мета перевірки – формальна відповідність вимогам контрагентів або кредиторів, а не реальна оцінка ефективності функціонування системи інформаційної безпеки. Загалом результати опитування демонструють низький рівень системності та культури безперервного аудиту в малому бізнесі, що є загрозливим чинником у контексті наростаючої складності кіберзагроз. Такий підхід, вимагає як просвітницьких заходів і навчання власників бізнесу, так і впровадження спрощених методик аудиту, адаптованих до ресурсних можливостей суб'єктів малого підприємництва. Інституційна підтримка, типові шаблони чек-листів, надання консультаційних послуг у сфері інформаційної безпеки можуть сприяти інтеграції процесів самооцінки та внутрішнього контролю в загальну стратегію управління ризиками малого підприємництва.

Результати опитування засвідчують, що більшість суб'єктів малого підприємництва не мають систематизованого підходу до проведення внутрішніх аудитів інформаційної безпеки, що свідчить про низький рівень культури контролю інформаційної безпеки та обмежену обізнаність щодо її стратегічного значення. Така ситуація підвищує ризики невиявлених вразливостей та неготовності до реагування на кіберінциденти. Для підвищення ефективності управління безпекою необхідне впровадження спрощених механізмів самоконтролю, доступних методик аудиту та інституційної підтримки, що дозволить малому бізнесу підвищити свою цифрову стійкість навіть за умов обмежених ресурсів.

Одним із основних інструментів превентивного захисту є регулярне резервне копіювання інформації, що дозволяє мінімізувати ризики втрати даних у разі кібератак, технічних збоїв або людських помилок. Проте в умовах обмежених фінансів, кадрового дефіциту та відсутності політик інформаційної безпеки, багато представників малого бізнесу нехтують цим процесом або здійснюють його епізодично. Аналіз практик резервного копіювання в малому бізнесі дозволяє виявити структурні прогалини в системі інформаційної безпеки, а також визначити потенційні напрями для формування ефективної моделі захисту даних на мікроекономічному рівні.

Результати опитування суб'єктів малого підприємництва щодо частоти здійснення резервного копіювання критичних даних, представлено на рис. 2.15.

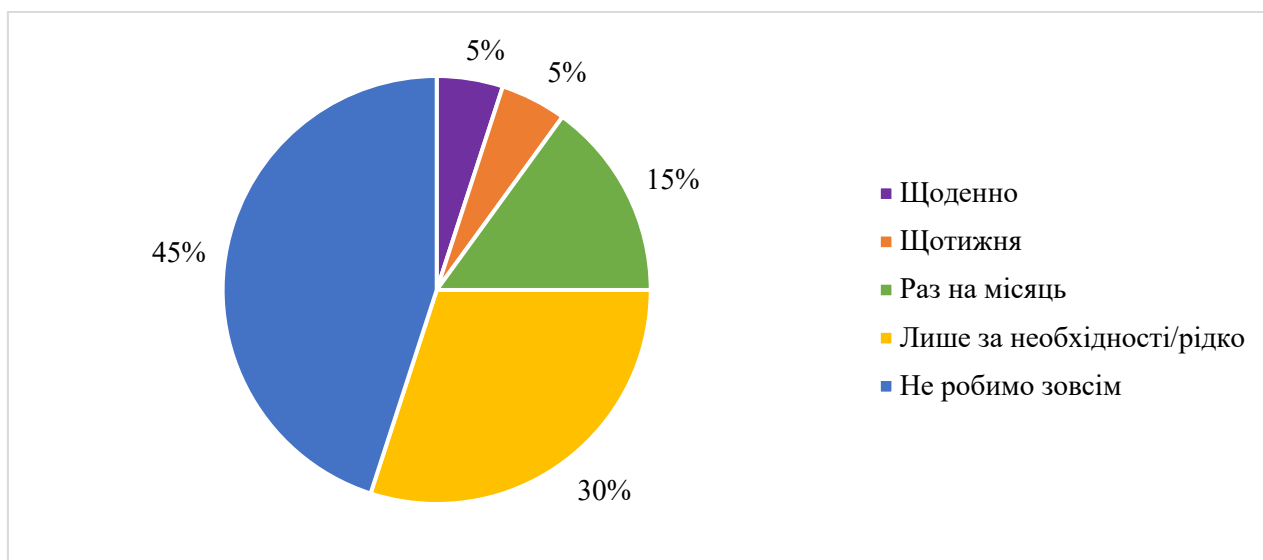


Рис. 2.15. Результати опитування суб'єктів малого підприємництва щодо частоти здійснення резервного копіювання критичних даних.

Джерело: побудовано автором за результатами опитування

Переважна частина респондентів зазначила, що резервне копіювання здійснюється нерегулярно або вручну, часто за ініціативою окремих працівників. Такий підхід, не гарантує збереження критичної інформації в разі інцидентів (збій обладнання, кібератака, помилка персоналу), що створює високі ризики втрати даних без можливості їх відновлення. Зазначене особливо небезпечно для бізнесів, які працюють із замовленнями, фінансовими операціями або

персональними даними клієнтів. Незначна частка досліджуваних суб'єктів малого підприємництва (5 %) вказала, що резервне копіювання здійснюється щотижня або щодня, причому за допомогою автоматизованих інструментів. Такі підприємства зазвичай мають вищий рівень цифрової зрілості, використовують хмарні технології та інтегрують IT-безпеку в загальну операційну діяльність. Їхній досвід свідчить про доцільність впровадження політик резервного копіювання навіть за обмежених фінансових ресурсів – за рахунок використання безкоштовних або доступних інструментів резервування.

Також важливим є той факт, що ряд респондентів (45 %) не здійснюють резервного копіювання взагалі, що є тривожним показником з точки зору базового рівня захищеності та може бути пов'язано як із відсутністю знань про ризику, так і з недооцінкою вартості втрачених даних. У таких умовах навіть незначні інциденти можуть призвести до повної втрати інформації та припинення бізнес-діяльності. Отже, результати опитування свідчать про необхідність формування культури відповідального ставлення до збереження даних у секторі малого бізнесу. Рекомендовано впроваджувати заходи з впровадження стандартних процедур резервного копіювання, використання хмарних сервісів, навчання персоналу та інтеграція копіювання в загальну стратегію інформаційної безпеки підприємства. Інституційна підтримка, типові політики та доступні технічні рішення можуть значно посилити рівень готовності малих підприємств до реагування на загрози втрати даних.

Результати опитування свідчать про низький рівень системності резервного копіювання критичних даних серед суб'єктів малого підприємництва, що створює суттєві ризики втрати інформації у разі інцидентів. Брак регулярності, автоматизації та обізнаності щодо важливості захисту даних свідчить про необхідність впровадження спрощених, доступних рішень і формування базових політик збереження інформації. Посилення інституційної підтримки та навчання персоналу є важливими умовами підвищення стійкості малого бізнесу до кіберзагроз і технічних збоїв.

Результати опитування суб'єктів малого підприємництва щодо часових рамок на виявлення серйозного інциденту безпеки (приклад: злам, зловмисна активність), представлено на рис. 2.16.

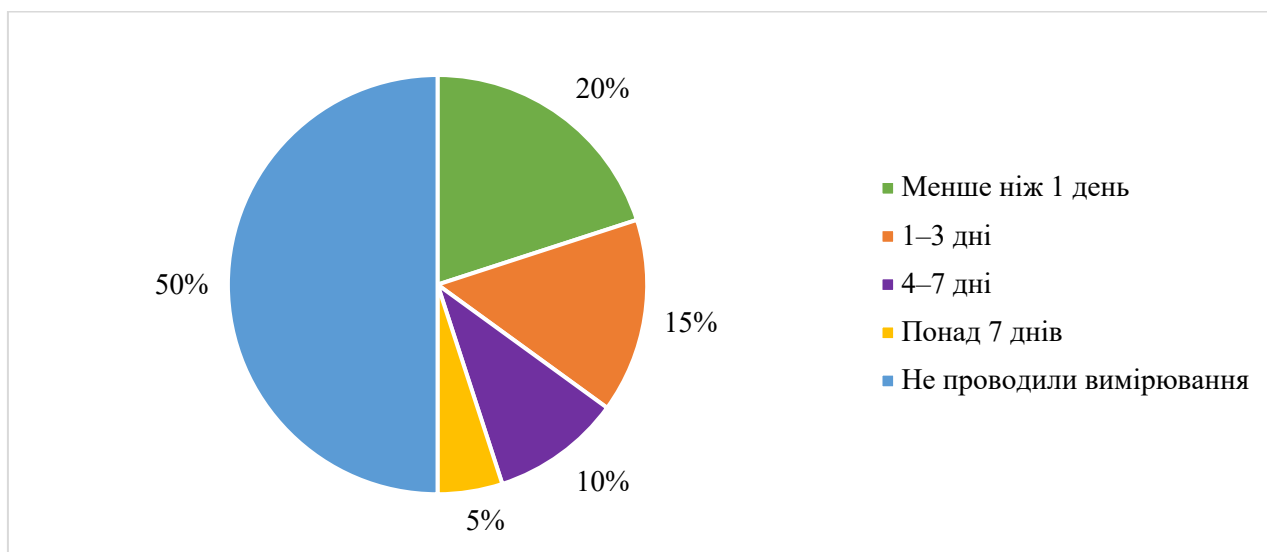


Рис. 2.16. Результати опитування суб'єктів малого підприємництва щодо часових рамок на виявлення серйозного інциденту безпеки.

Джерело: побудовано автором за результатами опитування.

Згідно з опитуванням, значна частка респондентів виявляє серйозні інциденти лише через кілька днів або тижнів після їх настання, що вказує на відсутність ефективних засобів спостереження та аналізу аномальної активності. Такий часовий спектр суттєво ускладнює можливість оперативного реагування та обмежує шанси на відновлення інформації або зменшення шкоди. У багатьох випадках інциденти виявляються випадково або після зовнішніх скарг (від клієнтів, партнерів, постачальників), що свідчить про реактивний, а не проактивний характер системи інформаційної безпеки. Лиш незначна частка суб'єктів малого підприємництва (20 %) фіксує інциденти протягом кількох годин або в день їх виникнення.

Особливо тривожним є те, що половина респондентів (50 %) взагалі не знає, скільки часу їм знадобиться для виявлення інциденту, що свідчить про повну відсутність систем моніторингу або політик реагування. Зазначене підтверджує висновок про те, що значна частина малого бізнесу функціонує в умовах «інформаційної сліпоти», що може призводити до накопичення

невиявлених загроз і зростання репутаційних та фінансових ризиків. Таким чином, отримані результати вказують на потребу у формуванні базових механізмів виявлення інцидентів, включаючи прості системи сповіщення, щоденний перегляд журналів доступу, використання хмарних сервісів з вбудованим моніторингом, а також навчання персоналу основам кібергігієни. Впровадження навіть мінімального рівня інструментів моніторингу може суттєво скоротити час виявлення інцидентів і підвищити інформаційну стійкість малого бізнесу.

Результати опитування свідчать, що більшість суб'єктів малого підприємництва неспроможні оперативно виявляти серйозні інциденти інформаційної безпеки, що значно підвищує ризики втрати даних, фінансових збитків і репутаційних втрат. Відсутність системного моніторингу та реагування свідчить про потребу у впровадженні навіть базових інструментів кіберспостереження, а також підвищенні обізнаності персоналу щодо ознак і сценаріїв порушення безпеки. Зменшення часу виявлення інцидентів є важливим чинником зміцнення цифрової стійкості малого бізнесу та формування ефективної стратегії інформаційної безпеки.

Результати опитування суб'єктів малого підприємництва щодо частоти оновлення програмного забезпечення (ОС, бізнес-застосунки) на робочих станціях і серверах, представлено на рис. 2.17.

Переважна частина суб'єктів малого підприємництва зазначила, що оновлення здійснюються нерегулярно або лише в разі виникнення технічних проблем, що свідчить про відсутність планового підходу до оновлення систем і про нехтування превентивними заходами захисту. Такий підхід значно підвищує ризик експлуатації відомих вразливостей з боку зловмисників, адже саме застаріле ПЗ є одним із найпоширеніших векторів кібератак, включаючи фішинг, шкідливе ПЗ та несанкціонований доступ.

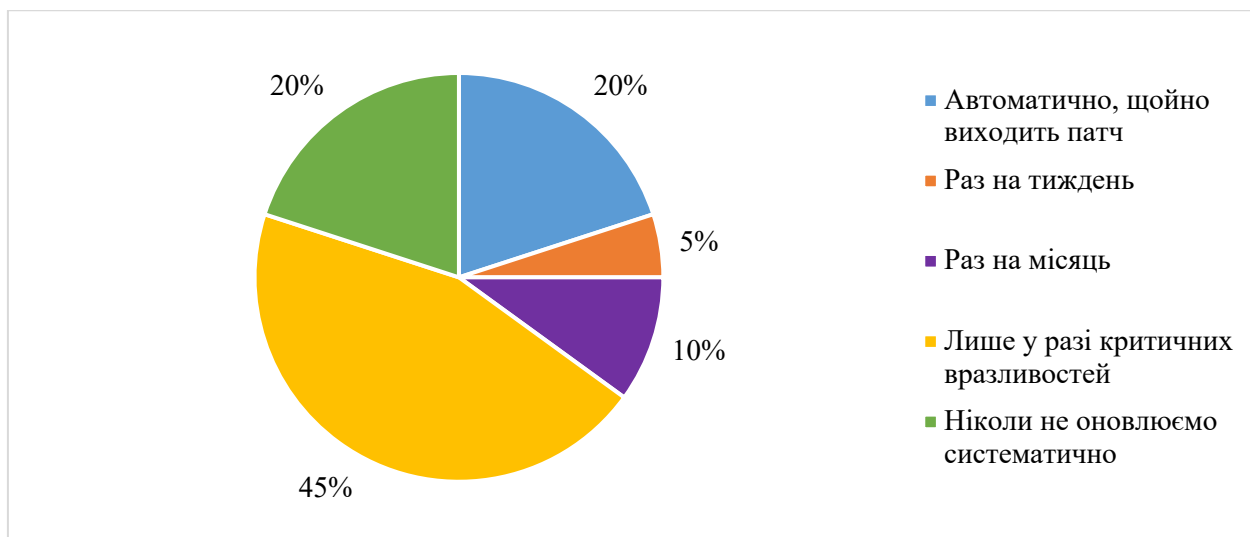


Рис. 2.17. Результати опитування суб'єктів малого підприємництва щодо частоти оновлення програмного забезпечення.

Джерело: побудовано автором за результатами опитування.

Незначна частка суб'єктів малого підприємництва (20 %) повідомила про автоматизоване або регулярне оновлення ПЗ, зокрема за графіком або в межах централізованого управління, що свідчить про вищу цифрову зрілість таких підприємств, а також про наявність ІТ-фахівця або партнерів з аутсорсингового обслуговування, які відповідають за підтримку інформаційної інфраструктури. Регулярне оновлення в таких випадках розглядається як частина загальної політики інформаційної безпеки і інтегрується в інші процеси управління ризиками.

Особливу занепокоєність викликає той факт, що деякі підприємства взагалі не контролюють або не відстежують частоту оновлень, що свідчить про повну відсутність політики керування життєвим циклом ПЗ. У такому середовищі ризики несанкціонованого втручання або збоїв у роботі систем мають високу ймовірність, і будь-який інцидент може призвести до серйозних економічних або репутаційних наслідків. Таким чином, результати опитування засвідчують низький рівень уваги до оновлення ПЗ у малому бізнесі, що потребує корекції через впровадження базових процедур ІТ-менеджменту, автоматизацію оновлень, навчання персоналу та розробку типових політик інформаційної безпеки для підприємств мікро- та малого рівня. Регулярне оновлення

операційних систем і програмних рішень має стати важливим елементом стратегій кіберзахисту малого бізнесу.

Результати опитування свідчать, що переважна більшість суб'єктів малого підприємництва не дотримується системного підходу до оновлення програмного забезпечення, що створює серйозні вразливості в їхній інформаційній інфраструктурі. Відсутність регулярного оновлення підвищує ризик експлуатації відомих вад у ПЗ, знижує загальний рівень безпеки та демонструє недостатню цифрову культуру управління ризиками. У цьому контексті важливим є впровадження доступних механізмів автоматичного оновлення, формування політик ІТ-обслуговування та підвищення обізнаності малого бізнесу щодо ролі оновлень як важливого компонента інформаційної безпеки.

Результати опитування суб'єктів малого підприємництва щодо рівня готовності інвестувати в інформаційну безпеку представлено на рис. 2.18.

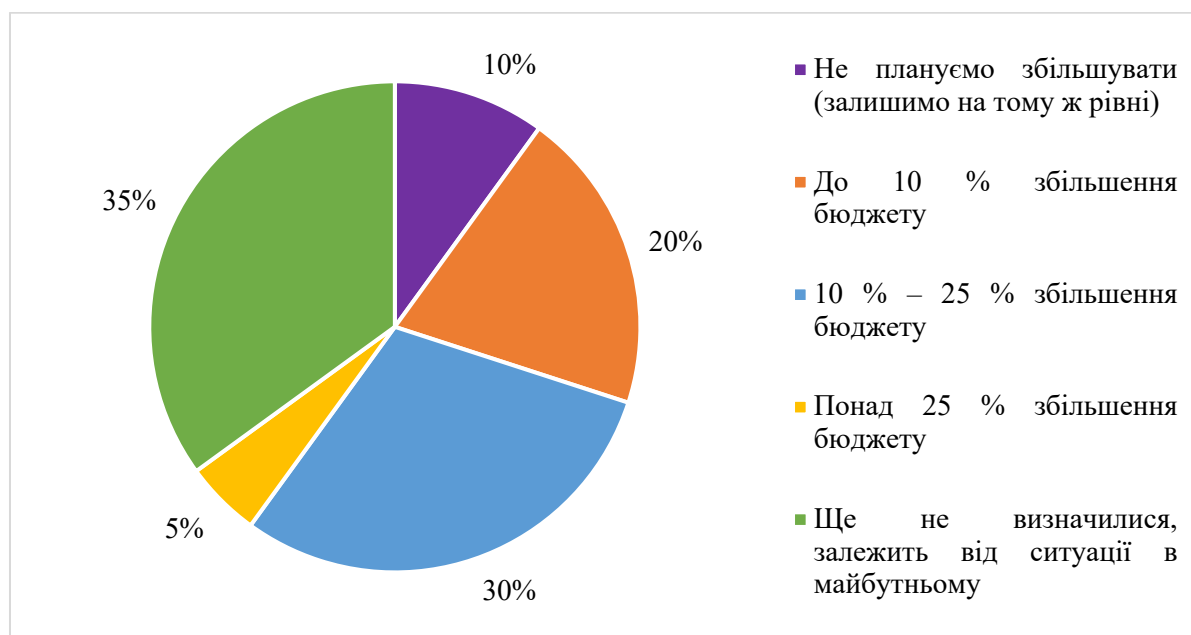


Рис.2.18. Результати опитування суб'єктів малого підприємництва щодо рівня готовності інвестувати в інформаційну безпеку.

Джерело: побудовано автором за результатами опитування.

Згідно з даними опитування, найбільша частка респондентів (35 %) ще не визначилась щодо рівня готовності інвестувати в інформаційну безпеку. Проте, 30 % респондентів, готова збільшити витрати на інформаційну безпеку в межах

10-25% у порівнянні з попереднім роком, що свідчить про переважно консервативний підхід до планування безпекових бюджетів, у якому превалюють короткострокові міркування та реакція на безпосередні загрози, а не довгострокові стратегії розвитку цифрової стійкості. Така ситуація пояснюється як браком ресурсів, так і відсутністю формалізованого підходу до оцінки ризиків.

Близько 5 % опитаних підприємств вказали на можливість збільшити інвестиції у сферу інформаційної безпеки на понад 25%, що є позитивною ознакою усвідомлення значущості інформаційної безпеки в умовах цифровізації та свідчить про появу більш проактивної позиції в частини підприємств, зокрема тих, що працюють в онлайн-середовищі, обслуговують замовлення через інтернет або зберігають персональні дані споживачів. У таких компаніях безпека розглядається як конкурентна перевага та засіб формування довіри з боку споживачів.

Також 10 % респондентів не планують змінювати обсяги фінансування інформаційної безпеки, що може свідчити як про стабільність, так і про недооцінку потенційних ризиків. Часто така позиція обумовлена відсутністю інцидентів у минулому або відсутністю інструментів оцінки ефективності вже здійснених заходів, що створює ілюзію безпеки, яка може виявитися хибною в умовах зростаючої складності атак. Загалом отримані результати демонструють, що попри зростання обізнаності про важливість інформаційної безпеки, готовність малого бізнесу до масштабного збільшення інвестицій у цю сферу залишається обмеженою. Такий підхід, вимагає формування економічно досяжних рішень з кіберзахисту та активізації освітніх програм, демонстрації практичної вигоди від вкладень у інформаційну безпеку, а також створення інституційних механізмів підтримки цифрової трансформації суб'єктів малого підприємництва.

Результати опитування свідчать, що попри зростаюче усвідомлення важливості інформаційної безпеки, більшість суб'єктів малого підприємництва готові збільшити інвестиції в інформаційну безпеку лише в обмеженому обсязі, орієнтуючись переважно на мінімально необхідні витрати. Така тенденція вказує

на потребу у формуванні доступних, економічно обґрунтованих моделей захисту, а також у розробці стимулюючих механізмів з боку держави та професійних об'єднань. У довгостроковій перспективі, системний підхід до інвестування в інформаційну безпеку дозволить забезпечити стійкість малого бізнесу в умовах зростаючих цифрових загроз.

Рівень інформаційної безпеки суб'єктів малого підприємництва може визначатись наявним співвідношення витрат на досліджувані процеси та отриманими доходами. Обсяги витрат на інформаційну безпеку важко визначити у зв'язку зі складністю виокремлення їх в структурі витрат, доцільність проведення детальних підрахунків та певною мірою через комерційну таємницю. Тому, в опитуванні суб'єктів малого підприємництва було запропоновано зазначити обсяги витрат на інформаційну безпеку у відносних величинах (%). Причому враховуючи, що в останні роки на суб'єкти бізнесу мали вплив ряд деструктивних факторів (пандемія та війна), тому обсяги витрат на інформаційну безпеку кориливалися і цими процесами.

Зазначимо, що згідно з аналітичними дослідженнями в Україні та ЄС, типова частка витрат на інформаційну безпеку у малому бізнесі коливається:

- у межах 1,0-2,5% від загального доходу, за умов мінімального цифрового навантаження [111];
- до 5% від загального доходу для бізнесів з помірною цифровою залежністю (наприклад, онлайн-торгівля, сервісні послуги) [112];
- вище 5% від загального доходу у високотехнологічному сегменті або при нещодавньому досвіді кібератак [113].

Для побудови моделі доцільно розрахував витрати на інформаційної безпеки як відсоткову частку від річного доходу підприємства (Y) з урахуванням середньостатистичної поведінки суб'єктів малого підприємництва у сфері безпеки:

- для підприємств із доходами до 5 млн грн, пропонуємо застосувати коефіцієнт 1,5-2,0% [114];

- для підприємств із доходами понад 5 млн грн – коефіцієнт 1,2-1,5% (через ефект економії на масштабі) [115];

- для цифрово-активних компаній (за результатами опитувальника) – коефіцієнт 2,5–3,0% [116].

Оскільки вибірка охоплює саме суб'єкти малого підприємництва Волині, на нашу думку, витрати доцільно помірковано знизити порівняно з теоретичним максимумом. Середнє значення частки витрат на інформаційну безпеку у цій моделі становить близько 1,7% від доходу.

Таким чином, в нашому дослідженні, обравши надані суб'єктами малого підприємництва питомі частки витрат на інформаційну безпеку в структурі доходів, а також взявши дані обсяги доходів суб'єктів малого підприємництва, що вказані на порталі «YouControl», визначено орієнтовні обсяги витрат на інформаційну безпеку досліджуваних суб'єктів у 2023 р. (табл. 2.7).

Таблиця 2.7 – Вихідні дані для розрахунку кореляційної залежності обсягів доходів суб'єктів малого підприємництва від обсягів витрат на інформаційну безпеку

Суб'єкти підприємництва	У – обсяги доходів, тис. грн.	Х – орієнтовні обсяги витрат на інформаційну безпеку, тис. грн.
ТОВ «Espresso Lab»	6800	102
ТзДВ «Елтех»	12000	180
ТОВ «Августіно»	4500	72
ТОВ «Добра Кухня»	3200	51
ТОВ «Хімпласт»	8900	134
ТОВ «КаДар-Україна»	7700	115
ФОП «Райсон»	3100	47
ТОВ «Татрафан»	15000	225
ТОВ «СМ-хім»	4200	67
ПП «Артеспресо»	2500	41
ТОВ «Бест Бебі Комфорт»	3800	59
ТОВ «Атлант-Плюс»	6700	101
ФОП «Стохід»	1900	32
ПП «Аква Прінт»	2700	45
ФОП «Creative Play»	3900	63
ТОВ «Віва»	9300	139
ПрАТ «ВГП»	11000	165
ФОП «Black Mirror»	3000	46
ПП «Гарна хата»	4700	71
ПП «Vinvest»	5600	84

Джерело: побудовано автором за результатами опитування та [117].

Маючи розраховані показники обсягів витрат на інформаційну безпеку та доходів суб'єктів малого підприємництва, здійснено визначення їх кореляційної залежності. Де, y – обсяги доходів, тис. грн. – залежна змінна, x – орієнтовні обсяги витрат на інформаційну безпеку досліджуваних суб'єктів підприємництва, тис. грн., незалежна змінна. Таким чином, при побудові кореляційної залежності обсягів доходів досліджуваних суб'єктів малого підприємництва від обсягів витрат на інформаційну безпеку сформована лінійна залежність (рис. 2.19).

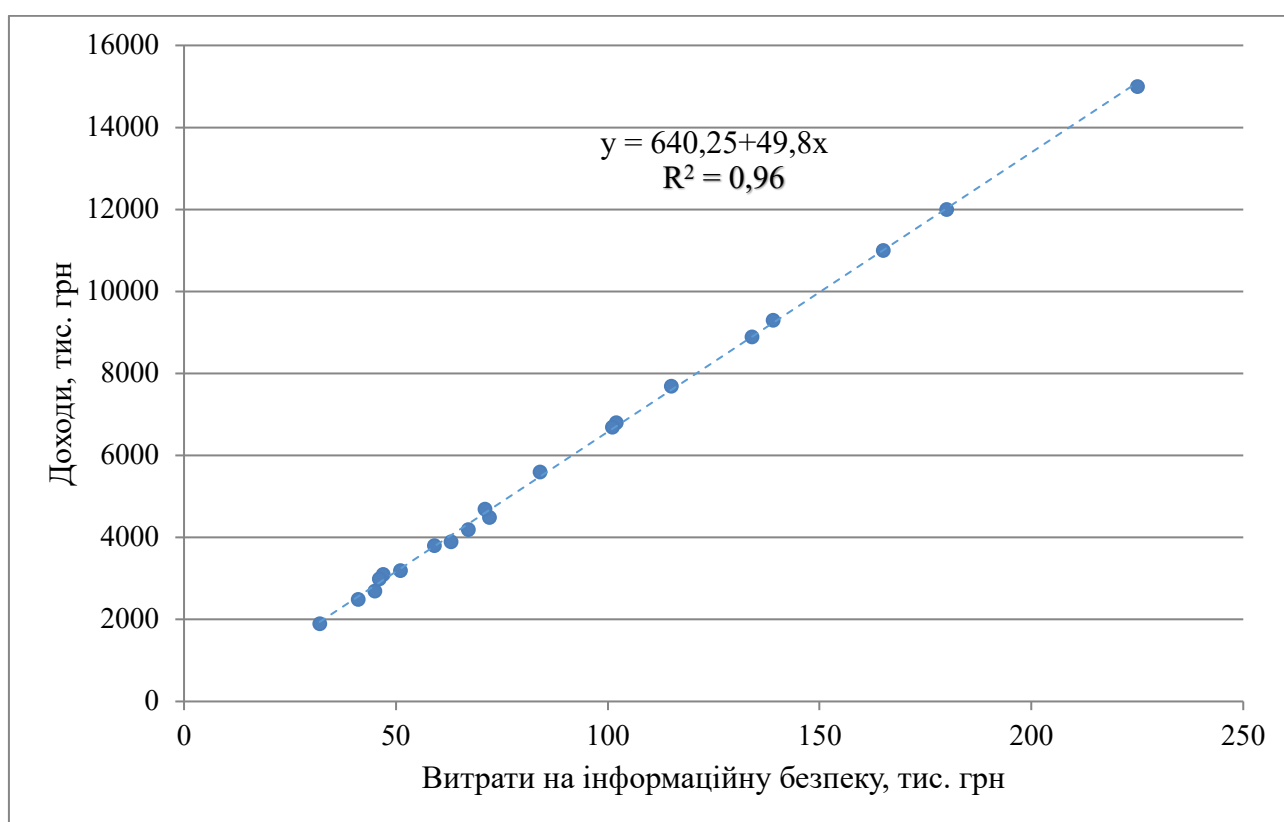


Рис. 2.19. Кореляційна залежність обсягів доходів досліджуваних суб'єктів малого підприємництва від обсягів витрат на інформаційну безпеку.

Джерело: побудовано автором.

Графічне відображення кореляційної залежності між витратами на інформаційну безпеку та річними доходами суб'єктів малого підприємництва, відображає наявність позитивного зв'язку між обсягами інвестицій у заходи кіберзахисту та фінансовими результатами діяльності підприємств. Зокрема,

побудована регресійна модель демонструє, що зі збільшенням витрат суб'єктів підприємництва на інформаційну безпеку зростають також і річні доходи підприємств, що свідчить про ефективність таких інвестицій. Побудована залежність обсягів доходів досліджуваних суб'єктів малого підприємництва від обсягів витрат на інформаційну безпеку, підтверджує припущення про стратегічну роль інформаційної безпеки у зміцненні конкурентоспроможності малого бізнесу в умовах цифрової трансформації та загроз зовнішнього середовища.

Отримане рівняння регресії:

$$Y=640,25+49,80X \quad (2.21),$$

відображає лінійну залежність між витратами на інформаційну безпеку (X) та доходами підприємств (Y). Це рівняння свідчить про те, що за відсутності інвестицій в інформаційну безпеку ($X = 0$), прогнозований дохід підприємства становитиме орієнтовно 640,25 тис.грн. При цьому кожна додаткова тисяча гривень, витрачена на інформаційну безпеку, потенційно підвищує річний дохід на 49,8 тис. грн, що свідчить про високу чутливість прибутків до рівня цифрового захисту.

Коефіцієнти моделі мають економічну інтерпретацію, константа відображає базовий рівень доходу без вкладень у інформаційну безпеку, а нахил регресійної прямої – середній ефект від інвестицій в інформаційну безпеку. Побудова такої моделі дозволяє формалізувати залежність між показниками, а також використовується для обґрунтування стратегічних управлінських рішень щодо доцільного рівня фінансування заходів з кіберзахисту в малому бізнесі. Отримані результати свідчать про необхідність включення інформаційної безпеки як пріоритетного напрямку інвестування, що може забезпечити зростання економічної результативності суб'єктів малого підприємництва в умовах зростання кіберризиків.

Зазначимо, що у цій моделі коефіцієнт достовірності (Пірсона) складає $R^2 = 0,96$, тобто на 96 %, тому можна вважати, що залежність є високою та достовірною. І орієнтовно зміна доходів на 96 % може залежати від зміни обсягів

витрат на інформаційну безпеку. Таким чином, графічне відображення свідчить про наявність сильної позитивної кореляції, що відповідає дуже тісному зв'язку між змінними.

Маючи обсяги витрат на інформаційну безпеку досліджуваних суб'єктів підприємства у відносних та абсолютних показниках можна побудувати модифіковану матрицю BCG та визначити групи досліджуваних суб'єктів за рівнем інформаційної безпеки (таблиця 2.8).

Таблиця 2.8 – Вихідні дані для побудови модифікованої матриці BCG щодо рівня інформаційної безпеки суб'єктів малого підприємства

Суб'єкти підприємства	Питома вага витрат на інформаційну безпеку суб'єктів, %	Орієнтовні (розраховані) обсяги витрат на інформаційну безпеку, тис. грн.
ТОВ «Espresso Lab»	1,50	102
ТзДВ «Елтех»	1,50	180
ТОВ «Августіно»	1,60	72
ТОВ «Добра Кухня»	1,59	51
ТОВ «Хімпласт»	1,51	134
ТОВ «КаДар-Україна»	1,49	115
ФОП «Райсон»	1,52	47
ТОВ «Татрафан»	1,50	225
ТОВ «СМ-хім»	1,60	67
ПП «Артеспрессо»	1,64	41
ТОВ «Бест Бебі Комфорт»	1,55	59
ТОВ «Атлант-Плюс»	1,51	101
ФОП «Стохід»	1,68	32
ПП «Аква Прінт»	1,67	45
ФОП «Creative Play»	1,62	63
ТОВ «Віва»	1,49	139
ПрАТ «ВГП»	1,50	165
ФОП «Black Mirror»	1,53	46
ПП «Гарна хата»	1,51	71
ПП «Vinvest»	1,50	84

Джерело: побудовано автором за результатами опитування та [117].

Застосування вихідних даних дозволяє провести стратегічне позиціонування підприємств за двома основними критеріями, питомою вагою витрат на інформаційну безпеку та абсолютним обсягом цих витрат. Такий підхід сприяє ідентифікації груп підприємств, залежно від рівня їх залученості у процес забезпечення інформаційної безпеки, що, створює аналітичне підґрунтя для

формування адресних стратегій посилення інформаційної безпеки з урахуванням специфіки витратних пріоритетів і можливостей окремих суб'єктів бізнесу [118].

На рис. 2.20 представлена матриця рівнів інформаційної безпеки досліджуваних суб'єктів підприємництва побудована за допомогою таблиць Excel.

Знаючи питомі (відносні) та абсолютні обсяги витрат на інформаційну безпеку кожного підприємства, доцільно здійснити їх класифікацію за рівнем інформаційної безпеки за допомогою модифікованої матриці BCG. Зміст методу – побудувати двовимірну матрицю, де по горизонтальній осі зазначено питома вага витрат на інформаційну безпеку (%) як показник «рівня» уваги до безпеки, а по вертикальній – абсолютний обсяг витрат (тис. грн) як показник «масштабу» вкладень. Відповідно до методики, доцільно виділити окрему стратегічну групу підприємств за рівнем інформаційної безпеки.

На рис. 2.20 зображено побудовану матрицю BCG для вибірки суб'єктів малого підприємництва Волині. Точками на ній, позначено підприємства (їх положення визначається % витрат на інформаційну безпеку та сумою витрат у тис. грн згідно таблиці 2.8). Матриця дозволяє візуалізувати розподіл 20 досліджуваних підприємств за двома критеріями: інтенсивністю інвестицій у безпеку (питома вага у доході) та абсолютним розміром витрат на інформаційну безпеку. Такий підхід дає змогу оцінити пріоритетність інформаційної безпеки у його внутрішній стратегії. Хоча більшість досліджуваних суб'єктів згруповані близько до 1,5% (через невелику варіацію часток витрат), матриця все ж дозволяє умовно виділити чотири сегменти: «лідери» (висока відносна і абсолютна кібербезпека), «активні інноватори» (значні витрати при відносно низькій їх частці), «консерватори» (низькі витрати і частка) та «потенційні новатори» (висока частка витрат при невеликому абсолютному їх обсязі).

Лідери – підприємства з достатньо високим рівнем інформаційної безпеки, які виділяють значні ресурси на інформаційну безпеку (обсяг витрат – найвищий у вибірці).

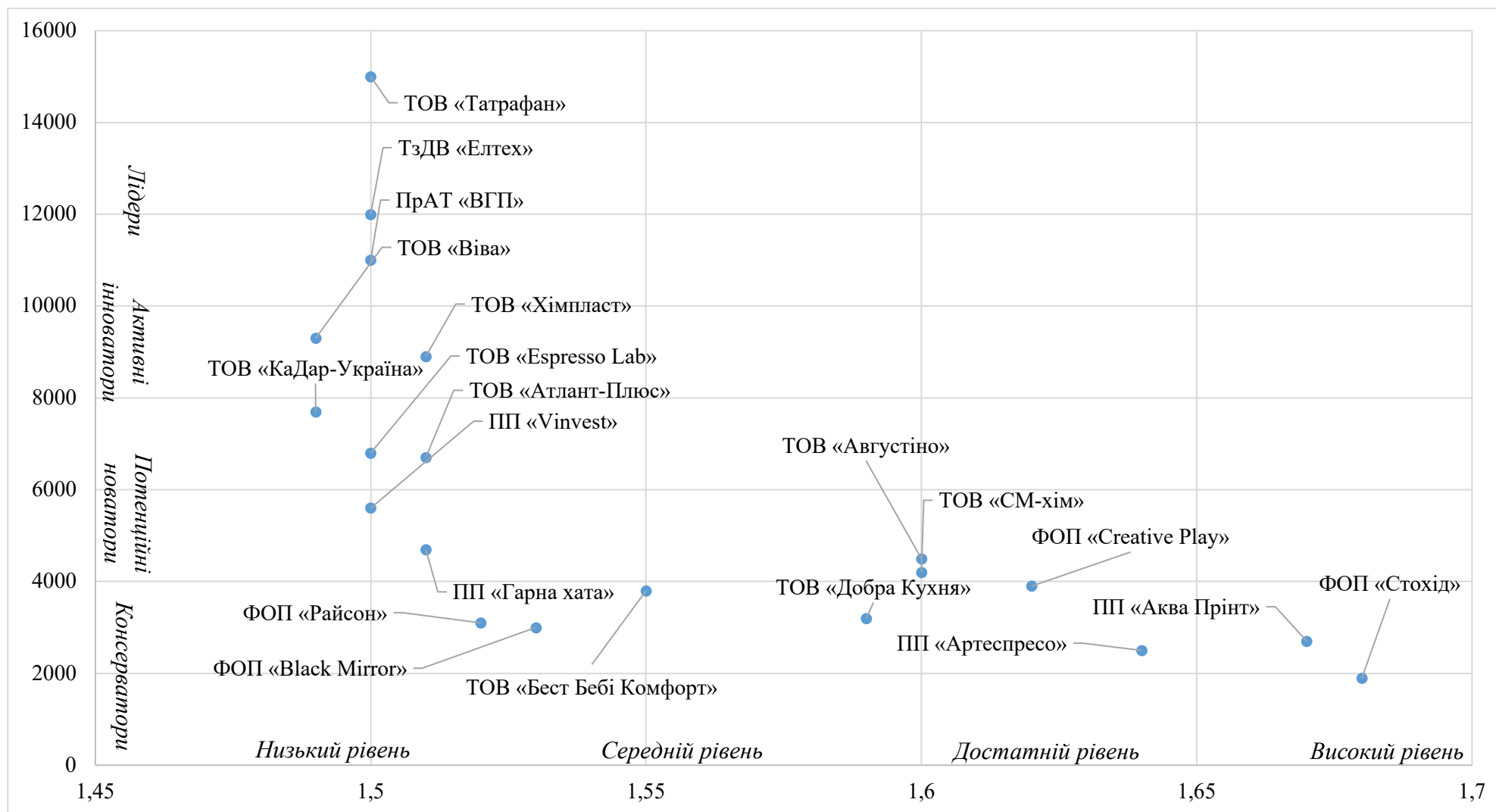


Рис. 2.20. Матриця рівнів інформаційно ї безпеки суб'єктів малого підприємництва.

Джерело: побудовано автором.

Такі суб'єкти можна вважати флагманами з точки зору цифрової безпеки – вони мають фінансові та кадрові можливості впроваджувати сучасні засоби захисту і виступають своєрідними «локомотивами» підвищення кіберстійкості у малому бізнес-секторі. До лідерів за рівнем інформаційної безпеки, у нашому дослідженні віднесено підприємства: ТзДВ «Елтех», ТОВ «Татрафан», ПрАТ «ВГП» та ТОВ «Віва» – всі вони мають найбільші доходи у вибірці (9-15 млн грн) і витрачають на інформаційну безпеку близько 135-225 тис. грн на рік (майже 1,5% від доходу). Фактично, ці компанії забезпечують собі достатньо високий кіберзахист і можуть слугувати орієнтиром для інших.

Активні інноватори (послідовники) – група підприємств, які також здійснюють значні заходи щодо інформаційної безпеки, але обсяги використання захисних технологій у них дещо нижчі, ніж у лідерів. Це, як правило, бізнеси з вищими за середні витратами на інформаційну безпеку, проте частка цих витрат у доході в них невисока (близько 1,5% або менше). Іншими словами, вони інвестують у інформаційну безпеку значні суми, але в межах базових потреб (наприклад, через ефект економії масштабу у відносно більших компаніях частка витрат природно менша). До активних інноваторів можна віднести: ТОВ «Хімпласт», ТОВ «КаДар-Україна», ТОВ «Espresso Lab», ТОВ «Атлант-Плюс» та ПП «Vinvest». Кожне з них витрачає на інформаційну безпеку, приблизно 100-134 тис. грн/рік, що співставно з лідерами, але їхня частка витрат (біля 1,5% чи менше) свідчить про те, що ці витрати, ймовірно, відповідають типовому мінімуму для їхнього масштабу бізнесу. Тим не менш, такі підприємства впроваджують необхідні засоби захисту і належать до достатнього рівня інформаційної безпеки (не поступаючись лідерам за ресурсами, але можливо менш проактивні у впровадженні новітніх практик).

Потенційні новатори – гіпотетична категорія «зірок» (за аналогією з класичною матрицею BCG), тобто підприємств, які б одночасно демонстрували дуже значний обсяг і високу частку витрат на інформаційну безпеку (що свідчило б про їхню проактивну інноваційну позицію та готовність інвестувати, наперед у масштабні проєкти кіберзахисту). Серед досліджуваних малих підприємств не

виявлено таких, що відповідали б критеріям потенційних новаторів (висока відносна і абсолютна витрата). Це означає, що жодне опитане підприємство наразі не інвестує в кібербезпеку більше, ніж того вимагає його поточний розмір та ризику. Всі знаходяться радше в руслі «наздоганяючої» стратегії, ніж випереджаючої. У теорії, поява компаній-потенційних новаторів могла б означати, що окремі малі підприємства почали витрачати на інформаційну безпеку помітно більше середнього (скажімо, 3-5% доходу), що вирізняло б їх як піонерів впровадження нових стандартів безпеки. Проте поки що для Волинського малого бізнесу таке явище не характерно.

Консерватори – підприємства, що поки що не досягли значного прогресу у розбудові системи інформаційної безпеки. Вони характеризуються низькими витратами на інформаційну безпеку як в абсолютному вимірі, так і за часткою від доходу. Здебільшого це найменші за розмірами бізнесу у вибірці, для яких вкладення у інформаційну безпеку є тягарем. Такі фірми обмежуються хіба що базовими засобами захисту (антивірус, резервне копіювання тощо) або можуть відкладати інвестиції у цю сферу через брак коштів чи знань. До групи консерваторів потрапили: ФОП «Райсон», ПП «Артеспресо», ФОП «Black Mirror», ПП «Аква Прінт» та ФОП «Стохід». Їхні витрати на інформаційну безпеку становлять менше 50 тис. грн на рік, а частка – близько 1,5-1,7% (у двох найменших – хоч і 1,7%, але це всього 32-45 тис. грн). Таким підприємствам переважно притаманний низький рівень інформаційної безпеки: вразливості у їхніх системах можуть залишатися непоміченими, політики безпеки – неформалізованими, а резервного фонду на кіберзахист фактично немає. Це найбільш ризикована група з точки зору потенційних інцидентів.

Крім зазначених категорій систематизуємо досліджувані суб'єкти малого підприємництва за рівнем інформаційної безпеки, визначивши чотири основних типи: низький, середній, достатній та високий. Відповідно до нашого аналізу, розподіл досліджуваних підприємств Волинської області за рівнем інформаційної безпеки виглядає таким чином:

Низький рівень інформаційної безпеки – підприємства-консерватори, що витрачають мінімальні кошти на кібербезпеку. Для них характерна відсутність системного підходу до інформаційної безпеки, мінімально необхідні засоби захисту та реактивна (а не проактивна) позиція. Представниками такого рівня є: ТЗДВ «Елтех», ТОВ «Татрафан», ПрАТ «ВГП», ТОВ «Віва», а також ТОВ «КаДар-Україна», ТОВ «Espresso Lab», та ТОВ «Хімпласт», ПП «Vinvest». Ці бізнеси потребують підвищення уваги до безпеки, адже наразі їхній захист можна вважати недостатнім.

Середній рівень інформаційної безпеки – підприємства, що мають помірні (середні) досліджувані показники. Вони здійснюють певні витрати та заходи, але все ще не досягають оптимального рівня. Як правило, це невеликі компанії, які витрачають 50-70 тис. грн на рік (1,6% доходу) і впровадили базові політики безпеки. Представниками серед досліджуваних суб'єктів за таким рівнем інформаційної безпеки є: ТОВ «Добра Кухня», ТОВ «СМ-хім», ТОВ «Бест Бебі Комфорт», ПП «Гарна хата», ТОВ «Августіно». Ці підприємства демонструють розуміння необхідності інформаційної, але їм слід нарощувати інвестиції та заходи для виходу на вищий рівень захищеності.

Достатній рівень інформаційної безпеки – підприємства-«послідовники» та частина лідерів, які забезпечили прийнятний, хоча й не максимальний рівень кібербезпеки. Вони витрачають значні кошти (близько 70-120 тис. грн на рік) і мають більш-менш комплексну систему захисту (політики, ІТ-рішення, резервні копії тощо). Даний рівень можна вважати таким, що відповідає поточним ризикам малого бізнесу. Представниками серед досліджуваних суб'єктів за таким рівнем інформаційної безпеки є: ПП «Артеспресо» та ФОП «Creative Play». Вони вже сьогодні інвестують в інформаційну безпеку близько 1,5% доходу, що в абсолюті становить 80-115 тис. грн – цього достатньо для впровадження основних засобів захисту.

Високий рівень інформаційної безпеки – підприємства-лідери, які вирізняються найвищими показниками як за витратами, так і за інтеграцією інформаційної безпеки в бізнес-процеси. Вони фактично наблизилися до меж

потенціалу малого бізнесу у сфері безпеки. Представниками серед досліджуваних суб'єктів за таким рівнем інформаційної безпеки є: ПП «Аква Прінт» та ФОП «Стохід». Ці компанії можна охарактеризувати як такі, що мають комплексну систему інформаційної безпеки: виділено бюджет під сучасні технології захисту, залучено фахівців, діють внутрішні політики та плани реагування. Високий рівень інформаційної безпеки став для них частиною бізнес-стратегії, що забезпечує стійкість до загроз та довіру споживачів.

Таким чином, проведене дослідження виявило, що рівень інформаційної безпеки у більшості малих підприємств регіону наразі є помірним або низьким. Більшість компаній витрачають на інформаційну безпеку близько 1,5% від доходу, що відповідає мінімально рекомендованим значенням для малого бізнесу і вказує на обережне ставлення до цих витрат. Лише декілька підприємств-лідерів досягли відносно високого рівня інформаційної безпеки, інтегрувавши захист у свою діяльність і виділяючи на це відповідні ресурси. Позитивним моментом є виявлена висока кореляція між витратами на інформаційну безпеку та фінансовими результатами, що аргументує бізнес-цінність інвестицій у інформаційну безпеку. Однак загальна картина свідчить, що малий бізнес Волинської області поки що реагує на кіберризики, а не випереджає їх. Так, жодне з опитаних підприємств не інвестує «проактивно» понад необхідний мінімум. Низка суб'єктів консерваторів фактично залишаються вразливими до інцидентів – відсутність спеціалістів і малий бюджет не дозволяють їм вибудувати дієву систему захисту. З огляду на зростання кіберзагроз (у тому числі внаслідок війни) та негативні наслідки інцидентів (фінансові втрати, простої, витік даних, шкода репутації), стан інформаційної безпеки малого бізнесу потребує покращення. Необхідно підвищувати зрілість ІБ-практик, впроваджувати стратегії, політики, сучасні технології захисту та розвивати культуру кібергігієни серед персоналу. Без цих кроків багато підприємств залишатимуться легкими цілями для кіберзлочинців, що ставить під загрозу їх стабільність і розвиток.

Інформаційна безпека має стати невід'ємною складовою стратегій розвитку малого бізнесу. В сучасних умовах виживання і успіх підприємства багато в чому залежать від його здатності захистити свої цифрові активи. Як слушно зазначено багатьма експертами, вкладення в інформаційну безпеку – це не просто витрати, а необхідна умова стабільного функціонування і зростання компанії.

Висновки до розділу 2

Доведено, що системне дослідження стану інформаційної безпеки потребує застосування науково обґрунтованих методичних підходів, які поєднують кількісні та якісні критерії оцінювання, дозволяють враховувати специфіку суб'єктів підприємництва та забезпечують об'єктивність і надійність результатів. Оцінювання інформаційної безпеки має базуватися на комплексному використанні індикаторів, що відображають технічний, організаційний, економічний та поведінковий виміри захищеності підприємства.

Обґрунтовано доцільність використання ризик-орієнтованої методології, що поєднує кількісне моделювання (зокрема на основі порогових значень, індикаторних систем і матриць ризиків) з експертними оцінками. Такий підхід забезпечує діагностику поточного стану інформаційної безпеки та формування стратегічних орієнтирів її розвитку з урахуванням зовнішніх викликів, внутрішнього потенціалу підприємства та змін нормативно-правового середовища.

Розроблено комплексний дев'ятиетапний алгоритм дослідження процесу забезпечення інформаційної безпеки суб'єктів малого підприємництва, який поєднує аналітичну оцінку фактичного рівня захищеності з формуванням стратегічних рішень щодо його підвищення. Запропонований підхід дозволяє об'єктивно оцінювати рівень інформаційної безпеки підприємств та адаптивно коригувати стратегії її забезпечення залежно від зміни зовнішнього середовища

та внутрішніх ресурсів, що має важливе прикладне значення в умовах цифрової трансформації економіки.

Доведено, що розвиток малого підприємництва в Україні зумовлюється комплексом взаємопов'язаних детермінант, а саме інституційних, економічних, правових, інформаційно-технологічних та соціально-культурних. Кожен з цих чинників має неоднаковий ступінь впливу залежно від регіональних умов, галузевої належності та рівня цифрової зрілості суб'єкта підприємництва. Критично важливою умовою сталої динаміки розвитку малого бізнесу є здатність підприємств адаптуватися до зовнішніх викликів, включаючи військові ризики, регуляторну невизначеність та нестабільне економічне середовище.

Визначено, що однією з провідних детермінант виступає доступ до фінансових і кредитних ресурсів, які значною мірою визначають інвестиційні можливості, темпи модернізації, а також здатність підприємства до цифрової трансформації. Іншим важливим чинником є рівень інформаційної безпеки, який безпосередньо впливає на довіру споживачів, партнерів і держави, а також забезпечує стійкість функціонування в умовах кіберзагроз. Крім того, важливу роль відіграють освітньо-інноваційні можливості, які формують потенціал підприємця до самонавчання, впровадження нових рішень і формування ефективних моделей управління.

Доведено, що формування сприятливого середовища для розвитку малого підприємництва вимагає комплексної державної політики, що має включати стимулювання інвестицій, спрощення регуляторних процедур, розвиток інфраструктури підтримки бізнесу, удосконалення системи податкових пільг та інституційної підтримки. Особливої актуальності набуває створення механізмів підтримки інформаційної безпеки, цифрової грамотності та інноваційного розвитку, які виступають фундаментальними умовами сталого зростання малого бізнесу в умовах сучасних трансформацій української економіки.

Проведено оцінку рівня інформаційної безпеки суб'єктів малого підприємництва, яка виявила значну диференціацію стану захищеності залежно від рівня витрат на інформаційну безпеку, технічної оснащеності, наявності

політик безпеки та рівня обізнаності персоналу. Дослідження підтвердило, що більшість малих підприємств перебуває на початковому або середньому рівні інформаційної безпеки, що вказує на високі ризики вразливості до сучасних кіберзагроз. Особливо критичними є аспекти недостатньої регламентації процесів безпеки, нерегулярного навчання персоналу, обмеженого фінансування та обмеженого застосування захисних технологій.

Визначено інтегральну оцінку досліджуваних процесів, яка дозволила ідентифікувати групи підприємств за рівнем їхньої кіберстійкості, що дало можливість сформулювати відповідні стратегії реагування та вдосконалення. Зокрема, підприємства з високим рівнем інформаційної безпеки відзначаються системним підходом до безпеки, інтегрованими рішеннями та регулярним аудитом, тоді як підприємства з низьким рівнем часто нехтують базовими заходами безпеки, що створює передумови для значних втрат у разі інцидентів. Аналіз питомої ваги витрат на інформаційну безпеку у загальній структурі бюджету підприємств засвідчив, що в більшості випадків такі витрати залишаються мінімальними й не відповідають реальному рівню ризиків.

Проаналізовано результати оцінювання, що підтвердило необхідність розроблення адресних заходів державної, регіональної та галузевої підтримки у сфері підвищення рівня інформаційної безпеки малого підприємництва. Актуальним є впровадження механізмів оцінки ризиків, створення систем моніторингу та індикаторів інформаційної безпеки, а також розвиток культури інформаційної безпеки через навчання та підвищення цифрової грамотності персоналу. Отримані результати можуть стати базою для формування інституційної підтримки та стратегічних рішень у сфері кіберзахисту малого бізнесу.

РОЗДІЛ 3

НАУКОВО-МЕТОДИЧНИЙ ІНСТРУМЕНТАРІЙ УДОСКОНАЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА

3.1 Науково-методичні підходи до побудови системи інформаційної безпеки підприємства

У сучасних умовах цифровізації економіки, зростаючої залежності бізнес-процесів від інформаційних систем та глобального поширення кіберзагроз, побудова ефективної системи інформаційної безпеки стає важливим елементом забезпечення стабільного функціонування підприємств. Інформаційна безпека сьогодні розглядається як стратегічна складова корпоративного управління, яка безпосередньо впливає на фінансову сталість, конкурентоспроможність та ділову репутацію підприємства. В умовах динамічного розвитку ІТ-середовища та нових викликів, пов'язаних із хмарними технологіями, мобільною роботою, віддаленим доступом та штучним інтелектом, традиційні підходи до захисту інформаційних ресурсів не забезпечують належного рівня захищеності [119].

Науково-методичні підходи до створення ефективної системи інформаційної безпеки підприємства потребують комплексного врахування організаційних, технічних, економічних, правових та поведінкових чинників, що вимагає інтеграції знань з управління ризиками, кібербезпеки, інформатики, правознавства, фінансового менеджменту тощо. Наукова література свідчить про значну кількість запропонованих моделей та концепцій побудови системи інформаційної безпеки, однак у практичній площині часто спостерігається розрив між теоретичними розробками та можливостями їх реалізації в умовах обмежених ресурсів, особливо на малих та середніх підприємствах [120]. З огляду на це, особливої актуальності набуває систематизація та осмислення науково-методичних підходів до формування політики інформаційної безпеки підприємства, вибору інструментів оцінювання ризиків, розроблення та

впровадження організаційно-технічних рішень, адаптованих до специфіки його діяльності. Ефективна система інформаційної безпеки має будуватись на основі принципів гнучкості, превентивності, економічної доцільності та постійного моніторингу загроз, що вимагає застосування сучасних наукових методологій і доказових практик управління безпекою [121].

Система інформаційної безпеки кожного підприємства є суто індивідуальною, оскільки формується під впливом низки унікальних внутрішніх і зовнішніх чинників. До них належать сфера діяльності, масштаб підприємства, рівень цифрової трансформації, структура інформаційних потоків, категорії оброблюваної інформації, ступінь критичності інформаційних ресурсів, а також наявні технічні та кадрові ресурси. Універсальних шаблонів для побудови ефективної системи інформаційної безпеки не існує, а кожне підприємство має розробити власну модель захисту з урахуванням конкретного ризикового середовища та стратегічних пріоритетів [122]. Індивідуалізація системи інформаційної безпеки вимагає глибокого розуміння технологічної архітектури підприємства та проведення ґрунтового аудиту інформаційних активів, оцінки потенційних загроз і вразливостей, а також прогнозування наслідків можливих інцидентів. Методичні підходи до моделювання ризиків, визначення порогових значень захищеності, впровадження системи управління інцидентами та заходів реагування є важливими з огляду на проблему. Такий підхід дозволяє забезпечити адаптивність системи інформаційної безпеки до змін.

Індивідуальна побудова системи інформаційної безпеки не виключає потреби у дотриманні загальновизнаних міжнародних стандартів, таких як ISO/IEC 27001, NIST SP 800-53, які задають орієнтири для структуризації процесів безпеки [123].

Проте застосування таких стандартів потребує їх адаптації до специфіки бізнесу з урахуванням його організаційної культури, рівня цифрової грамотності працівників та бізнес-моделі.

Структурно-компонентна модель формування системи інформаційної безпеки підприємства запропонована на рис. 3.1.

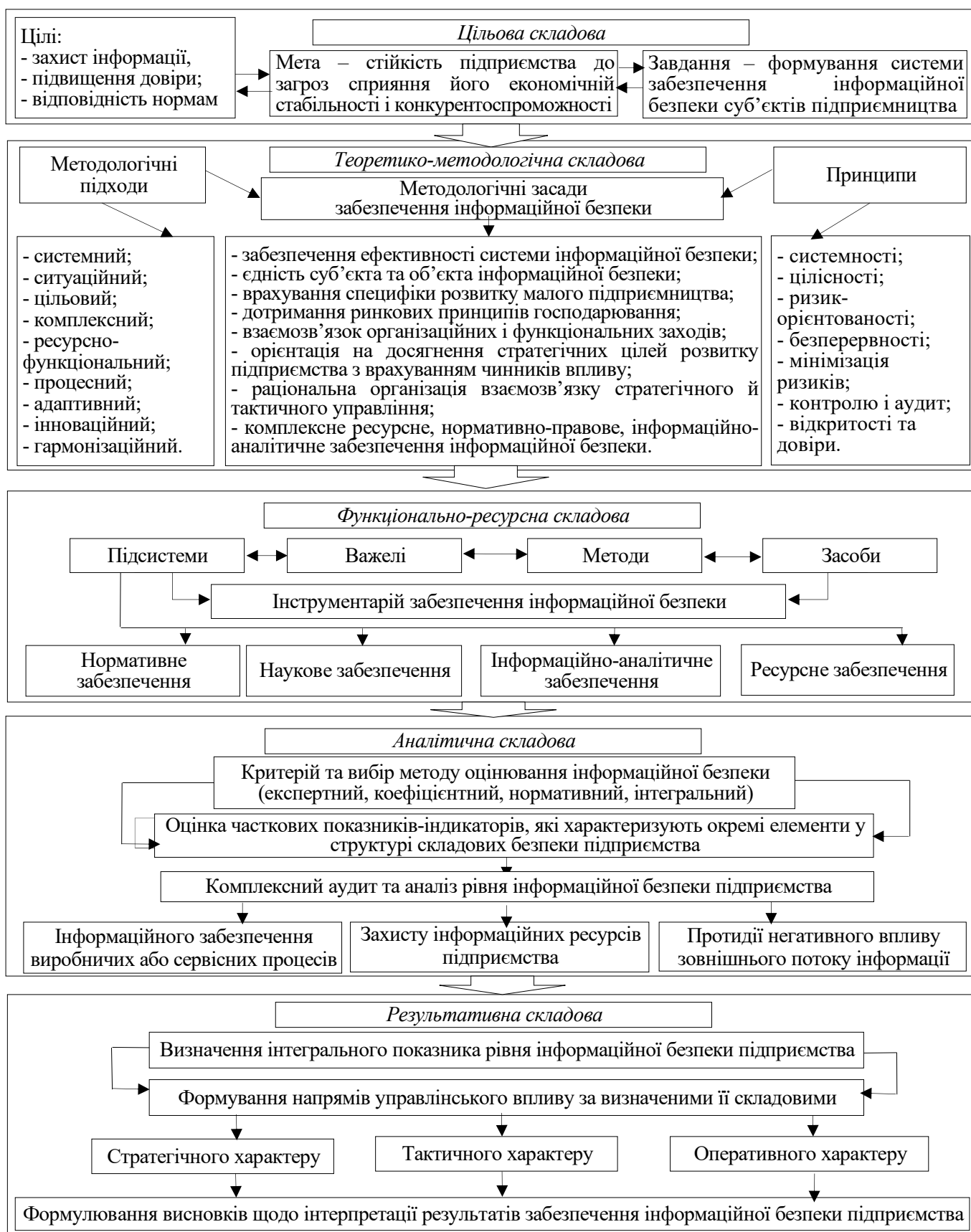


Рис. 3.1. Структурно-компонентна модель формування системи інформаційної безпеки підприємства.

Джерело: побудовано автором

Цільова складова визначає стратегічні орієнтири системи інформаційної безпеки підприємства. Основною метою є забезпечення стійкості підприємства до зовнішніх і внутрішніх загроз, що сприяє його економічній стабільності та конкурентоспроможності. Цілі включають захист інформації, підвищення довіри з боку партнерів і споживачів, а також відповідність чинним правовим нормам. Формулювання цілей є відправною точкою для побудови всієї системи, оскільки саме вони визначають зміст, структуру і функціональні параметри безпекової діяльності.

Теоретико-методологічна складова охоплює принципи, підходи та методологічні засади забезпечення інформаційної безпеки. До основних методологічних підходів належать: системний, процесний, ситуаційний, адаптивний, інноваційний, гармонізаційний тощо. Принципи системності, ризик-орієнтованості, безперервності, контролю, відкритості та довіри слугують базою для формування збалансованої політики інформаційного захисту [124]. Також враховується специфіка суб'єктів малого підприємництва, що передбачає більш гнучкий та адаптивний підхід до безпеки.

Функціонально-ресурсна складова відповідає за інструментарій реалізації інформаційної безпеки. Зазначена складова включає важелі, методи, засоби, ресурси (людські, фінансові, технічні) і нормативно-правове забезпечення. Вона включає також розробку інструментів, спрямованих на протидію загрозам, підтримку ефективної роботи інформаційної інфраструктури, запобігання витоку даних та впровадження сучасних ІТ-засобів захисту.

Аналітична частина моделі передбачає оцінювання стану інформаційної безпеки на основі часткових та інтегральних показників. Застосовуються різні методи оцінювання – експертні, коефіцієнтні, нормативні та інтегральні. Оцінка охоплює інформаційне забезпечення процесів, захист інформаційних ресурсів, протидію негативному впливу зовнішньої інформації тощо. На основі аналізу визначаються слабкі місця системи та напрями коригування стратегії.

Комплексний аудит та аналіз забезпечує поглиблену перевірку системи інформаційної безпеки з урахуванням внутрішніх і зовнішніх чинників. Аудит

охоплює як технічні, так і організаційні аспекти, дозволяючи виявити порушення, прорахунки, неузгодженості у функціонуванні окремих елементів системи, що створює основу для прийняття обґрунтованих управлінських рішень.

Результативна складова включає визначення рівня інформаційної безпеки, формування управлінських рішень стратегічного, тактичного та оперативного рівнів. Після цього проводиться формулювання висновків щодо ефективності заходів, що були впроваджені, та визначення напрямів подальшого розвитку системи. Загалом, структурно-компонентна модель формування системи інформаційної безпеки підприємства є багатовимірним конструктом, який враховує технічні, організаційно-управлінські, нормативні, ресурсні та аналітичні аспекти. Її впровадження забезпечує цілісне бачення захисту інформаційного середовища підприємства як важливого елементу загальної бізнес-стратегії.

Таким чином, структурно-компонентна модель формування системи інформаційної безпеки підприємства є цілісною науково-методичною конструкцією, що поєднує стратегічні, методологічні, функціонально-ресурсні, аналітичні та результативні елементи, забезпечуючи комплексний підхід до захисту інформаційного середовища підприємства. Її реалізація дозволяє ефективно протидіяти внутрішнім і зовнішнім загрозам та формувати адаптивну, гнучку та довгостроково стійку систему управління інформаційною безпекою. Завдяки чітко визначеним цілям, продуманим принципам, багаторівневому інструментарію та науково обґрунтованій методиці оцінювання, модель сприяє зміцненню конкурентоспроможності підприємства, підтриманню довіри з боку партнерів та забезпеченню відповідності нормативно-правовим вимогам в умовах сучасного цифрового середовища.

Проведений аналіз засвідчив, що сьогодні інформаційні ресурси стають одним із найцінніших активів, а їх втрата або компрометація може призвести до серйозних економічних та репутаційних збитків. У зв'язку з цим виникає нагальна потреба у формуванні системного підходу до побудови ефективної

системи інформаційної безпеки, яка б забезпечувала технічний захист даних та охоплювала організаційні, нормативні, кадрові й аналітичні аспекти управління безпекою. Тому, розробка чіткого алгоритму дій зі створення такої системи є важливою умовою зміцнення інформаційної стійкості підприємства в умовах динамічного середовища (рис. 3.2).

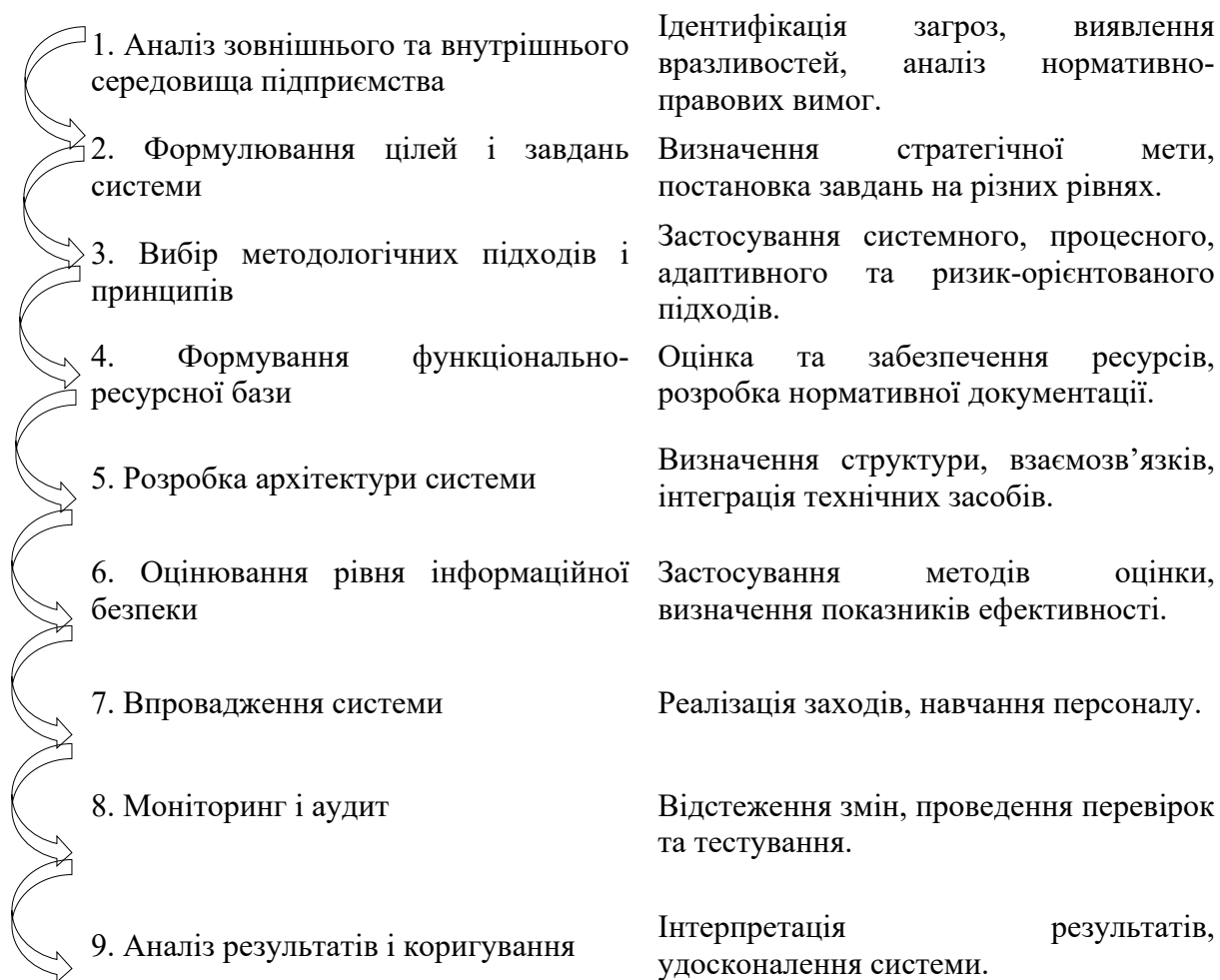


Рис. 3.2. Алгоритм послідовності дій зі створення системи інформаційної безпеки підприємства.

Джерело: побудовано автором на основі [125-127].

На початковому етапі важливо здійснити всебічний аналіз чинників, які впливають на стан інформаційної безпеки. Доцільно виявити потенційні загрози (кіберзлочинність, витік даних, технічні збої), оцінити внутрішні вразливості (організаційні прогалини, недостатня кваліфікація персоналу) та дотримання нормативно-правових вимог. Такий етап дозволяє сформулювати реалістичне

уявлення про вихідну позицію підприємства та загрозу його функціональній стабільності.

Цілі та завдання мають бути сформульовані відповідно до стратегічних пріоритетів підприємства. Основна мета полягає у гарантуванні конфіденційності, цілісності та доступності інформації, а також у підвищенні довіри з боку партнерів і споживачів. Чітко визначені завдання, деталізують шляхи досягнення цілей, розподіляються за ієрархією управління – від оперативного до стратегічного рівнів.

Вибір методологічних підходів і принципів визначає основи побудови системи, які забезпечують її цілісність і адаптивність. Застосування системного підходу дозволяє охопити всі функціональні рівні підприємства, адаптивний – врахувати змінність загроз, ризик-орієнтований – зосередити зусилля на найбільш критичних точках. Принципи безперервності, контролю, відкритості й довіри створюють основу для сталого управління інформаційною безпекою.

Ефективна система інформаційної безпеки не може існувати без належного забезпечення ресурсами, що охоплює як матеріальні ресурси (технічні засоби, програмне забезпечення), так і кадрові (кваліфікований ІТ-персонал, служби безпеки), а також нормативні документи (інструкції, регламенти). Особливу роль відіграє інформаційно-аналітичне забезпечення, яке дозволяє приймати обґрунтовані управлінські рішення.

На етапі розробки архітектури системи, формується структура системи інформаційної безпеки, зокрема визначаються її підсистеми (організаційна, технічна, аналітична, юридична). Архітектура має передбачати взаємодію між усіма елементами, що дозволяє забезпечити її узгодженість, ефективність і гнучкість. Особливо важливою є інтеграція сучасних технологічних рішень, які забезпечують активний моніторинг і реагування на інциденти.

Оцінювання рівня інформаційної безпеки доцільно здійснювати систематично, за допомогою різних методів – експертного, коефіцієнтного, нормативного або інтегрального, що дозволяє встановити рівень захищеності підприємства, виявити основні елементи та оцінити ефективність упроваджених

заходів. Використання індикаторів дозволяє кількісно оцінити ступінь ризиків і динаміку їх змін.

Впровадження передбачає реалізацію комплексу організаційно-технічних заходів, таких як інсталяція засобів захисту, налаштування політик доступу, підвищення рівня обізнаності персоналу. Окреме місце посідає навчання працівників правилам інформаційної безпеки, що знижує ризик «людського фактору» – однієї з найпоширеніших причин витоку інформації.

Система інформаційної безпеки повинна працювати в умовах постійного моніторингу. Аудит забезпечує перевірку її ефективності та відповідності стандартам. Регулярний перегляд ризиків, оновлення захисних механізмів і тестування на проникнення дозволяють своєчасно реагувати на нові загрози.

Фінальним етапом є аналіз досягнутих результатів та визначення шляхів удосконалення, що дозволяє адаптувати систему до нових умов і підвищити її ефективність. Постійне оновлення системи є необхідною умовою збереження її релевантності в умовах швидкої трансформації інформаційного середовища.

Таким чином, створення ефективної системи інформаційної безпеки підприємства потребує послідовного, науково обґрунтованого підходу, що охоплює всі основні складові захисту інформаційних ресурсів – від аналізу загроз до постійного моніторингу та вдосконалення системи. Запропонований алгоритм дозволяє забезпечити цілісність, адаптивність і результативність безпекових заходів, що є надзвичайно важливими для збереження стабільності підприємства, зниження ризиків інформаційних втрат та підтримання високого рівня довіри з боку партнерів і споживачів. В умовах цифрової трансформації та зростання кіберзагроз така система стає технічною необхідністю та елементом стратегічного управління розвитком підприємства.

Незважаючи на те, що суб'єкти малого підприємництва, як правило, не мають значних інформаційних активів у порівнянні з великими корпораціями, саме вони найчастіше стають об'єктами кібератак через обмежені ресурси, недостатню захищеність та низький рівень організаційної зрілості у сфері інформаційної безпеки [128]. Тому, виникає потреба в розробці доступних,

логічно структурованих та стандартизованих підходів до побудови системи інформаційної безпеки, які б були придатними до реалізації в малих організаціях.

Пропонуємо сформувати фреймворк на основі систематизації кращих практик у сфері інформаційної безпеки, рекомендацій міжнародних стандартів та досвіду впровадження практичних рішень для малого бізнесу. В основу такого фреймворку пропонуємо покласти структурно-компонентну модель, яка дозволяє чітко ідентифікувати елементи інформаційної системи підприємства, описати їх функціональне призначення, взаємозв'язки, відповідні інструменти та засоби реалізації. Модель, сприятиме ефективному управлінню інформаційної безпеки та виступатиме методичним орієнтиром для подальшої оптимізації цифрового середовища підприємства (табл. 3.1).

Таблиця 3.1 – Фреймворк системи інформаційної безпеки суб'єктів малого підприємництва

Компонент (блок)	Функціональне призначення	Інструменти / технології	Сумісні продукти	Відповідні стандарти
Інтерфейс доступу	Надання авторизованого доступу до системи	Web-портал, Client app	Apache, Nginx, Remote Desktop	ISO/IEC 27002, OWASP
Система автентифікації (MFA)	Перевірка особи користувача	2FA, OTP, Biometric	Authy, Google Authenticator, Keycloak	NIST SP 800-63B
Керування доступом	Призначення прав доступу до об'єктів системи	ACL, RBAC, IAM	FreeIPA, Microsoft AD, LDAP	ISO/IEC 27001, NIST SP 800-53
Інформаційні ресурси	Дані, бази даних, документи	DBMS, документообіг	PostgreSQL, Nextcloud	ISO/IEC 27001
Моніторинг та аудит	Виявлення інцидентів безпеки, логування	SIEM, лог-сервери	Graylog, Wazuh, ELK	ISO/IEC 27035, NIST SP 800-92
Мережевий захист	Захист трафіку, фільтрація запитів	Firewall, IDS/IPS, VPN	pfSense, Snort, WireGuard	ISO/IEC 27033, NIST SP 800-41
Резервне копіювання та відновлення	Запобігання втраті даних, відновлення після інцидентів	Backup agents, Disaster Recovery Tools	Veeam, Duplicati, Acronis	ISO/IEC 27031, NIST SP 800-34
Політики та процедури	Формалізація правил ІБ	IS Policy templates, ISO Toolkits	Open Policy Agent (OPA), Doc Generator	ISO/IEC 27001 Annex A
Обізнаність персоналу	Зменшення людського чинника	Тренінги, курси, соціальні тести	KnowBe4, Coursera, Google Cybersecurity	ISO/IEC 27002, ISO/IEC 27005

Джерело: побудовано автором на основі [129-145].

Розробка ефективної системи інформаційної безпеки суб'єктів малого підприємництва потребує структурованого підходу, який поєднує як технічні, так і організаційні складові. Запропонований фреймворк базується на структурно-компонентному принципі, що передбачає виокремлення ряду блоків системи інформаційної безпеки з урахуванням їх функціонального призначення, відповідних технологій, рекомендованих інструментів і стандартів. Такий підхід дозволяє підприємствам гнучко адаптувати модель захисту під власні потреби, враховуючи обмежені ресурси, ризикове середовище та рівень цифрової зрілості.

Одним із базових компонентів є інтерфейс доступу, що забезпечує вхід користувача до системи. Це може бути веб-портал, локальний застосунок або інтерфейс віддаленого доступу. Безпечність цього етапу важлива, оскільки саме на ньому відбувається первинна ідентифікація. Для забезпечення надійної перевірки особи передбачено впровадження мультифакторної автентифікації (MFA) – зокрема, через технології двофакторної ідентифікації, одноразових паролів, біометрії тощо. Інструменти як Google Authenticator чи Keycloak дають змогу реалізувати цей рівень захисту навіть у малих організаціях.

Далі важливо реалізувати механізми керування доступами, які відповідають за контроль прав користувачів до інформаційних ресурсів. Застосування політик контролю доступу (ACL, RBAC, IAM) дозволяє структурувати обов'язки, мінімізуючи ризик несанкціонованого втручання. Сучасні системи на кшталт FreeIPA чи Microsoft Active Directory дають змогу централізовано управляти обліковими записами, ролями та доступами. На рівні інформаційних ресурсів, до яких відносяться бази даних, документи, внутрішні застосунки, доцільно використовувати системи управління базами даних (DBMS), такі як PostgreSQL, а також системи корпоративного документообігу, як Nextcloud.

Окремим напрямом є моніторинг і аудит, що включає виявлення інцидентів безпеки, збір та аналіз журналів подій. Інструменти типу SIEM або лог-сервери (Graylog, Wazuh, ELK) дозволяють оперативно реагувати на аномалії у функціонуванні системи, забезпечуючи цілісність інформаційного

середовища. Для захисту на рівні мережевої інфраструктури доцільно впроваджувати засоби мережевого захисту – це можуть бути VPN, міжмережеві екрани, IDS/IPS системи. Такі рішення, як «pfSense» чи «Snort», ефективно фільтрують трафік, запобігаючи атакам типу «людина посередині», DoS, SQL-ін'єкціям тощо.

Важливою складовою є система резервного копіювання та відновлення, яка дозволяє запобігти втраті важливої інформації у разі інциденту. Інструменти на кшталт Veeam або Duplicati забезпечують регулярне копіювання даних із можливістю їхнього швидкого відновлення, що підвищує загальну стійкість системи. Крім технічних елементів, важливо формалізувати політики та процедури інформаційної безпеки, які визначають правила доступу, дії при інцидентах, вимоги до паролів, політику резервного копіювання тощо. Використання шаблонів політик або платформ, як наприклад «Open Policy Agent» (OPA) дозволяє стандартизувати процеси інформаційної безпеки навіть у невеликих командах [146].

Окрему увагу слід приділити підвищенню обізнаності персоналу, оскільки саме людський чинник часто стає головним джерелом порушень безпеки. Проведення регулярних тренінгів, курсів та імітацій фішингових атак за допомогою платформ типу KnowBe4 дозволяє зменшити кількість внутрішніх інцидентів, пов'язаних із необережністю або незнанням працівників. Запропонований фреймворк охоплює як технічні, так і організаційні аспекти інформаційної безпеки, що дозволяє реалізувати повноцінну систему захисту в малому підприємстві, дотримуючись міжнародних стандартів та принципів ризик-орієнтованого підходу.

Отже, розробка структурно-компонентного фреймворку системи інформаційної безпеки для суб'єктів малого підприємництва дозволяє комплексно осмислити основні аспекти захисту інформаційного середовища, з урахуванням обмежених фінансових, технічних та кадрових ресурсів. Запропонована таблична модель дає змогу інтегрувати як технічні, так і організаційні компоненти безпеки в єдину цілісну систему, яка базується на

принципах адаптивності, масштабованості, функціональності та відповідності міжнародним стандартам. Застосування такого фреймворку спрощує процес прийняття рішень щодо впровадження необхідних технологій, забезпечує прозору і логічно структуровану побудову архітектури інформаційної безпеки, а також сприяє підвищенню загального рівня кіберстійкості підприємства. Таким чином, розроблений фреймворк може бути ефективним практичним інструментом як для оцінки наявного стану інформаційної безпеки, так і для проектування нових систем захисту в умовах цифрової трансформації малого бізнесу.

У сучасних умовах стрімкого розвитку цифрових технологій та посилення кіберзагроз ефективна система інформаційної безпеки стає необхідною складовою стабільного функціонування будь-якого підприємства, зокрема малого. Незважаючи на обмежені фінансові та кадрові ресурси, саме суб'єкти малого підприємництва дедалі частіше стають об'єктами атак через їхню вразливість, низький рівень формалізації процесів та недостатню зрілість систем захисту. У цьому контексті особливого значення набувають структуровані методологічні підходи до побудови архітектури інформаційної безпеки, які дозволяють забезпечити узгодженість захисних механізмів із загальними бізнес-цілями.

Одним із найпотужніших інструментів стратегічного проектування системи інформаційної безпеки суб'єктів малого підприємництва є TOGAF – загальновизнаний міжнародний стандарт архітектурного управління, який успішно використовується в різних сферах економічної діяльності. TOGAF переважно застосовується у великих організаціях, проте його адаптація до умов малого підприємництва дозволяє структурувати процес створення системи інформаційної безпеки, зробити його поетапним, контрольованим і результативним [147]. Пропонуємо фреймворк TOGAF застосувати для побудови ІБ-архітектури суб'єктів малого підприємництва, з урахуванням особливостей його ресурсного забезпечення, рівня цифрової зрілості та вимог до захищеності інформаційного середовища (рис. 3.2).

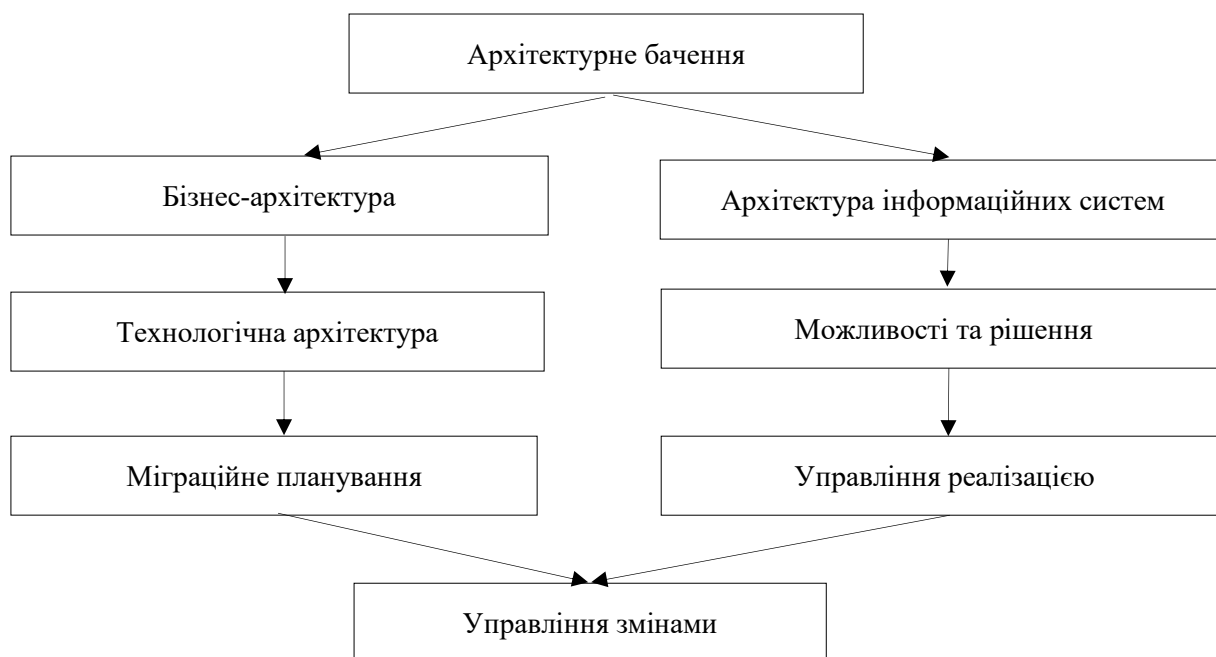


Рис. 3.3. Застосування TOGAF-підходу до побудови системи інформаційної безпеки суб'єктів малого підприємництва.

Джерело: побудовано автором на основі [130-132, 148-151].

Методологія TOGAF (The Open Group Architecture Framework), яка є загальновизнаним стандартом побудови архітектур підприємств, демонструє високу ефективність та може бути адаптована для суб'єктів малого підприємництва, зокрема у сфері інформаційної безпеки. Основою TOGAF є ADM (Architecture Development Method) – метод побудови архітектури, який передбачає послідовне проходження десяти фаз, кожна з яких має чітке функціональне навантаження, логіку реалізації та очікувані результати [152, 153]. Застосування цієї методики дозволяє перейти від фрагментарного підходу до системного управління інформаційною безпекою суб'єктів малого підприємництва, що особливо важливо в умовах зростання складності ІТ-середовища та кібервикликів.

Архітектурне бачення побудови системи інформаційної безпеки є відправною точкою, де формуються основні цілі та розуміння безпекової архітектури підприємства. Вона забезпечує стратегічне узгодження майбутньої системи інформаційної безпеки із загальними бізнес-цілями, акцентуючи увагу

на вартості безпеки для збереження операційної безперервності. Бізнес-архітектура системи інформаційної безпеки орієнтована на моделювання основних бізнес-процесів, виявлення інформаційних потоків, точок доступу до даних, а також визначення ролей і відповідальностей. На цьому етапі визначаються найвразливіші ланки бізнес-діяльності, які потребують пріоритетного захисту.

Архітектура інформаційних систем передбачає деталізацію застосованого і інформаційного рівнів, описуються структури баз даних, програмних рішень, внутрішніх і зовнішніх застосунків, а також визначаються відповідні контролю доступу, політики безпеки, автентифікація та шифрування. Після цього, на етапі формування технологічної архітектури, здійснюється вибір конкретних технічних засобів реалізації механізмів безпеки, включаючи засоби захисту периметра, VPN, засоби моніторингу, резервного копіювання тощо. Основною вимогою тут є адаптація інструментів до можливостей суб'єктів малого підприємництва з урахуванням економічної доцільності.

Фаза можливостей та рішень передбачає формування пакетів рішень, які інтегрують бізнес-вимоги з технологічними ресурсами, що дозволяє виробити чіткі рекомендації щодо пріоритетності впровадження окремих компонентів системи інформаційної безпеки. Фаза міграційне планування спрямована на поетапне впровадження рішень, визначення ресурсного навантаження, термінів та етапів реалізації. Особливо важливою вона є для суб'єктів малого підприємництва, де збої можуть спричинити серйозні наслідки. Тому, фреймворк передбачає мінімізацію ризиків за допомогою поступового переходу.

Фази управління реалізацією та управління змінами, забезпечують контроль за втіленням архітектурних змін, регулярне оцінювання ефективності впроваджених рішень та оновлення політик відповідно до нових загроз і змін у середовищі. Для суб'єктів малого підприємництва, це особливо актуально, оскільки навіть незначні технологічні зміни можуть порушити загальну систему безпеки [154]. Таким чином, TOGAF-орієнтований підхід дозволяє раціоналізувати процес побудови системи інформаційної безпеки та забезпечити

її стійкість, адаптивність та відповідність сучасним стандартам кіберзахисту. Застосування TOGAF у контексті малого бізнесу є інноваційним рішенням, що дозволяє поєднати структурованість корпоративної архітектури з гнучкістю малих організацій [155]. Такий підхід забезпечує технічну реалізацію інформаційної безпеки та формує управлінську культуру стратегічного підходу до інформаційної безпеки як до довгострокового активу підприємства.

Таким чином, застосування методології TOGAF у процесі формування системи інформаційної безпеки суб'єктів малого підприємництва дозволяє реалізувати цілісний, стратегічно орієнтований та адаптивний підхід до проектування архітектури інформаційної безпеки. Завдяки чіткому структуруванню фаз ADM-моделі, підприємство отримує змогу поетапно перейти від визначення потреб до впровадження технічних рішень та управління змінами в системі. Такий підхід забезпечує узгодженість безпекових ініціатив з бізнес-цілями, підвищує прозорість процесів, дозволяє ефективно розподіляти ресурси та знижує ризики впровадження. TOGAF-підхід сприяє побудові гнучкої, масштабованої та довготривалої системи інформаційної безпеки, що особливо важливо для малого бізнесу в умовах динамічного цифрового середовища та зростаючої кіберзагрози. Формування ефективної системи інформаційної безпеки на основі архітектурного підходу TOGAF створює передумови для забезпечення стабільності функціонування підприємств, підвищення їх конкурентоспроможності та адаптивності до сучасних викликів цифрової економіки. Такий підхід, сприяє зміцненню економічної безпеки суб'єктів малого підприємництва та забезпеченню їх довгострокового розвитку в умовах постійного зростання кіберризиків.

3.2. Методика проведення аудиту інформаційної безпеки підприємства

Аудит інформаційної безпеки є важливим елементом управління ризиками та забезпечення стійкості підприємства в умовах зростаючої кількості кіберзагроз. У сучасному інформаційному середовищі, де цифрові активи є

стратегічними ресурсами бізнесу, ефективність функціонування будь-якої організації значною мірою залежить від рівня захищеності її інформаційних систем. Проведення аудиту дозволяє виявити вразливості в політиках, процесах та технічних засобах захисту та оцінити відповідність чинним нормативним вимогам, корпоративним стандартам та міжнародним протоколам безпеки. Методика аудиту інформаційної безпеки формує комплексний підхід до діагностики стану інформаційної безпеки, включаючи аналіз ризиків, перевірку процедур доступу, оцінку програмного та апаратного забезпечення, а також аудит поведінки персоналу, що в сукупності забезпечує основу для подальшого вдосконалення захисної інфраструктури підприємства [156].

Аудит інформаційної безпеки доцільно розглядати як спосіб виявлення потенційних загроз та вразливих місць у конкретній організації шляхом застосування комплексу заходів, який дозволяє оцінити захищеність інформаційних систем та перевірити, чи відповідають вони чинним стандартам безпеки. Нині такими стандартами є ISO 27001 та ISO 27002, а також рекомендації загального регламенту захисту даних GDPR.

Проведення аудиту інформаційної безпеки, на нашу думку, є складовою системи забезпечення інформаційної безпеки підприємства. Такий процес дозволяє оцінити поточний стан захищеності інформаційних ресурсів та виступає важливим етапом у формуванні довгострокової політики кіберзахисту. У межах реалізації такої стратегії здійснюється системний моніторинг ризиків і відповідності нормативним вимогам, а також проводиться цілеспрямована підготовка кваліфікованих фахівців, організовується постійне професійне навчання персоналу, забезпечується придбання, впровадження та регулярне оновлення технічних засобів захисту [157]. Скоординоване виконання цих заходів забезпечує цілісність, конфіденційність та доступність критичної інформації, що є запорукою стабільної та безперебійної діяльності підприємства в цифровому середовищі.

Забезпечення інформаційної безпеки підприємства за характером організації та джерелом ініціації, передбачає проведення двох основних типів аудиту:

- *внутрішнього* – здійснюється власними силами підприємства на постійній або періодичній основі відповідно до внутрішніх нормативних документів, стандартів і процедур. Такий аудит проводиться для моніторингу відповідності поточних практик безпеки встановленим політикам, виявлення вразливостей та вдосконалення системи управління інформаційною безпекою з урахуванням специфіки організаційної структури;

- *зовнішнього* – реалізується незалежними фахівцями або спеціалізованими організаціями, які залучаються ззовні за ініціативою керівництва підприємства, власників, інвесторів або державних контролюючих органів. Аудитори діють на підставі договору та проводять об'єктивну оцінку відповідності інформаційної безпеки підприємства чинним стандартам, законодавчим вимогам або договірним зобов'язанням [158].

Ефективне управління інформаційною безпекою суб'єктів підприємництва, передбачає впровадження технічних рішень та системного оцінювання рівня захищеності з використанням інструментів аудиту. Аудит інформаційної безпеки підприємства дозволяє виявити слабкі місця в організаційній, процедурній і технологічній сферах, визначити актуальні ризики та сформулювати обґрунтовані рекомендації для їх мінімізації.

Пропонуємо візуально сформувати структуру аудиту інформаційної безпеки підприємства, яку розуміємо як багаторівневу систему, що охоплює як зовнішнє експертне оцінювання, так і внутрішній самоконтроль (рис. 3.4). Такий підхід забезпечує всебічне охоплення факторів, що впливають на стан захищеності підприємства, і дає змогу адаптувати заходи безпеки до реальних умов функціонування суб'єктів підприємництва.

Зовнішній аудит орієнтований на виявлення вразливостей у системі інформаційної безпеки підприємства з акцентом на економічну доцільність.

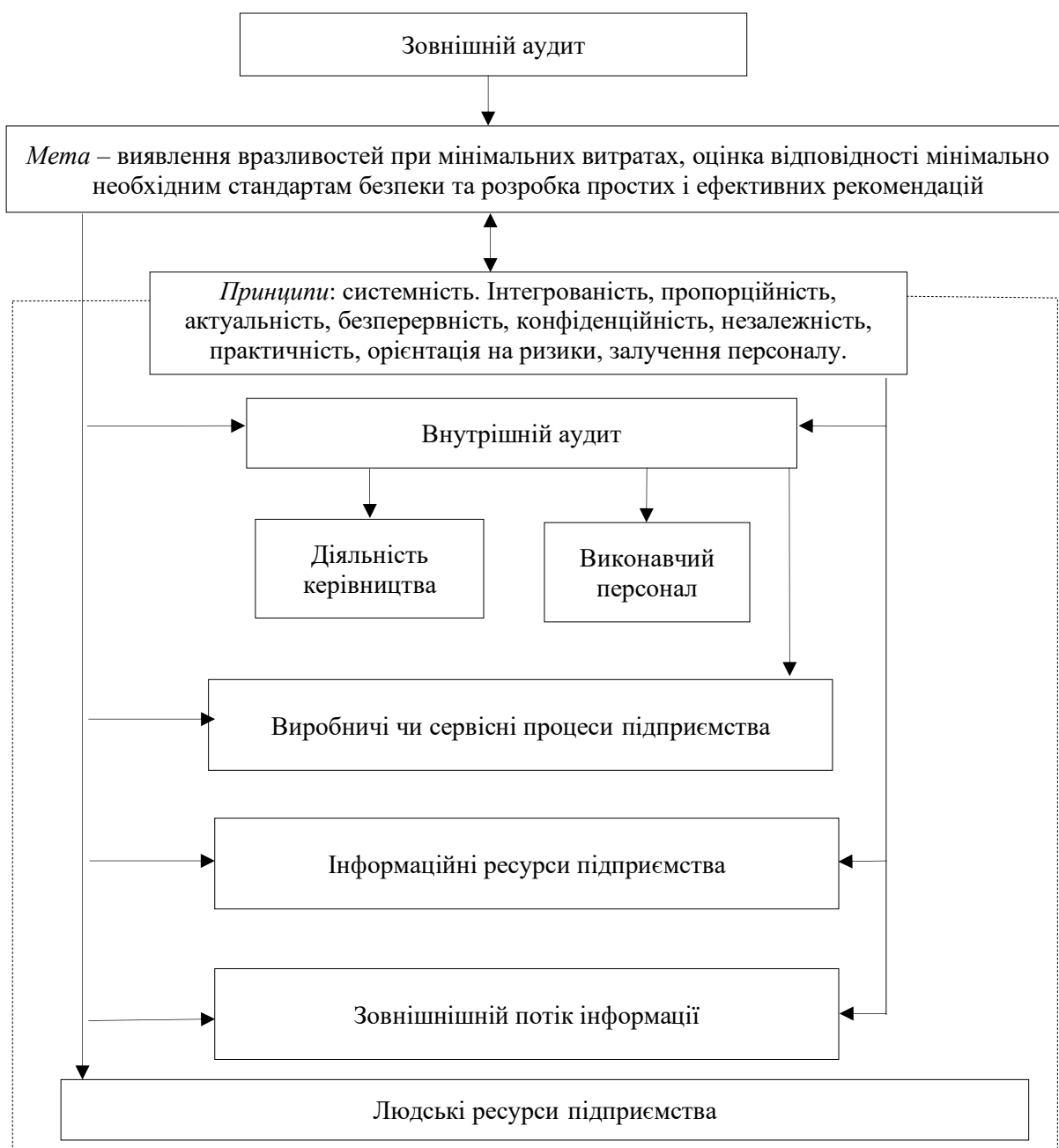


Рис. 3.4. Структура аудиту інформаційної безпеки підприємства.

Джерело: побудовано автором на основі [159-168].

Його мета полягає у мінімізації витрат під час досягнення базового рівня захищеності та формуванні простих і ефективних рекомендацій. До принципів аудиту віднесемо (додаток В1):

- системність – аудит повинен охоплювати всі рівні та елементи системи забезпечення інформаційної безпеки підприємства, від стратегічного управління до технічних засобів захисту;

- інтегрованість – аудит має враховувати взаємозв'язки між організаційними, технічними, кадровими та правовими компонентами системи забезпечення інформаційної безпеки підприємства;

- пропорційність (доцільність витрат) – масштаб та глибина аудиту мають відповідати розмірам підприємства, його ресурсним можливостям та рівню загроз (ля малого бізнесу – це аудит з акцентом на основні зони ризику);

- актуальність – методика повинна враховувати сучасні типи загроз (фішинг, соціальна інженерія, атак на постачальників тощо), а також актуальні міжнародні стандарти (ISO/IEC 27001, NIST, GDPR);

- безперервність – аудит не повинен бути одноразовим заходом, а має проводитися періодично або після суттєвих змін у структурі, технологіях чи зовнішньому середовищі підприємства;

- конфіденційність – усі результати аудиту мають використовуватись виключно у межах внутрішнього управління безпекою, а персонал, який його проводить, повинен дотримуватися політики нерозголошення;

- практичність – результати аудиту повинні бути подані у вигляді конкретних, реалістичних і пріоритетних рекомендацій, які можливо реалізувати на практиці в межах наявного бюджету;

- орієнтація на ризики – оцінювання рівня безпеки повинно ґрунтуватися на аналізі потенційних ризиків, вірогідності їх реалізації та можливих наслідків для підприємства;

- залучення персоналу – процес аудиту має бути комунікативним: персонал повинен брати участь у заповненні анкет, інтерв'ю та тестуванні, що підвищує об'єктивність оцінки;

- незалежність (для зовнішнього аудиту) – зовнішній аудит має здійснюватися об'єктивно, без конфлікту інтересів, із залученням незалежних експертів, які не беруть участі в діяльності підприємства.

Визначені принципи формують методологічну основу для проведення аудиту інформаційної безпеки, яка враховує як міжнародний досвід, так і специфіку українських підприємств, зокрема суб'єктів малого підприємництва.

Внутрішній аудит здійснюється ресурсами самого підприємства та має більш деталізований характер. До основних напрямів аудиту, які охоплюють діяльність керівництва та виконавчого персоналу, пропонуємо віднести: виробничі чи сервісні процеси, інформаційні ресурси, зовнішні потоки інформації та людські ресурси та їх діяльність. Така деталізація дозволяє охопити усі можливі вектори потенційних загроз, від управлінських рішень до технічного стану інформаційних систем і компетентності персоналу. Зокрема, аналіз діяльності керівництва передбачає оцінку політик безпеки, стратегічного бачення та контролю ризиків. Аудит виконавчого персоналу зосереджений на дотриманні процедур, рівні обізнаності та поведінкових чинниках. Аналіз інформаційних ресурсів включає перевірку захищеності баз даних, мереж, сервісів і програмного забезпечення.

Особливе значення має аналіз зовнішнього інформаційного потоку, який передбачає вивчення каналів комунікації з партнерами, споживачами, постачальниками тощо. Такі взаємодії часто є джерелом інформаційних ризиків. Діяльність персоналу як об'єкт аудиту розглядаються з позиції кваліфікаційного рівня працівників, наявності відповідної підготовки у сфері інформаційної безпеки, а також розробки впровадження політик найму, доступу до інформації та навчання персоналу [169]. Врахування взаємозв'язків між різними об'єктами аудиту забезпечує виявлення технічних вразливостей та організаційних, процедурних і поведінкових недоліків у системі захисту. Запропонована схема демонструє системний і структурований підхід до аудиту інформаційної безпеки, що дозволяє підприємству виявити слабкі місця в системі захисту та сформулювати ефективну стратегію забезпечення інформаційної безпеки суб'єктів малого підприємництва в умовах сучасного інформаційного середовища та адаптовану до поточних умов і можливостей організації.

Внутрішній аудит інформаційної безпеки здійснюється безпосередньо внутрішніми службами підприємства, зазвичай уповноваженими працівниками. Такий аудит має системний і регулярний характер та виконується згідно з

внутрішніми регламентами, стандартами або політиками підприємства. Внутрішній аудит дозволяє оперативно адаптувати заходи безпеки до змін внутрішнього середовища та враховувати стратегічні цілі підприємства [170]. Процес проведення внутрішнього аудиту інформаційної безпеки підприємства представлено на рис. 3.5.



Рис. 3.5. Процес проведення внутрішнього аудиту інформаційної безпеки підприємства

Джерело: побудовано автором.

Зовнішній аудит інформаційної безпеки здійснюється незалежними експертами, спеціалізованими аудиторськими компаніями або за дорученням сторонніх ініціаторів (керівництва, наглядових органів, інвесторів). Такий аудит має об'єктивний характер, оскільки сторонній аудитор не залежить від внутрішньої структури підприємства. Згідно з наведеною схемою, зовнішній аудит охоплює усю підприємницьку діяльність суб'єкта господарювання, здійснюючи перевірку відповідності стандартам (наприклад, ISO/IEC 27001), вимогам регуляторів або умовам контрактів. Зовнішні аудиторі аналізують і внутрішні процеси і зовнішнє економіко-правове середовище, що дозволяє оцінити ризики інформаційної безпеки в ширшому контексті, включно з

галузевими, державними та міжнародними вимогами. Зміст зовнішнього аудиту інформаційної безпеки підприємства представлено на рис. 3.6.



Рис. 3.6. Зміст зовнішнього аудиту інформаційної безпеки підприємства

Джерело: побудовано автором.

У межах методики забезпечення інформаційної безпеки підприємства виокремлюються різні види зовнішнього аудиту, кожен з яких має свою специфіку та призначення. Зовнішній аудит може виконуватись у формі незалежної експертної оцінки загального стану інформаційної безпеки або ж у вигляді офіційної процедури сертифікації, що базується на відповідності чинним стандартам (наприклад, ISO/IEC 27001, NIST, COBIT тощо). Такий аудит проводиться спеціалізованими зовнішніми організаціями або консалтинговими компаніями з метою об'єктивного аналізу ефективності системи захисту, виявлення вразливостей, формулювання рекомендацій щодо їх усунення, а також, у разі сертифікації – офіційного визнання рівня інформаційної безпеки підприємства [171]. Зазначимо, що зовнішній аудит часто ініціюється

внутрішніми потребами та вимогами партнерів, інвесторів або державних регуляторів.

Об'єкти перевірки інформаційної безпеки в межах зовнішнього аудиту охоплюють найважливіші компоненти цифрової інфраструктури підприємства. Насамперед оцінюється стабільність бізнес-процесів і сервісів, що передбачає перевірку їх здатності функціонувати в умовах кіберзагроз. Важливим напрямом є ідентифікація вразливостей IT-інфраструктури, які можуть бути використані зловмисниками для порушення цілісності або доступності систем. Значну увагу доцільно приділити стійкості та захищеності інформаційних ресурсів, які є об'єктом потенційних атак. Крім того, доцільно перевірити швидкість реагування на зовнішній негативний інформаційний вплив та ефективність механізмів інцидент-менеджменту, виявити ризики несанкціонованого доступу третіх осіб до корпоративних даних, особливо через вразливі зовнішні канали комунікації [172]. Сукупність цих об'єктів перевірки дозволяє забезпечити репрезентативне оцінювання рівня інформаційної безпеки підприємства.

Отже, комплексне поєднання внутрішнього та зовнішнього аудиту формує ефективну систему контролю за інформаційною безпекою підприємства. Внутрішній аудит забезпечує оперативність, гнучкість і адаптацію до внутрішніх процесів, у той час як зовнішній аудит гарантує об'єктивність, відповідність зовнішнім стандартам і нормативам, а також надає незалежну оцінку кіберстійкості підприємства [173].

Важливою складовою аудиту є процес перевірки та методологія збору достовірних і релевантних доказів, на основі яких будуть формуватись висновки. В умовах обмежених ресурсів, особливо в секторі малого та середнього бізнесу, надзвичайно важливо застосовувати чітко визначені критерії, що дозволяють ефективно ідентифікувати як впроваджені дії в межах системи інформаційної безпеки, так і реальні результати їх впливу. Такий підхід забезпечує об'єктивність оцінювання, підвищує якість аудиторських рішень і формує основу для прийняття стратегічно важливих управлінських рішень у сфері інформаційної безпеки. Критерії збору аудиторських доказів щодо об'єкту

«інформаційна безпека» в контексті ідентифікації дій та результатів систематизовано в таблиці 3.2.

Таблиця 3.2 – Критерії збору аудиторських доказів щодо об'єкту «інформаційна безпека» в контексті ідентифікації дій та результатів

Категорія	Критерій	Приклад реалізації
Ідентифікація дій	Наявність політик та процедур	Документи з ІБ-політиками, правилами доступу, резервного копіювання тощо
	Встановлені технічні засоби захисту	Антивіруси, фаєрволи, системи контролю доступу
	Підготовка персоналу	Навчання, інструктажі, тести на обізнаність щодо кіберзагроз
	Аудит логів подій	Журнали спроб входу, зміни конфігурації систем
	Функціонування ІТ-служби	Наявність відповідальних осіб/підрядників з безпеки
	Оновлення ПЗ	Регулярність встановлення оновлень і патчів
Ідентифікація результатів	Зменшення інцидентів	Статистика скорочення кількості атак або збоїв
	Результати тестування на проникнення	Рівень виявлених уразливостей та їх усунення
	Відповідність стандартам	ISO/IEC 27001, GDPR, локальні нормативи
	Безперервність бізнес-процесів	Успішне перемикавання на резервні системи
	Результати сертифікації	Позитивний висновок зовнішніх аудиторів
	Оцінка обізнаності персоналу	Анкетування, контрольні завдання щодо ІБ

Джерело: визначено автором.

Визначені критерії відображають системний підхід до збору аудиторських доказів у процесі оцінювання інформаційної безпеки підприємства. Вони структуровані за двома основними категоріями: ідентифікація дій, що демонструють фактичне впровадження заходів інформаційної безпеки та ідентифікація результатів, які свідчать про ефективність цих заходів у практичному вимірі. До першої категорії віднесемо такі критерії, як: наявність формалізованих політик, функціонування технічних засобів захисту, навчання персоналу, аудит логів подій, регулярність оновлення програмного забезпечення тощо. Зазначені критерії дозволяють аудитору підтвердити, що підприємство активно впроваджує базові та спеціалізовані заходи безпеки в свою діяльність [174].

Другий блок критеріїв орієнтований на оцінку досягнутого ефекту від реалізованих заходів. До такої категорії віднесемо такі критерії, як: показники зменшення інцидентів безпеки, результати тестувань на проникнення, відповідність міжнародним стандартам, наявність сертифікацій, рівень обізнаності персоналу та здатність підприємства забезпечити безперервність критичних бізнес-процесів. Такі критерії мають надзвичайно важливе значення, оскільки дозволяють формально оцінити відповідність та визначити реальну ступінь інформаційної безпеки підприємства. Такий підхід підвищує достовірність аудиту, сприяє виявленню слабких місць і формує надійну основу для прийняття стратегічних рішень у сфері інформаційної безпеки.

У теоретично ідеальному економічному середовищі, аудит інформаційної безпеки підприємства мав би бути невід'ємною складовою діяльності кожного суб'єкту господарювання, де можливість втрати даних чи порушення доступності бізнес-процесів та сервісів загрожує істотними фінансовими збитками та іміджевими втратами. Аудит дозволяє вчасно виявляти вразливості, попереджати кіберінциденти та підвищувати загальний рівень інформаційної стійкості суб'єкта підприємництва [175]. Проте у практичних умовах регулярні перевірки інформаційної безпеки здебільшого впроваджуються великими корпораціями та, дещо меншою мірою, середніми підприємствами, що зумовлено їхніми фінансовими ресурсами, жорсткішими нормативними вимогами, а також наявністю спеціалізованих ІТ-підрозділів або відділів кіберзахисту. Крім того, представники малого бізнесу нерідко ігнорують такі заходи через обмеженість бюджету, недостатнє усвідомлення загроз або переконання, що їхні інформаційні ресурси не становлять інтересу для зловмисників. Така позиція формує оманливе відчуття безпеки, яке в умовах ускладнення кібератак може призвести до серйозних наслідків. У зв'язку з цим особливого значення набуває застосування адаптованих під потреби малого бізнесу підходів до оцінювання інформаційних ризиків, що забезпечують базовий рівень захищеності та дозволяють визначити пріоритетні заходи реагування навіть за обмежених фінансових можливостей.

Вихідні дані для аудиту інформаційної безпеки суб'єктів малого підприємництва визначено в таблиці 3.3.

Таблиця 3.3 – Вихідні дані для аудиту інформаційної безпеки суб'єктів малого підприємництва

Категорія даних	Приклади вихідних даних	Джерело отримання
Організаційна документація	Статут, організаційна структура, внутрішні регламенти	Внутрішні документи підприємства
Політики інформаційної безпеки	Політика управління паролями, політика контролю доступу, політика реагування на інциденти, інструкції, протоколи реагування	Локальні нормативні акти
Інформаційна інфраструктура	Опис серверів, робочих станцій, мережевого обладнання, картографія, баз даних, ІТ-мереж	Інвентаризація, технічна документація
Облікові записи та права доступу, журнали подій та лог-файли	Списки облікових записів користувачів, ролі, права доступу до систем і ресурсів	Системні журнали, звіти служби підтримки
Звіти про інциденти безпеки	Реєстр виявлених інцидентів, хронологія подій, звіти про витоки	Внутрішні документи підприємства
Результати попередніх аудитів	Документація з попередніх перевірок, результати аналізів ризиків, виконані рекомендації	Звіти
Контракти з ІТ-провайдером	Договори з постачальниками хмарних сервісів, технічна підтримка, SLA	Договірна документація
Кадрові ресурси	Інформація про компетенції співробітників, навчання з ІБ	HR-документація, звіти про навчання
Фінансові ресурси на ІБ	Бюджетні статті, витрати на ІБ	Фінансові звіти, бюджет підприємства
Оцінка ризиків	Результати попередніх оцінок ризиків або їх відсутність	Звіти, опитування персоналу

Джерело: удосконалено автором на основі [62, 160, 176-178].

Проведення якісного аудиту інформаційної безпеки потребує ґрунтовного збору вихідних даних, які дозволяють оцінити поточний стан захисту інформаційних ресурсів підприємства. Перш за все, аудитор повинен мати доступ до організаційної документації, яка включає установчі документи, внутрішню структуру підприємства, розподіл відповідальності та чинні регламенти роботи. Такі документи дозволяють зрозуміти рівень формалізації управлінських процесів і наявність контрольних механізмів [179].

Важливим є наявність політик інформаційної безпеки, що визначають правила поводження з інформацією, порядок контролю доступу, вимоги до паролів, заходи реагування на інциденти, правила використання ІТ-ресурсів тощо. Такі документи мають бути затверджені на рівні керівництва і регулярно оновлюватися відповідно до змін нормативного середовища або ризиків. Основним об'єктом аудиту є інформаційна інфраструктура підприємства, тобто перелік технічних засобів (сервери, маршрутизатори, комп'ютери), мережеві карти, топології, схеми доступу та інші компоненти. Аудитору необхідно перевірити наявність оновлень програмного забезпечення, антивірусного захисту, а також ізольованість критичних сегментів мережі.

Облікові записи та системи доступу включають перелік користувачів, їхні ролі та повноваження, а також журнали входу до систем і доступу до ресурсів. Аудит вимагає перевірки дотримання принципу мінімального доступу та регулярності перегляду прав користувачів. Невід'ємним джерелом інформації є журнали подій та лог-файли, які дають змогу виявити спроби несанкціонованого доступу, підозрілу активність або помилки в роботі систем. Разом з цим необхідно проаналізувати звіти про інциденти безпеки, що містять дані про порушення, вжиті заходи, строки реагування та усунення загроз.

Для порівняння динаміки безпеки та ефективності змін аудитор враховує результати попередніх аудитів, рекомендації, звіти про реалізацію заходів і результати аналізу ризиків. Також важливо переглянути контракти з ІТ-провайдерами, включаючи умови обслуговування, SLA, політики збереження даних, щоб перевірити відповідність третіх сторін політикам безпеки підприємства. Додатково аналізується штатна структура ІТ-підрозділів, кваліфікація персоналу, їхня обізнаність у питаннях кібербезпеки та результати навчання. Останньою, але не менш важливою категорією є система резервного копіювання, її періодичність, цілісність, безпечність і можливість відновлення даних після збою або атаки.

Шкала оцінки рівня збитку суб'єктів малого підприємництва, представлена в таблиці 3.4.

Таблиця 3.4 – Шкала оцінки рівня збитку

Рівень збитку	Наслідки	Впливу на підприємство
Незначний	Втрати незначні, не впливають на виконання основних функцій. Можливе порушення допоміжних процесів.	Локальні порушення. Не вимагає суттєвих витрат на усунення. Не має впливу на зовнішніх контрагентів.
Помірний	Часткове порушення бізнес-процесів. Обмеження в роботі окремих підрозділів.	Можливе зниження продуктивності, незначні фінансові втрати, потребує втручання ІТ-служби.
Відчутний	Суттєві порушення процесів управління, збої в обробці критичних даних, втрата певної кількості інформації.	Відчутний вплив на репутацію, збільшення витрат на відновлення, порушення договірних зобов'язань.
Серйозний	Зупинка основних бізнес-функцій, масова втрата або викрадення інформації, порушення безперервності діяльності.	Значні фінансові втрати, репутаційні ризики, втручання керівництва та зовнішніх регуляторів.
Критичний	Повна втрата керованості, повний вихід із ладу ІТ-систем, серйозні юридичні наслідки.	Довготривала зупинка діяльності, незворотні втрати, загроза існуванню підприємства.

Джерело: доповнено автором на основі [62, 180-185].

Оцінка рівня збитку, що може бути завданий підприємству внаслідок порушення інформаційної безпеки, є важливою складовою ризик-орієнтованого підходу до управління інформаційною безпекою. У статті Роя Я.В., Мазура Н.П. та Складанного П.М. запропоновано шкалу оцінки збитків, яка дозволяє класифікувати наслідки кіберінцидентів залежно від їх впливу на бізнес-процеси, репутацію, фінансову стабільність та загальну життєздатність підприємства [62].

Незначний рівень збитку характеризується локальними порушеннями, які не мають системного впливу на основну діяльність підприємства. Такі інциденти, як правило, не потребують великих витрат для усунення наслідків та не зачіпають критичну інформацію. Їх наслідки обмежуються внутрішнім середовищем підприємства. Помірний рівень збитку передбачає часткове порушення роботи окремих підрозділів або тимчасове зниження ефективності виконання бізнес-функцій, що може включати короточасні збої в роботі систем управління, потребу в технічному втручанні ІТ-фахівців, незначні втрати даних або уповільнення обробки інформації. На відчутному рівні, відбувається істотне

порушення бізнес-процесів, що може супроводжуватися втратою частини критичних даних, затримками в обслуговуванні клієнтів, невиконанням зобов'язань перед контрагентами. У такому разі підприємство може зазнати репутаційних втрат, а також вимушене нести додаткові витрати на компенсацію чи відновлення. Серйозний рівень, характеризується зупинкою основних бізнес-функцій, компрометацією або масовою втратою важливої інформації, а також значними матеріальними збитками. Такі ситуації часто супроводжуються втручанням вищого керівництва, юридичних підрозділів та, можливо, зовнішніх органів контролю. Критичний рівень передбачає катастрофічні наслідки для підприємства: повну втрату керованості, виведення з ладу основних ІТ-систем, юридичні ускладнення та незворотні наслідки, які можуть поставити під загрозу саме існування організації. Такий сценарій є найнебезпечнішим і потребує максимальної уваги в системах аудиту та управління інформаційною безпекою. Запропонований підхід дозволяє якісно оцінити можливий збиток та сформувані обґрунтовані сценарії реагування та пріоритизації захисних заходів залежно від критичності виявлених загроз.

Визначенв шкала оцінки ймовірності атаки на суб'єкти малого підприємництва представлена в таблиці 3.5.

Таблиця 3.5 – Шкала оцінки ймовірності атаки

Рівень ймовірності	Опис ймовірності	Умови реалізації загрози
Дуже низький	Ймовірність атаки практично відсутня	Загроза відома, але її реалізація потребує значних ресурсів або малоімовірних умов. Система має високий рівень захисту.
Низький	Атака можлива за наявності специфічних умов	Існують поодинокі вразливості, реалізація можлива лише за глибокого знання внутрішнього середовища.
Середній	Атака є потенційно реальною	Відомі вразливості, є зацікавлення об'єктом, рівень захисту частково адекватний.
Високий	Атака ймовірна при помірних зусиллях	Наявні критичні уразливості, низький рівень контролю, зловмисники мають мотивацію.
Дуже високий	Атака майже гарантована	Критичні вразливості відкриті, немає належного захисту, об'єкт має високу цінність для атакуючих.

Джерело: доповнено автором на основі [62, 180-185].

Оцінка ймовірності реалізації загроз є важливою складовою аудиту інформаційної безпеки, оскільки дозволяє визначити ступінь ризику виникнення

атаки на інформаційну систему підприємства. У низці досліджень, запропоновано шкалу ймовірності атаки, яка дозволяє ранжувати потенційні загрози за п'ятибальною шкалою, від дуже низької до дуже високої ймовірності. Кожен рівень у такій класифікації супроводжується характеристикою умов, за яких може відбутися атака [62].

На дуже низькому рівні ймовірності атака практично не може бути реалізована без надзвичайно складної підготовки або малоймовірних зовнішніх обставин. У такому випадку система зазвичай має високий рівень захисту, а вразливості або відсутні, або маловідомі. Такий рівень передбачає мінімальний ризик і не потребує негайного втручання, але вимагає періодичного моніторингу. Низький рівень ймовірності вказує на те, що атака можлива лише за наявності специфічних умов, наприклад, знання внутрішньої архітектури системи або наявності слабко задокументованих вразливостей. У таких ситуаціях загроза існує, але її реалізація малоймовірна без цілеспрямованих і технічно складних дій злоумисника. При середньому рівні ймовірності атаки зростає, оскільки існують відомі вразливості, а об'єкт потенційно становить інтерес для атакуючих. Захист є частково ефективним, однак має прогалини, які можуть бути використані вразливими місцями. Такий рівень передбачає необхідність вдосконалення політик безпеки та перевірки конфігурацій. Високий рівень ймовірності означає, що атака може бути реалізована при відносно помірних зусиллях. Уразливості легко виявити або вони вже експлуатуються в аналогічних системах. Об'єкт атаки є привабливим, а засоби захисту – недостатні. У такому випадку підприємство має терміново реагувати на ризики шляхом посилення контролю доступу, оновлення ПЗ або впровадження засобів моніторингу. Дуже високий рівень ймовірності свідчить про фактичну відкритість системи до атак. Критичні вразливості не закриті, рівень захисту є мінімальним або взагалі відсутній, а сам об'єкт становить значну цінність для злоумисників – фінансову, політичну або технологічну. У таких умовах атака фактично є питанням часу, і ймовірність її реалізації наближається до 100%. Застосування такої якісної шкали дозволяє формалізувати оцінку ризиків у процесі аудиту та приймати

обґрунтовані управлінські рішення щодо пріоритетності впровадження засобів захисту, зосередження ресурсів на найвразливіших ділянках системи та підвищення загальної кіберстійкості підприємства [186].

Проведене дослідження дозволило обґрунтувати методичний підхід до аудиту інформаційної безпеки підприємства як комплексної процедури, що поєднує зовнішнє та внутрішнє оцінювання, охоплюючи при цьому всі основні елементи інформаційної інфраструктури, бізнес-процесів і управлінських рішень. Запропонована структура аудиту забезпечує системність, адаптивність і орієнтацію на ризики, що є особливо важливим у сучасному інформаційно насиченому середовищі, де підприємства стикаються з постійними загрозами цифрового характеру.

Запропоновані принципи аудиту, критерії збору аудиторських доказів та індикатори результативності дозволяють перетворити процес аудиту з формальної перевірки на дієвий інструмент стратегічного управління безпекою. Важливим аспектом є чіткий поділ між ідентифікацією дій (регламентів, технічних заходів, інструктажів) та ідентифікацією результатів (реальне зниження ризиків, підвищення обізнаності, відповідність стандартам), що забезпечує підвищення точності оцінювання. Таким чином, запропонована методика аудиту може бути ефективно адаптована як для великих підприємств, так і для малого бізнесу, який потребує простих, економічно обґрунтованих і практично орієнтованих рішень у сфері інформаційної безпеки.

3.3 Стратегічні орієнтири розвитку системи забезпечення інформаційної безпеки суб'єктів малого підприємництва

Особливість малого підприємництва полягає в обмежених ресурсах, гнучкості управління, вузькому колі компетенцій, а також високій залежності від людського чиннику. Такі характеристики значною мірою ускладнюють застосування типових моделей інформаційної безпеки, орієнтованих на великі корпорації. Більше того, малі підприємства часто не усвідомлюють критичності

інформаційної безпеки або не мають чіткої стратегії щодо її забезпечення, що підвищує їхню вразливість до зовнішніх атак, внутрішніх порушень або непередбачуваних технічних збоїв [187]. У цьому контексті стратегічний підхід, адаптований до потреб, масштабів і можливостей малого бізнесу, постає як важлива передумова ефективного захисту його цифрових активів та інформаційних ресурсів.

Незважаючи на наявність окремих методичних рекомендацій, сучасна наукова думка ще не сформувала комплексної моделі стратегічного управління інформаційною безпекою суб'єктів малого підприємництва з урахуванням національного та регіонального контексту. Сьогодні актуальними залишаються питання розробки адаптивних стратегій, які б включали інституційні, технологічні та освітні компоненти, орієнтовані на мінімізацію ризиків за умов обмеженості ресурсів [187]. Проведений аналіз засвідчив, що важливими є публічно-приватні ініціативи, цифрова інклюзія та розбудова локальних екосистем безпеки, що дозволяють суб'єктам малого підприємництва об'єднуватися, отримувати доступ до знань, сервісів та інфраструктури інформаційного захисту. Необхідність наукового дослідження формування та реалізації стратегій інформаційної безпеки суб'єктів малого підприємництва зумовлена як викликами цифрового середовища, так і потребою в нових управлінських підходах, які забезпечать довготривалу стійкість, гнучкість і конкурентоспроможність малого бізнесу в цифрову епоху.

Аналіз досліджуваної проблеми засвідчив, що у більшості випадків суб'єкти малого підприємництва не мають фахівців з кібербезпеки, працюють на основі стандартного програмного забезпечення та не впроваджують формалізованих політик безпеки. Така ситуація створює ризики як для самих підприємств так і для їх споживачів і партнерів, що робить проблему інформаційної безпеки системною. Тому, суб'єктам малого підприємництва, необхідно впроваджувати гнучкі, адаптивні та поетапні стратегії захисту, що враховують їх поточний стан захищеності. Відсутність системного підходу призводить до накопичення ризиків, втрат комерційної інформації та зниження

конкурентоспроможності [188]. У зв'язку з цим, актуальним є поділ підприємств за рівнями інформаційної безпеки та відповідне стратегічне планування, що дозволяє раціонально розподілити ресурси та підвищити стійкість до кіберзагроз. Зважаючи на проведені дослідження, суб'єктам малого підприємництва доцільно використовувати адаптовані стратегії інформаційної безпеки, виходячи з визначених рівнів їхньої відносної захищеності. Систематизовані характеристики кожного рівня, рекомендовані стратегії та основні управлінські дії представлено в таблиці 3.6.

Таблиця 3.6 – Стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва залежно від поточного рівня інформаційної безпеки

Поточний рівень ІБ	Характеристика стану ІБ	Рекомендована стратегія	Рекомендовані дії
Низький	Відсутність системного підходу до розвитку ІБ, низька обізнаність персоналу, високі ризики	Стратегія базового захисту	Встановлення базового антивірусу, навчання працівників, регулярні резервні копії
Середній	Наявні окремі заходи захисту, політики ІБ фрагментарні, недостатній технічний контроль	Стратегія формування системи ІБ	Розробка політики безпеки, аудит поточних засобів, мінімізація вразливостей
Достатній	Формалізовані політики безпеки, регулярне оновлення ПЗ, частковий моніторинг	Стратегія оптимізації і контролю	Впровадження систем моніторингу, періодичне тестування захищеності, розмежування прав доступу
Високий	Повноцінна система управління ІБ, аудит, інтеграція ІБ у бізнес-процеси	Стратегія інтеграції та розвитку	Автоматизація процедур безпеки, зовнішній аудит, інвестиції у кіберстійкість

Джерело: визначено автором.

Аналіз процесу управління інформаційною безпекою суб'єктів малого підприємництва засвідчив важливість врахування специфіки ресурсного, організаційного та кадрового потенціалу досліджуваних суб'єктів господарювання. Тому, вибір стратегії забезпечення інформаційної безпеки доцільно здійснювати на основі поточного рівня захищеності, адаптуючи підходи до реалій малого бізнесу. Суб'єкти малого підприємництва з низьким рівнем інформаційної безпеки характеризуються повною відсутністю системного підходу, низькою обізнаністю працівників, відсутністю навіть базових технічних засобів захисту (антивірусів, фаєрволів) та високими ризиками витоку або втрати даних [189]. У таких умовах пропонуємо

застосовувати стратегію базового захисту, головна мета якої – якнайшвидше знизити критичні загрози. До основних дій належать: впровадження мінімально необхідного ПЗ для захисту, організація резервного копіювання даних, а також підвищення обізнаності персоналу шляхом коротких тренінгів або інструктажів.

Суб'єкти підприємництва з середнім рівнем інформаційної безпеки характеризуються фрагментарним впровадженням відповідних заходів, де зазвичай, деякі засоби вже працюють (наприклад, обмежений контроль доступу або використання антивірусу), але загальна політика безпеки не систематизована, а ризики залишаються значними [190]. Для цього рівня підходить стратегія формування системи інформаційної безпеки, яка передбачає проведення внутрішнього або зовнішнього аудиту наявної ситуації, створення політики інформаційної безпеки підприємства, мінімізацію виявлених вразливостей та підвищення технічної грамотності співробітників.

Достатній рівень інформаційної безпеки суб'єктів підприємництва свідчить про те що, підприємство вже має формалізовану політику безпеки, здійснює оновлення програмного забезпечення та резервне копіювання, контролює доступ до ресурсів, однак рівень автоматизації або моніторингу ще не є високим [191]. У цьому випадку доцільно впроваджувати стратегію оптимізації і контролю, яка орієнтована на регулярний аналіз ефективності наявних рішень, застосування систем моніторингу активності (наприклад, логування подій), а також сегментацію доступу до важливих даних за принципом мінімального привілею.

Високий рівень інформаційної безпеки суб'єктів підприємництва передбачає наявність сформованої системи інформаційної безпеки, її відповідність національним або міжнародним стандартам (зокрема ISO/IEC 27001), регулярний аудит та інтеграцію процесів інформаційної безпеки у загальну бізнес-стратегію [192]. У таких умовах найбільш ефективною буде стратегія інтеграції та розвитку, що фокусується на вдосконаленні поточних рішень, автоматизації процесів, впровадженні кіберстійких підходів, а також залученні зовнішніх експертів або участі в галузевих ініціативах з кіберзахисту.

Таким чином, поетапне просування від базового захисту до стратегічного управління інформаційною безпекою є реалістичним шляхом для малих підприємств. Він забезпечує відповідність регуляторним вимогам та підвищення конкурентоспроможності за рахунок надійного захисту інформаційних активів.

Визначена рівнева класифікація інформаційної безпеки суб'єктів малого підприємництва дозволяє сформулювати адаптивну стратегію управління, що відповідає поточному стану захищеності та ресурсним можливостям бізнесу. Кожен із чотирьох рівнів, від низького до високого, потребує специфічного підходу: від впровадження базових технічних засобів і навчання персоналу до інтеграції інформаційної безпеки у стратегічне управління та цифрову трансформацію підприємства. Такий диференційований підхід забезпечує поступове зниження ризиків та формує основу для стійкого розвитку суб'єктів малого підприємництва в умовах зростаючої кіберзагрозової активності та цифрової економіки.

Стратегічне управління інформаційною безпекою суб'єктів малого підприємництва потребує системного і комплексного підходу, який поєднує місію, бачення, аналіз зовнішнього та внутрішнього середовища, формування цілей, визначення стратегічних ініціатив, впровадження, контроль та інноваційний розвиток [193].

Система побудови стратегії забезпечення інформаційної безпеки суб'єктів підприємництва представлена на рис. 3.7.

У запропонованій моделі визначено логічну послідовність етапів формування стратегії, яка базується на сучасних концепціях стратегічного менеджменту, цифрової трансформації та ризик-орієнтованого мислення, що загалом являє собою інклюзивне інституційне забезпечення досліджуваних процесів. Першим етапом є визначення місії та бачення розвитку системи забезпечення інформаційної безпеки, що дозволяє окреслити довгострокові орієнтири підприємства у сфері інформаційної безпеки.

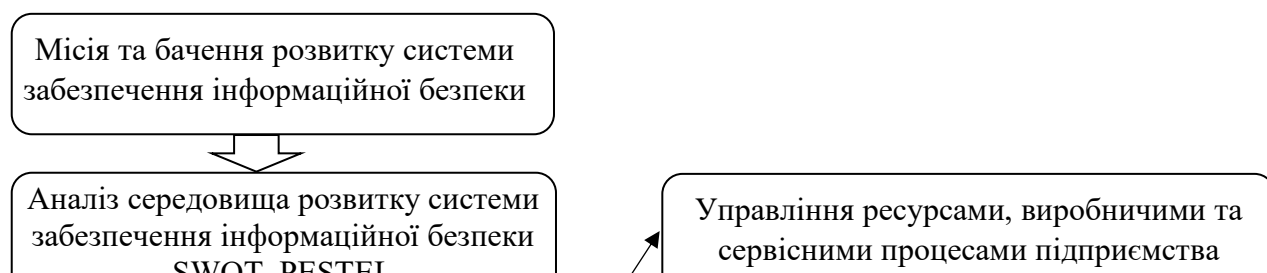


Рис. 3.7. Система побудови стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва.

Джерело: удосконалено автором на основі [186, 191, 194, 195].

Місія відображає основне призначення системи – збереження конфіденційності, цілісності та доступності інформаційних активів, а бачення формує уявлення про бажаний стан системи інформаційної безпеки у перспективі.

Другим етапом є аналіз середовища функціонування системи інформаційної безпеки, що здійснюється з використанням таких інструментів, як SWOT-аналіз (визначення сильних і слабких сторін, можливостей та загроз) та PESTEL-аналіз (оцінка політичних, економічних, соціальних, технологічних, екологічних і правових чинників). Такий підхід дозволяє адаптувати стратегію до реального контексту функціонування суб'єктів малого підприємництва, виявити бар'єри та драйвери цифрової безпеки.

На основі аналітичної оцінки формуються цілі та завдання системи інформаційної безпеки, які мають бути конкретними, вимірюваними, досяжними, релевантними та обмеженими в часі (SMART). Цілі охоплюють як превентивні заходи (запобігання інцидентам), так і реактивні (оперативне реагування та відновлення), а також стратегічні – інтеграцію інформаційної безпеки у загальну систему управління підприємством.

Стратегічні напрями та ініціативи визначають вектори дій для досягнення поставлених цілей. Сюди належать розробка політик безпеки, впровадження навчальних програм, вибір технологічних рішень, побудова партнерських мереж тощо. Важливо, що стратегічні напрями мають бути узгоджені з конкурентною стратегією підприємства, адже інформаційна безпека все частіше розглядається як чинник конкурентоспроможності.

Особливу увагу доцільно приділити інноваціям у сфері інформаційної безпеки, які передбачають впровадження новітніх технологій (AI, Big Data, Zero Trust), адаптацію до змін у цифровому середовищі, розвиток інституційних форм підтримки (наприклад, ІБ-кластерів). Зазначене пропонуємо доповнити цифровізацією виробничих і сервісних процесів, що вимагає відповідних механізмів захисту цифрових платформ, даних споживачів і транзакцій.

У практичному аспекті реалізації стратегії значущим є компонент управління ресурсами, включаючи кадрові, фінансові та технічні ресурси, необхідні для функціонування системи інформаційної безпеки, що також передбачає впровадження механізмів контролю результативності, зокрема моніторинг KPI, регулярні аудити та оцінку ефективності прийнятих рішень.

Завершальним етапом стратегічного циклу є управління ризиками та змінами, що дозволяє підтримувати гнучкість системи інформаційної безпеки, швидко адаптуватися до нових загроз і переглядати політики безпеки відповідно до змін у внутрішньому або зовнішньому середовищі. Цей етап забезпечує життєздатність стратегії та її динамічну відповідність викликам цифрової епохи.

Таким чином, запропонована система побудови стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва є логічно цілісною,

адаптованою до сучасних умов ведення бізнесу та орієнтованою на результат. Її впровадження сприятиме підвищенню рівня захищеності МП та формуванню довіри з боку споживачів, партнерів і держави. Розроблена модель ґрунтується на комплексному підході, що поєднує стратегічне бачення, аналітичну оцінку середовища, формування цілей, визначення пріоритетних ініціатив, ресурсне забезпечення, інноваційність та ефективні механізми реалізації. Така структура дозволяє суб'єктам малого підприємництва протистояти сучасним інформаційним загрозам та інтегрувати інформаційну безпеку в загальну бізнес-стратегію як чинник конкурентної переваги досліджуваних підприємств. Запропонована модель системи побудови стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва є адаптованою до специфіки малого бізнесу, враховує обмеженість ресурсів та високий рівень операційної гнучкості, що дозволяє поступово нарощувати зрілість системи інформаційної безпеки відповідно до рівня цифрової трансформації підприємства. Її практична реалізація сприятиме зниженню ризиків та підвищенню довіри споживачів, партнерів і регуляторів, що в сучасних умовах є важливим для сталого функціонування та розвитку суб'єктів малого підприємництва.

На основі проведеного аналізу, вважаємо за доцільне створити адаптивний алгоритм формування стратегії інформаційної безпеки, який поєднує системний підхід до оцінювання ризиків та загроз із врахуванням психологічних і поведінкових характеристик підприємців (рис. 3.4). Такий алгоритм дозволяє формувати реалістичні та дієві управлінські рішення, враховуючи специфіку організаційної поведінки, обмежену раціональність та типові моделі мислення, притаманні малому бізнесу.

Запропонований алгоритм формування стратегії забезпечення рівня інформаційної безпеки суб'єктів малого підприємництва з врахуванням поведінкових аспектів, репрезентує логічно послідовну й адаптивну модель ухвалення рішень щодо розвитку системи інформаційної безпеки у малому бізнесі.



Рис. 3.8. Алгоритм формування стратегії забезпечення рівня інформаційної безпеки суб'єктів малого підприємництва з врахуванням поведінкових аспектів

Джерело: удосконалено автором на основі [196-199].

Його побудова враховує як класичні принципи стратегічного менеджменту, так і специфіку поведінкових моделей, характерних для суб'єктів малого підприємництва, що забезпечує реалістичність і практичну цінність

підходу. Перший етап передбачає проведення оцінювання поточного рівня інформаційної безпеки суб'єктів малого підприємництва. На цьому етапі здійснюється аналіз існуючих методик, показників, а також визначається рівень зрілості ІБ-системи. Йдеться як про технічні характеристики (наявність антивірусного захисту, резервного копіювання тощо) так і про організаційні практики, кадрові компетенції, рівень дотримання політик. Цей етап є основою для подальших управлінських дій.

Другий етап пов'язаний із виявленням, аналізом та оцінкою зовнішніх і внутрішніх загроз, які можуть впливати на інформаційну безпеку підприємства. Тут доцільно враховувати як технічні (кіберзагрози, вразливості в ПЗ), так і поведінкові чинники (недбалість персоналу, слабка мотивація, відсутність обізнаності). Також доцільно переглянути набір чинників, що мають вплив на загальний рівень захищеності, зокрема законодавчі обмеження, партнерські ризики або цифрова неготовність. За необхідності може відбутися повернення до попередніх кроків для перегляду методик або уточнення групи експертів.

Третій етап полягає у визначенні стратегічних орієнтирів розвитку системи інформаційної безпеки, які мають бути співвіднесені із загальними цілями підприємницької діяльності. На цьому етапі формулюється бачення майбутнього стану інформаційної безпеки, окреслюються цілі (наприклад, сертифікація, автоматизація, мінімізація ризиків витоку даних), а також визначаються часові горизонти та важливі індикатори результативності.

Четвертий етап передбачає обґрунтування конкретної стратегії забезпечення інформаційної безпеки. На цьому етапі доцільно синтезувати результати оцінювання, загроз і стратегічного бачення та сформувати одну або кілька альтернативних стратегій. Цей етап передбачає аналіз ресурсів, бар'єрів, ризиків реалізації, а також ступінь відповідності стратегій поведінковим патернам прийняття рішень керівництвом підприємства.

П'ятий етап передбачає вибір оптимальної стратегії подальшого розвитку підприємства в рамках бажаного стану його інформаційної безпеки. Особливістю цього етапу є врахування поведінкових аспектів прийняття рішень

(наприклад, схильність до уникнення втрат, недостатня раціональність, обмеженість уваги тощо), які можуть суттєво впливати на управлінські пріоритети в малому бізнесі. Таким чином, процес прийняття рішень стає психологічно релевантним, що дозволяє уникнути хибної оптимізації або ігнорування основних загроз.

Отже, представлений алгоритм є цілісною адаптивною моделлю, що поєднує в собі стратегічне планування, аналіз ризиків та поведінкову економіку, що в сукупності підвищує ефективність інформаційної безпеки в умовах обмежених ресурсів суб'єктів малого підприємництва. Такий алгоритм є ефективним інструментом стратегічного управління в умовах сучасного цифрового середовища. Його етапність дозволяє системно оцінити рівень захищеності підприємства, ідентифікувати актуальні загрози, сформулювати реалістичні орієнтири розвитку та обрати найбільш доцільну стратегію, що відповідає ресурсним, організаційним і поведінковим особливостям малого бізнесу.

Такий підхід забезпечує технічну стійкість до кіберзагроз та підвищення організаційної культури безпеки, що є необхідною умовою для сталого функціонування підприємства в умовах цифрової трансформації.

На основі діаграми Ганта зобразимо узагальнено процес реалізації стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва відповідно до зазначених концептів (рис. 3.9), що дозволить відобразити поетапний підхід до формування та реалізації стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва.



Рис. 3.9. Узагальнення процесу формування та реалізації стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва на діаграмі Ганта

Джерело: побудовано автором на основі експертного підходу.

Відображена на діаграмі Ганта послідовність процесу формування та реалізації стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва, узагальнює технологію впровадження системи інформаційної безпеки та визначає логіку розвитку з чітко встановленими часовими рамками, ресурсним забезпеченням і системою зворотного зв'язку, що дозволяє суб'єктам малого підприємництва, навіть із обмеженими ресурсами, планово та стратегічно формувати свою стійкість до кіберзагроз.

План реалізації стратегії забезпечення інформаційної безпеки суб'єктів підприємництва представлено в таблиці 3.7.

Таблиця 3.7 – План реалізації стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва

Етапи	Завдання	Терміни	Ресурси	Результати
Діагностика поточного стану ІБ	Проводиться аналіз наявного стану ІБ підприємства, включаючи інфраструктуру, політики, процедури та практики захисту даних.	2026-07-01 – 2026-07-07	Внутрішній аудит, співбесіди, аналіз документації	Повна картина стану ІБ підприємства
Ідентифікація загроз і вразливостей	Ідентифікуються основні зовнішні та внутрішні загрози, а також вразливості ІТ-систем і організаційних процесів, що можуть призвести до порушення конфіденційності, цілісності або доступності інформації.	2026-07-08 – 2026-07-14	Інструменти аналізу ризиків, консультації з фахівцями	Визначення основних ризиків для ІБ

Продовження табл. 3.7

Визначення стратегічних цілей ІБ	Визначаються довгострокові цілі інформаційної безпеки з урахуванням ризик-орієнтованого підходу, законодавчих вимог та стратегічного бачення розвитку підприємства.	2026-07-15 – 2026-07-21	Аналіз нормативних вимог, стратегічні документи	Постановка чітких стратегічних орієнтирів
Формування політики та плану дій	Розробляється політика безпеки та деталізований план дій, що передбачає механізми управління ризиками, відповідальність персоналу та вимоги до технологій захисту.	2026-07-22 – 2026-07-31	Аналітики ІБ, експерти з управління ризиками	Описані політики та дії з безпеки
Розробка та затвердження стратегії	Створюється комплексна стратегія ІБ, що проходить погодження із зацікавленими сторонами. Визначаються основні показники ефективності та відповідальні особи.	2026-08-01 – 2026-08-09	Команда проєкту, керівництво підприємства	Схвалена стратегія з показниками ефективності
Впровадження організаційних заходів	Впроваджуються організаційні заходи: зміни в структурі управління, делегування повноважень, створення груп відповідальності за ІБ.	2026-08-10 – 2026-08-19	Організаційні структури, накази, регламенти	Організаційна модель забезпечення ІБ
Технічне забезпечення ІБ	Встановлюються або оновлюються технічні засоби захисту: міжмережеві екрани, системи виявлення вторгнень, резервне копіювання, антивірусний захист тощо.	2026-08-20 – 2026-08-31	ІТ-фахівці, технічне обладнання та програмне забезпечення	Функціонуючі технічні механізми захисту
Підготовка та навчання персоналу	Проводиться навчання персоналу щодо політик, процедур та практик ІБ, формування культури безпеки та підвищення рівня обізнаності про кіберзагрози.	2026-09-01 – 2026-09-14	Інструктори, навчальні матеріали, платформи	Обізнаний персонал, зниження людського фактору
Контроль, аудит і коригування стратегії	Здійснюється постійний моніторинг стану ІБ, аудит відповідності вимогам політики, аналіз інцидентів, а також коригування стратегії відповідно до нових викликів.	2026-09-15 – 2026-09-30	Інструменти моніторингу, аудитори, аналітики	Своєчасне реагування та адаптація стратегії

Джерело: побудовано автором на основі експертного підходу.

З метою формування та реалізації стратегії розвитку системи забезпечення інформаційної безпеки суб'єктів малого підприємництва побудовано узагальнюючий поетапний алгоритм дій у форматі діаграми Ганта. Визначений алгоритм деталізує складові стратегічного підходу до забезпечення

інформаційної безпеки. Такий структурований підхід дозволяє візуалізувати взаємозв'язки між окремими заходами, оптимізувати розподіл ресурсів, а також забезпечити цілісність і послідовність реалізації стратегії.

Діагностика поточного стану інформаційної безпеки полягає у проведенні всебічного аналізу інформаційної інфраструктури підприємства, політик безпеки та організаційної практики. Метою є виявлення слабких місць у системі інформаційної безпеки, що слугує відправною точкою для подальших дій. Для цього використовуються методи внутрішнього аудиту, аналіз документації, співбесіди з відповідальними особами. Очікуваним результатом є об'єктивна картина стану інформаційної безпеки суб'єктів малого підприємництва.

Ідентифікація загроз і вразливостей передбачає аналіз можливих ризиків, що можуть впливати на цифрові активи підприємства. На цьому етапі доцільно застосувати методики оцінювання ризиків та консультації з ІТ-спеціалістами. Основна мета – класифікувати загрози та пріоритезувати ризики для подальшої стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва.

Визначення стратегічних цілей інформаційної безпеки охоплює постановку конкретних, вимірюваних та досяжних цілей з урахуванням внутрішніх потреб і зовнішніх нормативів. На цьому етапі доцільно використовувати аналітичні інструменти стратегічного планування та нормативно-правову базу. Результатом стає узгоджена стратегічна рамка, що спрямовує подальші дії суб'єктів малого підприємництва.

На етапі формування політики та плану дій відбувається конкретизація механізмів забезпечення інформаційної безпеки. Розробляється політика безпеки та операційний план, який включає відповідальність персоналу, сценарії реагування на інциденти, вимоги до ІТ-систем. Основним ресурсом на цьому етапі є експертна команда аналітиків з інформаційної безпеки. Результатом стає набір документів, що регламентують управління інформаційною безпекою суб'єктів малого підприємництва.

Розробка та затвердження стратегій є основним етапом, що передбачає створення єдиного стратегічного документа, який є обов'язковим до виконання

для усіх учасників економічної діяльності. Важливою складовою є визначення індикаторів ефективності та відповідальних осіб. Цей етап формує основу для подальшого впровадження інклюзивних інституцій суб'єктами підприємництва.

Реалізаційна частина починається з впровадження організаційних заходів, що охоплює формування структур управління інформаційною безпекою, видачу наказів, створення робочих груп. Організаційна підтримка є запорукою стабільного функціонування системи інформаційної безпеки підприємств.

Технічне забезпечення інформаційної безпеки передбачає встановлення необхідного ПЗ та обладнання (фаєрволи, антивіруси, резервні копії). На цьому етапі, доцільно задіяти технічних фахівців, які забезпечують надійність системи на практичному рівні реалізації стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва.

Людський фактор часто стає причиною інцидентів, тому підготовка та навчання персоналу є важливим етапом досліджуваних процесів. Проведення навчальних заходів, семінарів та інструктажів формує безпекову культуру на рівні суб'єкта малого підприємництва.

Контроль, аудит і коригування стратегії передбачає постійний моніторинг виконання стратегії, оцінку її ефективності, виявлення відхилень та внесення змін у відповідь на нові загрози. Такий підхід забезпечує гнучкість і довготривалу дієвість визначеної стратегії.

Таким чином, запропонований план реалізації стратегії забезпечення інформаційної безпеки охоплює весь життєвий цикл стратегії інформаційної безпеки суб'єктів малого підприємництва, від її концептуального формування до практичної реалізації та подальшої підтримки. Вона може бути використана як модель для розробки типових планів впровадження інформаційної безпеки на рівні суб'єктів малого підприємництва України.

Розроблений план реалізації стратегії забезпечення інформаційної безпеки дозволяє систематизувати процеси стратегічного планування, управління ресурсами та впровадження політик інформаційної безпеки у логічній та структурованій формі. Послідовне розгортання етапів забезпечує цілісність і

взаємозв'язок усіх складових стратегічного циклу. Чітке визначення завдань, відповідальних осіб, термінів виконання, ресурсного забезпечення та очікуваних результатів створює умови для ефективного контролю реалізації стратегії та досягнення високого рівня інформаційної безпеки навіть в умовах обмежених можливостей малого бізнесу. Такий підхід, сприяє підвищенню стійкості суб'єктів малого підприємництва до інформаційних загроз та формує підґрунтя для інтеграції інформаційної безпеки у загальну систему стратегічного управління. Практичне застосування такого підходу до забезпечення інформаційної безпеки суб'єктами малого підприємництва, може стати основою для створення адаптивних систем захисту, розвитку цифрової компетентності персоналу та формування довіри з боку споживачів і партнерів.

Стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва мають різну спрямованість залежно від часових горизонтів. Узагальнення основних цілей, завдань та показників ефективності стратегій у коротко-, середньо- та довгостроковій перспективі систематизовано в таблиці 3.8.

Таблиця 3.8 – Основні цілі та завдання стратегій забезпечення інформаційної безпеки суб'єктів малого підприємництва за часовими фреймами

Цілі	Приклади завдань	Показники ефективності
Короткострокова перспектива (1-2 роки)		
Формування базової системи ІБ та підвищення обізнаності персоналу	- встановлення антивірусу, бекапів; - розробка первинної політики ІБ; - проведення базового навчання персоналу;	- частка працівників, що пройшли навчання; - кількість встановлених базових засобів захисту; - наявність локальної політики ІБ;
Середньострокова перспектива (3-5 років)		
Систематизація управління ІБ, впровадження політик і процедур безпеки	- впровадження систем моніторингу та управління доступом; - аудит ІБ-ризиків; - регулярне оновлення ІБ-документації;	- наявність сертифікованих процедур; - зменшення кількості інцидентів; - регулярність аудитів і тестів на проникнення;
Довгострокова перспектива (5-10 років)		
Інтеграція ІБ у стратегічне управління підприємством, забезпечення кіберстійкості	- розробка антикризових сценаріїв кіберзахисту; - використання кіберстрахування; - участь у галузевих ініціативах із кібербезпеки;	- рівень інтеграції ІБ у стратегію бізнесу; - кількість кризових сценаріїв реагування; - дотримання міжнародних стандартів (ISO, NIST);

Джерело: побудовано автором.

Уніфіковані стратегічні підходи до формування цілей і завдань у сфері забезпечення інформаційної безпеки суб'єктів малого підприємництва враховують часові фрейми, коротко-, середньо- та довгострокову перспективу забезпечення системи досліджуваних процесів. Така класифікація дозволяє адаптувати управлінські дії до реалій функціонування малого бізнесу, враховуючи динаміку розвитку, зміну загрозового середовища, фінансові можливості та організаційні трансформації.

Короткострокова перспектива (1-2 роки) передбачає формування базової системи інформаційної безпеки. На цьому етапі головною метою є створення фундаменту для подальшого розвитку системи інформаційної безпеки. Завдання зосереджуються на впровадженні мінімально необхідних технічних рішень – встановлення антивірусного захисту, систем резервного копіювання, початкове формування політики безпеки, а також проведення базових навчань для персоналу. Основними показниками ефективності впровадження стратегій є частка працівників, що пройшли інструктаж або тренінг, наявність базових регламентів і засобів захисту, що дозволяє швидко знизити ризик критичних інцидентів.

Середньострокова перспектива (3-5 років) передбачає перехід від фрагментарного до системного управління інформаційною безпекою. Основна мета на цьому етапі полягає у впровадженні повноцінних політик, процедур та інструментів моніторингу. Завдання включають проведення аудитів ризиків, автоматизацію контролю доступу, впровадження журналювання подій і регулярне оновлення ІБ-документації. Показниками ефективності слугують зменшення кількості інцидентів, поява сертифікованих процесів, дотримання вимог внутрішнього контролю. У середньостроковому горизонті малі підприємства отримують змогу вибудувати керовану, прозору й масштабовану систему безпеки.

Довгострокова перспектива (5-10 років) орієнтована на глибоку інтеграцію інформаційної безпеки у загальну бізнес-стратегію підприємства, що передбачає технічне удосконалення та зміну управлінської культури та розвиток

кіберстійкості. Завдання цього етапу включають розробку кризових сценаріїв реагування, застосування кіберстрахування, створення центрів реагування на інциденти, а також активну участь у професійних спільнотах і стандартизованих платформах кіберзахисту. Рівень інтеграції інформаційної безпеки у стратегічне планування, відповідність міжнародним стандартам (ISO/IEC 27001, NIST тощо) та наявність гнучких моделей реагування виступають головними критеріями ефективності.

Таким чином, поділ стратегій інформаційної безпеки за часовими фреймами дозволяє формувати поетапний підхід до розвитку системи забезпечення інформаційної безпеки суб'єктів малого підприємництва, що забезпечує як адаптивність, так і цільову результативність на кожному етапі організаційного зростання. Крім того, такий підхід дозволяє сформувати структурований та адаптивний алгоритм управління ризиками в цифровому середовищі. Короткострокові дії спрямовані на усунення критичних вразливостей і підвищення базового рівня захищеності, середньострокові – на впровадження системних інструментів управління, довгострокові – на інтеграцію інформаційної безпеки у стратегічне планування та формування кіберстійкої організації. Така поетапна модель дозволяє суб'єктам малого підприємництва ефективно використовувати обмежені ресурси, поступово нарощуючи потенціал захисту в умовах зростаючих кіберзагроз і цифрової трансформації.

Проведений аналіз засвідчив, що рівень витрат на інформаційну безпеку залежить від масштабу діяльності підприємства, ступеня цифровізації бізнес-процесів, рівня потенційних інформаційних ризиків та необхідності впровадження сучасних інструментів кіберзахисту. Для суб'єктів малого підприємництва важливим є формування збалансованого підходу до розподілу фінансових ресурсів, який дозволить забезпечити базовий рівень захисту інформації без надмірного навантаження на бюджет підприємства [200]. У зв'язку з цим доцільним є визначення орієнтовних напрямів та обсягів витрат на

забезпечення інформаційної безпеки відповідно до рівня захищеності суб'єктів малого підприємництва, що представлено у табл. 3.9.

Таблиця 3.9 – Орієнтовні напрями та обсяги витрат на забезпечення інформаційної безпеки суб'єктів малого підприємництва

	Рівень інформаційної безпеки			
	Низький	Середній	Достатній	Високий
Орієнтовні напрями витрат	-придбання базового антивірусного ПЗ, -резервне копіювання (локальні носії), -проведення базового навчання персоналу.	-встановлення міжмережевого екрану, -аудит поточних ризиків, -розробка політик та інструкцій з ІБ.	-впровадження систем моніторингу доступу, -тестування на проникнення, -сегментація мережі та контроль прав доступу.	- інтеграція ІБ в ERP/CRM-системи, -використання хмарних сервісів кіберзахисту, - консультації із зовнішніми експертами.
Орієнтовні обсяги витрат (у % від загального бюджету ІТ)	5-10%	10-15%	15-20%	20-30%
Орієнтовна вартість пріоритетних пропозицій	Ліцензійний антивірус – 1 000 грн/рік. Зовнішній HDD – 2 500 грн. Базове навчання – 3 000 грн.	Міжмережевий екран – 6 000 грн. Аудит – 8 000 грн. Інструкції – 1 500 грн.	Система моніторингу – 10 000 грн. Пентест – 12 000 грн. Налаштування доступу – 5 000 грн.	Хмарні сервіси (річна підписка) – 15 000 грн. Інтеграція в CRM – 20 000 грн. Зовнішній консалтинг – 10 000 грн.

Джерело: побудовано автором на основі експертного підходу.

Визначені напрями та обсяги витрат щодо забезпечення інформаційної безпеки суб'єктів малого підприємництва дають змогу визначити загальну структуру витрат на інформаційну безпеку та забезпечити практичне підґрунтя для планування конкретних заходів у межах реального бюджету малого бізнесу.

На етапі низького рівня інформаційної безпеки суб'єктів малого підприємництва, як правило, не мають сформованої ІБ-інфраструктури, тому основні витрати спрямовуються на базовий захист: придбання антивірусного ПЗ, створення резервних копій даних на зовнішніх носіях, а також проведення первинного навчання персоналу. Орієнтовний бюджет у цьому випадку становить 5-10% від загального ІТ-бюджету. Пріоритетними є недорогі рішення з високою ефективністю на початковому етапі: базовий антивірус (1 000 грн/рік), зовнішній носій (2 500 грн), а також інструктаж з основ кібергігієни (3 000 грн).

Середній рівень інформаційної безпеки характеризується вже наявною частковою інфраструктурою захисту, тому витрати зосереджуються на вдосконаленні процедур, встановленні міжмережевих екранів, проведенні аудитів та створенні локальних політик. Орієнтовні витрати зростають до 10-15% від ІТ-бюджету. Пріоритетними інвестиціями стають фаєрволи (6 000 грн), внутрішній аудит або зовнішня консультація (8 000 грн) і розробка інструкцій (1 500 грн).

На достатньому рівні захищеності суб'єктів малого підприємництва вже впроваджено основні елементи інформаційної безпеки, а тому підприємство переходить до контролю та моніторингу, що включає встановлення систем моніторингу доступу, проведення тестів на проникнення, а також сегментацію мережі. Орієнтовні витрати становлять 15-20% ІТ-бюджету. Серед пріоритетних витрат: системи контролю (10 000 грн), пентести (12 000 грн) та налаштування доступу (5 000 грн).

Високий рівень інформаційної безпеки потребує стратегічної інтеграції інформаційної безпеки у основні бізнес-процеси. Інвестиції орієнтовані на хмарні рішення, захист у рамках ERP/CRM, а також на зовнішній консалтинг. Тут частка витрат сягає 20-30% ІТ-бюджету. Орієнтовна вартість включає хмарні сервіси ($\approx 15\,000$ грн/рік), інтеграцію у CRM ($\approx 20\,000$ грн), консалтинговий супровід ($\approx 10\,000$ грн).

Таким чином, запропоновані орієнтири витрат на забезпечення інформаційної безпеки суб'єктів малого підприємництва надають практичні вектори для підприємств у плануванні бюджету безпеки. Такий підхід дозволяє раціонально використовувати ресурси та забезпечити безперервний розвиток інформаційної безпеки відповідно до реального стану організації та динаміки загрозового середовища. Диференційований підхід до планування витрат на інформаційну безпеку суб'єктів малого підприємництва, заснований на оцінці поточного рівня їх захищеності, дозволяє сформулювати реалістичну, поетапну та економічно доцільну стратегію розвитку системи інформаційної безпеки. Визначення орієнтовних напрямів витрат і конкретних пріоритетних пропозицій

забезпечує можливість ефективного розподілу фінансових ресурсів з урахуванням обмеженого бюджету та актуальних ризиків.

У сучасному цифровому середовищі інформаційна безпека виступає однією з головних складових конкурентоспроможності суб'єктів малого підприємництва. Враховуючи обмежені фінансові, кадрові та технологічні ресурси суб'єктів малого підприємництва, стратегічним орієнтиром у підвищенні їхньої стійкості до інформаційних ризиків є розвиток інклюзивних інституцій, документів що забезпечують рівний доступ до знань, фінансів, цифрових сервісів, правового захисту, незалежно від розміру підприємства або регіону його функціонування [201, 202]. Інклюзивні інституції як стратегічний орієнтир у забезпеченні інформаційної безпеки суб'єктів підприємництва систематизовано в таблиці 3.10.

Таблиця 3.10 – Інклюзивні інституції як стратегічний орієнтир у забезпеченні інформаційної безпеки суб'єктів підприємництва

Орієнтири інклюзивних інституцій	Зміст механізму впливу	Приклади	Джерела
Формування сприятливого правового середовища	Ухвалення прозорих і адаптивних нормативно-правових актів, що регулюють ІБ суб'єктів малого підприємництва	Дія City, Закон України «Про інформацію»; EU Cybersecurity Act	Котусєв С. (2023); OECD (2021). Digital Security Policy for SMEs
Освітні та консультаційні ініціативи	Підвищення обізнаності МСП через тренінги, курси, вебінари та інформаційні кампанії	Diia.Business – освітні вебінари з кібербезпеки; ENISA тренінги	ENISA (2020). Cybersecurity Training for SMEs; Ситнік І.В. (2022)
Створення партнерств і платформ співпраці	Інституційне сприяння створенню публічно-приватних платформ, кластерів, онлайн-форумів	Український кластер кібербезпеки; European Cybersecurity Month	Kshetri N. (2019); ENISA (2022) Public-Private Cooperation for Cybersecurity
Фінансова та технічна підтримка	Надання грантів, пільгового фінансування, безкоштовного доступу до ІБ-інструментів	USAID гранти на цифрову трансформацію МСП; Horizon Europe фінансування	Мазур Н.П., Рой Я.В. (2018); European Commission (2021) SME Strategy
Моніторинг, стандартизація і сертифікація	Впровадження стандартів, шаблонів політик ІБ, добровільної сертифікації, звітності про ризики	Платформа GOV.UA для інцидентів; ENISA шаблони кібергігієни для МСП	Бегун А.В. (2011); ENISA (2023) Cybersecurity Standards & Guidelines

Джерело: побудовано автором на основі [69, 160, 201-210].

Інклюзивні інституції сприяють формуванню нормативного поля, що адаптоване до потреб малого бізнесу. У ЄС це реалізовано через EU Cybersecurity Act та General Data Protection Regulation (GDPR), які встановлюють стандарти захисту даних та безпеки для всіх типів підприємств, у тому числі МСП [204]. В Україні запроваджено спеціальний правовий режим «Дія City», який, хоча й орієнтований переважно на IT-компанії, створює прецедент гнучкого регулювання для цифрових малих підприємств [201]. Проте законодавчі ініціативи в Україні залишаються фрагментарними, зокрема щодо стандартів безпеки для непрофільних МП.

Освітня інституційна підтримка є важливим стратегічним напрямом забезпечення інформаційної безпеки підприємств. Наприклад, в Україні платформа Diia.Business надає доступ до курсів, вебінарів і шаблонів політик інформаційної безпеки, тоді як ENISA (Агенція ЄС з кібербезпеки) впроваджує навчальні програми, зокрема для МСП у сільських або транскордонних регіонах, що дозволяє підвищити цифрову грамотність і здатність до самозахисту навіть у найменших підприємствах [160].

Публічно-приватне партнерство також є стратегічним орієнтиром забезпечення інформаційної безпеки. Україна сьогодні розвивається в даному напрямі. Так, у Західній Україні діє Кібербезпековий кластер, що об'єднує університети, IT-компанії та громадські об'єднання для розробки політик інформаційної безпеки. Подібні моделі діють у Польщі, Фінляндії, Словаччині, де муніципальні платформи надають консультації МСП щодо кіберзагроз, що дозволяє зменшити залежність від централізованих ресурсів [205].

У регіональному вимірі між Україною та країнами ЄС простежується низка відмінностей. За даними Європейської комісії, понад 30% МСП у ЄС отримували консультаційну або фінансову підтримку з інформаційної безпеки на місцевому рівні, тоді як в Україні – лише 8% підприємств звертались за подібною підтримкою, і здебільшого до міжнародних донорів (наприклад, USAID) [207]. Така асиметрія обумовлена недофінансуванням регіональних інституцій в

Україні та недостатньою інтеграцією інформаційної безпеки у місцеві програми підтримки МП.

Фінансова та технічна підтримка є важливим аспектом забезпечення інформаційної безпеки. Наприклад, у ЄС діє низка програм (Digital Europe, Horizon Europe), які фінансують ІБ-компоненти проєктів МП. В Україні, натомість, ініціативи фінансування носять переважно донорський характер, а участь у національних програмах малого підприємництва, вимагає значного адміністративного ресурсу, що створює бар'єри для мікробізнесу, особливо в сільській місцевості [208].

Системна стандартизація та моніторинг є важливими функціями інклюзивних інституцій. ENISA публікує щорічні звіти та шаблони ІБ-документації для МСП, зокрема типові політики захисту персональних даних, інструкції реагування на інциденти тощо [204, 205]. В Україні подібна діяльність здійснюється на рівні CERT.GOV.UA, однак охоплення мікро- та малих підприємств є обмеженим.

Таким чином, інклюзивні інституції виступають стратегічним вектором розвитку системи забезпечення інформаційної безпеки суб'єктів малого підприємництва, формуючи організаційні, інформаційні, фінансові та правові засади функціонування безпечного цифрового середовища. Їх розвиток має базуватися на міжрегіональному співробітництві, трансфері кращих європейських практик та підвищенні локалізованої підтримки суб'єктів малого підприємництва.

Інклюзивні інституції виступають важливим стратегічним орієнтиром у формуванні ефективної та стійкої системи інформаційної безпеки суб'єктів малого підприємництва. Вони створюють нормативно-правові, організаційні та освітні умови для впровадження ІБ-рішень та сприяють зменшенню цифрової нерівності між великим і малим бізнесом. Інституційна підтримка забезпечує суб'єктам малого підприємництва доступ до знань, інструментів, фінансування та стандартів, що суттєво підвищує рівень їхньої цифрової стійкості.

Порівняльний аналіз забезпечення інформаційної безпеки підприємств, між Україною та країнами ЄС свідчить про те, що при наявності спільних тенденцій у підходах до підтримки суб'єктів малого підприємництва, рівень реалізації інституційних механізмів в Україні є значно нижчим, що вимагає розширення практики інституційного партнерства, локалізації європейських практик, зміцнення освітніх та фінансових платформ, а також активнішої участі держави у стимулюванні кіберзахисту малого бізнесу на регіональному рівні [209]. Тому, посилення ролі інклюзивних інституцій має стати пріоритетом державної цифрової політики та регіональних стратегій безпеки, з урахуванням потреб і можливостей суб'єктів малого підприємництва як важливого чинника сталого економічного розвитку.

У сучасних умовах у найменших суб'єктах підприємництва, забезпечення інформаційної безпеки стає основним завданням. Проте обмежені фінансові, кадрові та технічні ресурси не дозволяють малому бізнесу реалізовувати комплексні та дороговартісні системи захисту, характерні для великих компаній. У зв'язку з цим виникає необхідність у створенні адаптивних інституційних моделей інформаційної безпеки, які б поєднували простоту впровадження, ефективність реагування на загрози та відповідність базовим вимогам кіберзахисту.

Пропонуємо розробити уніфікований шаблон інституційної моделі інформаційної безпеки для малого бізнесу, з урахуванням практичних потреб підприємств та основних принципів безпеки (конфіденційність, цілісність, доступність), покликаний стати практичним керівництвом для формування мінімально необхідної, але функціональної системи захисту (рис. 3.10).

Такий підхід, дозволить підприємствам знизити ризики інформаційних інцидентів та підвищити цифрову грамотність працівників, налагодити комунікацію з питань інформаційної безпеки та закласти основу для подальшого стратегічного розвитку.

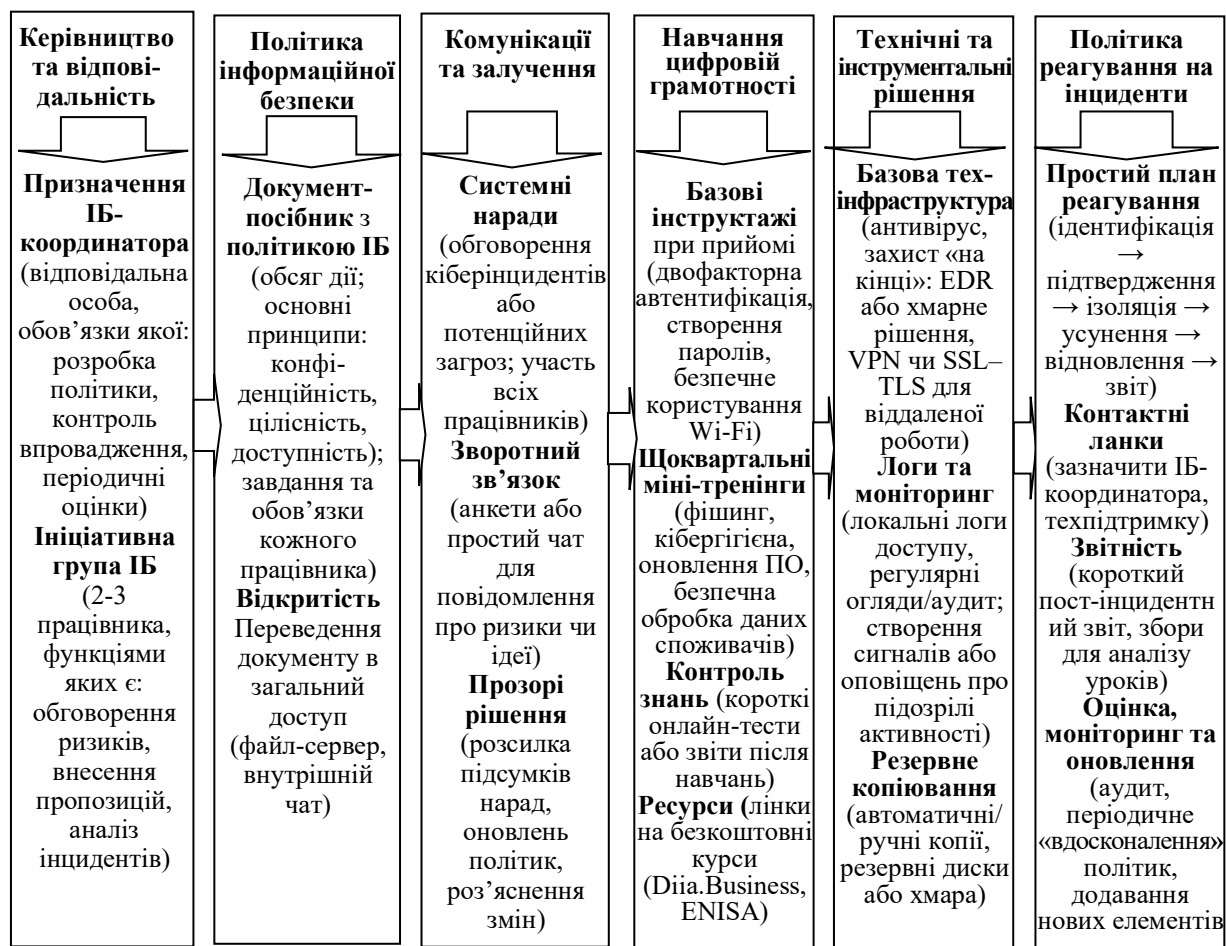


Рис. 3.10. Шаблон інституційної моделі інформаційної безпеки для бізнесу

Джерело: побудовано автором на основі експертного підходу.

Запропонована інституційна модель інформаційної безпеки для малого бізнесу, представлена у шаблоні, передбачає реалізацію комплексного підходу до формування стійкої системи інформаційної безпеки, адаптованої до обмежених ресурсів малого підприємства. Важливою складовою моделі є чіткий розподіл відповідальності: призначення ІБ-координатора, який відповідає за розробку політики, її впровадження та періодичну оцінку, а також створення ініціативної групи з 2-3 працівників для обговорення ризиків, аналізу інцидентів та формування пропозицій. Основою також є політика інформаційної безпеки, оформлена у вигляді доступного документа-посібника, який містить базові принципи (конфіденційність, цілісність, доступність), зону дії та обов'язки працівників. Принцип відкритості реалізується через публічне розміщення

політики на файлових серверах або внутрішніх чатах, що сприяє прозорості та підвищенню рівня залучення персоналу.

Комунікаційний блок шаблону передбачає системні наради для обговорення кіберінцидентів, створення каналів зворотного зв'язку (анкети, чати), а також прозору систему інформування через розсилки та пояснення змін. Навчання працівників є невід'ємною частиною моделі: включено базові інструктажі при прийомі на роботу, щоквартальні мінітренінги з актуальних тем (фішинг, кібергігієна, оновлення ПЗ), онлайн-тести та доступ до безкоштовних освітніх ресурсів (наприклад, Diia.Business, ENISA).

Технічна складова охоплює базову інфраструктуру захисту, антивірусне ПЗ, EDR або хмарні рішення, VPN/SSL для безпечної роботи онлайн, логування подій, аудит доступу та резервне копіювання (локальне чи в хмарі). Політика реагування на інциденти включає простий план дій у шість кроків (ідентифікація → підтвердження → ізоляція → усунення → відновлення → звіт), контактні ланки та звітність за результатами інцидентів. Постійний моніторинг та оновлення передбачає проведення аудитів, ревізії політик, врахування нових загроз та вдосконалення системи. Таким чином, шаблон дозволяє малому бізнесу впровадити ефективну систему інформаційної безпеки з мінімальними витратами, забезпечуючи баланс між доступністю, простотою та результативністю захисту.

Шаблон інституційної моделі інформаційної безпеки для малого бізнесу є практичним інструментом, який дозволяє впровадити базову, але системну архітектуру захисту інформаційних активів у межах обмежених ресурсів. Його структура охоплює компоненти управління інформаційної безпеки, від призначення відповідальних осіб і формалізації політики безпеки до організації навчання, технічного захисту та реагування на інциденти [210]. Впровадження такої моделі забезпечує підвищення стійкості підприємства до кіберзагроз, сприяє формуванню культури інформаційної безпеки та створює передумови для подальшого розвитку захисної інфраструктури у відповідності до зростаючих викликів цифрового середовища.

Висновки до розділу 3

Встановлено, що побудова ефективної системи інформаційної безпеки підприємства повинна базуватися на інтеграції науково обґрунтованих методологічних підходів, які забезпечують системність, адаптивність і цілеспрямованість захисних заходів. Аналіз літературних джерел і практик підтвердив важливість застосування системного, функціонального, ризик-орієнтованого та інформаційно-аналітичного підходів, що дозволяє враховувати як зовнішні, так і внутрішні чинники, які формують інформаційну вразливість підприємства.

Здійснено моделювання структури інформаційної безпеки на основі аспектноорієнтованих і багаторівневих моделей, які поєднують технічні, організаційні, правові та поведінкові компоненти. Обґрунтовано, що ефективність таких моделей значною мірою залежить від правильного визначення об'єкта захисту, ідентифікації критичних активів, встановлення порогових значень стану безпеки та формалізації показників оцінювання. Система інформаційної безпеки має бути не статичною, а такою, що постійно адаптується до змін у зовнішньому середовищі та внутрішній інфраструктурі підприємства.

Доведено, що науково-методичне забезпечення побудови системи інформаційної безпеки повинно включати процедури ризик-аналізу, моделювання сценаріїв інцидентів, визначення економічної доцільності заходів безпеки та впровадження моніторингових і превентивних інструментів. Також акцент зроблено на важливості кадрового забезпечення, цифрової обізнаності персоналу та наявності регламентованих політик і процедур безпеки, що суттєво підвищує ефективність функціонування інформаційної безпеки у динамічному середовищі.

Сформувано цілісну методику аудиту інформаційної безпеки підприємства, яка ґрунтується на принципах системності, об'єктивності, ризик-орієнтованого підходу та адаптивності до специфіки організаційної структури та

ресурсних можливостей підприємства. Аудит інформаційної безпеки розглядається як інструмент контролю та як засіб підвищення ефективності системи безпеки, виявлення критичних вразливостей, оптимізації ресурсів та зниження залишкового ризику.

Запропоновано алгоритм аудиту інформаційної безпеки, який охоплює підготовчий етап, ідентифікацію об'єктів аудиту, збір і перевірку доказів, оцінювання відповідності політик і практик безпеки встановленим стандартам, а також формування звіту з рекомендаціями щодо усунення виявлених недоліків. Доцільно формалізувати інструменти у вигляді чек-листів, критеріїв оцінки, матриць ризиків і класифікацій вразливостей, що дозволяє забезпечити прозорість та відтворюваність результатів.

Визначено, що ефективність аудиту значною мірою залежить від обраного підходу, а також від залучення компетентних фахівців, належного документування процесів інформаційної безпеки та доступності інформації для перевірки. Для суб'єктів малого підприємництва доцільним є використання спрощених методів оцінювання із залученням типових шаблонів і адаптованих критеріїв, що враховують обмежені фінансові та кадрові ресурси. Методика аудиту інформаційної безпеки підприємства виступає інструментом управління кіберризиками, дозволяє систематизувати оцінювання рівня захищеності інформаційних активів та визначити обґрунтовані напрями удосконалення безпекової інфраструктури. Вона має бути інтегрованою в загальну систему корпоративного управління та орієнтованою на безперервне вдосконалення, з урахуванням динаміки загроз та змін у внутрішньому і зовнішньому середовищі.

Доведено, що ефективне управління інформаційною безпекою потребує впровадження технічних засобів захисту та чітко структурованої стратегії, орієнтованої на довгострокову стійкість та адаптацію до зовнішніх викликів. Розроблений поетапний підхід, візуалізований на діаграмі Ганта, дозволяє сформувати логіку реалізації цілей у сфері інформаційної безпеки, від оцінювання вихідного стану до впровадження заходів і моніторингу їх ефективності. Стратегічне планування інформаційної безпеки суб'єктів малого

підприємництва має ґрунтуватися на адаптивності, ризик-орієнтованості та економічній доцільності впроваджуваних заходів. Визначення та реалізація стратегічних орієнтирів сприятимуть формуванню стійкої системи захисту, підвищенню довіри до бізнесу з боку партнерів і споживачів, а також забезпеченню конкурентоспроможності малого підприємництва в умовах цифрової трансформації економіки.

Визначено, що стратегічні орієнтири повинні базуватися на системному аналізі ризиків, ранжуванні загроз, визначенні пріоритетів інвестування та створенні умов для безперервного навчання персоналу. Важливою передумовою успішної реалізації стратегії є гармонійне поєднання технічного, організаційного та поведінкового векторів розвитку, що забезпечує цілісність і надійність системи інформаційної безпеки. Особливу увагу слід приділяти підтримці цифрової грамотності, впровадженню стандартів інформаційної безпеки (зокрема ISO/IEC 27001) і створенню механізмів адаптації малих підприємств до швидкоплинного інформаційного середовища.

Визначено послідовність основних дій, що забезпечують досягнення цілей у сфері інформаційної безпеки. Запропонований поетапний підхід базується на логічній взаємозалежності між аналітичними завданнями та стратегічними рішеннями, що робить його адаптивним і прикладним до умов функціонування малих підприємств. Особливу увагу зосереджено на інтеграції управління ризиками, інвестиційної доцільності та моніторингу ефективності заходів, що дозволяє створити систему інформаційної безпеки, орієнтовану на технічний захист та на стійкість бізнесу до цифрових загроз.

ВИСНОВКИ

У дослідженні запропоновано нове вирішення наукового завдання щодо формування та удосконалення системи забезпечення інформаційної безпеки суб'єктів підприємництва в умовах цифрової трансформації економіки. Отримані результати дали змогу сформулювати такі висновки:

Узагальнено та систематизовано теоретико-методичні засади формування системи інформаційної безпеки суб'єктів підприємництва в умовах цифрової трансформації економіки. Встановлено, що інформаційна безпека є стратегічним ресурсом забезпечення його конкурентоспроможності, стійкості та безперервності функціонування. На основі аналізу існуючих наукових підходів уточнено сутність інформаційної безпеки суб'єктів підприємництва як динамічного процесу забезпечення захищеності інформаційного середовища підприємства, спрямованого на збереження конфіденційності, цілісності, доступності та цінності інформаційних ресурсів у процесі досягнення стратегічних цілей розвитку.

Систематизовано сучасні виклики та бар'єри забезпечення інформаційної безпеки суб'єктів підприємництва з урахуванням особливостей функціонування підприємств різного масштабу. Визначено, що основними викликами є зростання кіберзагроз, цифровізація бізнес-процесів, людський фактор, недосконалість нормативного регулювання та обмеженість ресурсного забезпечення. Обґрунтовано, що для малого бізнесу найбільш критичними є фінансові та кадрові обмеження, для середнього – недостатня інтегрованість систем безпеки, а для великого – складність управління багаторівневою інформаційною інфраструктурою.

Удосконалено структурно-компонентну модель формування системи інформаційної безпеки підприємства шляхом інтеграції цільової, теоретико-методологічної, функціонально-ресурсної, аналітичної та результативної складових. Запропонована модель забезпечує логічний взаємозв'язок між стратегічними цілями підприємства, механізмами захисту інформаційних

ресурсів та інструментами оцінювання ефективності системи інформаційної безпеки, що сприяє підвищенню її адаптивності до змін середовища.

Сформовано концептуальну модель забезпечення інформаційної безпеки суб'єктів підприємництва, яка поєднує процеси ідентифікації, аналізу, попередження та нейтралізації інформаційних загроз із загальною системою управління підприємством. На відміну від існуючих підходів, модель забезпечує інтеграцію стратегічних, організаційних, функціональних та технологічних аспектів інформаційної безпеки в єдину систему управління ризиками та захистом інформаційних ресурсів.

Удосконалено організаційну модель системи управління інформаційною безпекою суб'єктів господарювання з урахуванням впливу внутрішнього та зовнішнього середовища. Запропонований підхід передбачає узгодження політики інформаційної безпеки з корпоративною стратегією розвитку підприємства, нормативно-правовими вимогами, інституційними умовами та сучасними викликами цифрового середовища.

Визначено функціонально-компонентний підхід до забезпечення інформаційної безпеки підприємства на основі інтеграції внутрішніх і зовнішніх процесів впливу та принципів ефективного управління безпекою. Доведено доцільність поєднання технічних, організаційних, економічних і правових складових із принципами конфіденційності, цілісності, доступності, адаптивності та економічної ефективності, що дозволяє забезпечити комплексний захист інформаційних ресурсів підприємства.

Удосконалено методичний підхід до оцінювання стану інформаційної безпеки суб'єктів підприємництва шляхом інтеграції системи кількісних і якісних показників та використання матричних методів стратегічного аналізу. Запропонований підхід дозволяє здійснювати комплексну діагностику рівня інформаційної безпеки, визначати критичні зони ризику, оцінювати ефективність витрат на захист інформації та формувати обґрунтовані управлінські рішення щодо підвищення рівня захищеності підприємства.

Запропоновано комплексний алгоритм створення та функціонування системи інформаційної безпеки підприємства, який охоплює етапи стратегічного планування, організаційного забезпечення, технічного впровадження, моніторингу та безперервного удосконалення. Реалізація запропонованого алгоритму забезпечує системність процесів управління інформаційною безпекою та підвищує здатність підприємства оперативно реагувати на нові виклики цифрового середовища.

Обґрунтовано підхід до формування системи інформаційної безпеки на основі деталізації її ключових компонентів, сучасних технологічних рішень і міжнародних стандартів. Визначено доцільність використання міжнародних стандартів серії ISO/IEC 27000, NIST Cybersecurity Framework та архітектурного підходу TOGAF для забезпечення узгодженості між бізнес-цілями підприємства та системою інформаційного захисту. Доведено, що використання TOGAF сприяє підвищенню керованості, гнучкості та ефективності процесів забезпечення інформаційної безпеки.

Запропоновано методику проведення аудиту інформаційної безпеки підприємства, яка поєднує внутрішній і зовнішній аудит у межах єдиної системи оцінювання. Методика базується на ризик-орієнтованому підході, передбачає структуризацію об'єктів аудиту, використання чітких критеріїв оцінювання та дозволяє своєчасно виявляти вразливості системи інформаційної безпеки.

Сформовано стратегічні орієнтири розвитку системи забезпечення інформаційної безпеки суб'єктів підприємництва, які спрямовані на інтеграцію інформаційної безпеки у стратегічне управління підприємством, розвиток інноваційних технологій захисту інформації, формування культури кібербезпеки та посилення інституційної підтримки цифрової трансформації бізнесу. Доведено, що реалізація запропонованих стратегічних орієнтирів сприятиме підвищенню конкурентоспроможності, економічної стійкості та безперервності функціонування суб'єктів підприємництва в умовах зростання інформаційних і кібернетичних загроз.

СПИСОК ВИКОРИСТАНОЇ ДЖЕРЕЛ

1. Porter M.E., Millar V.E. How Information Gives You Competitive Advantage. *Harvard Business Review*, 1985. July-August. URL: <https://hbr.org/1985/07/how-information-gives-you-competitive-advantage> (дата звернення: 20.05.2025).
2. OECD. Digital Economy Outlook 2015. OECD. Paris: OECD Publishing, 2015. URL: <https://www.oecd.org/digital/digital-economy-outlook-2015.htm> (дата звернення: 16.04.2025).
3. OECD. Digital Economy Outlook 2020: Resilience, Recovery and Transformation. OECD. Paris: OECD Publishing, 2020.: URL: <https://www.oecd.org/digital/digital-economy-outlook-2020.htm> (дата звернення: 16.04.2025).
4. UNESCO. Towards Knowledge Societies. UNESCO. Paris: UNESCO Publishing, 2005. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000141843> (дата звернення: 22.04.2025).
5. UNESCO. Knowledge Societies: Information Technology for Sustainable Development. UNESCO, International Council for Science. Paris: UNESCO Publishing, 2013. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000214274> (дата звернення: 22.04.2025).
6. McKinsey & Company. Cybersecurity in a Digital-first World: Risks, Opportunities, and Trends. McKinsey & Company, 2022: URL: <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity-in-a-digital-first-world> (дата звернення: 16.04.2025).
7. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*, 2016. 1. С. 17-23.
8. Абакумов В.М. Інформаційна безпека підприємства як об'єкт адміністративно-правової охорони. *Форум права*, 2012. № 4. С. 10-16

9. Концепція інформаційної безпеки України. URL: [http://mip.gov.ua/files/banners/Final%20Проект%20концепції%20\(Текст\)%20-%2030.09.15.pdf](http://mip.gov.ua/files/banners/Final%20Проект%20концепції%20(Текст)%20-%2030.09.15.pdf) (дата звернення: 15.07.2025).
10. Сороківська О. А., Гевко В. Л. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького національного університету*, 2010. № 2. Т. 2. С. 32-35.
11. Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів. Київ: ДУТ ННІЗІ, 2020. 167 с.
12. Забродський В.А., Кізім Н.А., Янов Л.І. Сучасні методи організації та управління промисловим виробництвом. Харків: АТ Бізнес-Інформ, 1997. 64.
13. Гладченко, Т.М. Індикатори економічної безпеки підприємницької діяльності. Донецьк: ДонДАУ. Менеджер, 2000. №12. С. 111-113.
14. Кицюк В.М., Пупинін О.С. Інформаційна безпека підприємства: теоретичний аспект. *Сучасний захист інформації*, 2024. 2 (58). С. 103-108.
15. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с.
16. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. *Ефективна економіка*, 2015. № 4. URL: <http://www.economy.nayka.com.ua/?op=1&z=5514> (дата звернення: 18.09.2025).
17. Hoffman L.J, Lawson-Jenkins K., Blum J. Trust beyond security: an expanded trust model. *Communications of the ACM*. 2006. Vol. 49, № 7, P. 94-101.
18. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. *Вісник Київського університету імені Т. Шевченка*. 1999. Вип. 14 : Міжнародні відносини. С. 46-48.
19. Богуш В., Юдін О. Інформаційна безпека держави. К.: МК-Прес, 2005. 432 с.
20. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-

комунікаційних технологій у сучасному Донбасі. *Наукові записки Інституту політичних і етнонаціональних досліджень імені І.Ф. Кураса НАН України*, 2015. Вип. 3. С. 220-237.

21. Чубаєвський В.І. Економічна ефективність систем захисту корпоративної інформації. Дисертація на здобуття ступеня доктора наук за спеціальністю 08.00.04 – економіка та управління підприємствами (за видами економічної діяльності). Державний торговельно-економічний університет, Київ, 2023 URL: <https://knute.edu.ua/file/Mg==/0db2781b1c367483d9b83547d693308b.pdf> (дата звернення: 18.09.2025).

22. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» № 537-V від 9 січня 2007 року. URL: <https://zakon.rada.gov.ua/laws/show/537-16#Text>.

23. Сніщенко Р.Г., Гринчуцький В.І. Інформаційна безпека як складова економічної безпеки суб'єктів господарювання. *Економічний аналіз*, 2020. Том 30. № 1. Частина 1. С. 241-248.

24. Борзенкова О.Д., Шрамко О. О. Інформаційна складова у структурі економічної безпеки підприємства. *Бізнесінформ*, 2017. № 4. С. 151-156.

25. Озарко К., Андрухів Т. Особливості формування оптимальних організаційних структур управління Іт-бізнесом як елемент його інформаційної безпеки. *Економіка та суспільство*, 2022. № 43. DOI: <https://doi.org/10.32782/2524-0072/2022-43-21> (дата звернення: 18.09.2025).

26. Бехтер А.А. Загрози інформаційної безпеки та захист інформації як складова економічної безпеки сільськогосподарських підприємств. *Агросвіт*, 2020. № 12. С. 66-70

27. Маруніч А.В. Захист інформації як основна складова економічної безпеки підприємства. *Управління розвитком*, 2014. № 14. С. 130-132.

28. Панченко О.А., Панченко Л.В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. *Правова інформатика*, 2015. 2 (46). С. 32-38.

29. Ковальська Л., Топалов В., Топалов Р. Інформаційна безпека регіону: підходи до розгляду та економічна сутність. *Економічний форум*, 2023. № 13 (2). С. 18-24.

30. Топалов В.М. Забезпечення інформаційної безпеки як детермінанта конкурентоспроможного розвитку підприємства. *Актуальні питання економічних наук* № 10, 2025. URL: <https://a-economics.com.ua/index.php/home/article/view/550/558> (дата звернення: 18.09.2025).

31. Гапєєва О.М., Ромашко С.М. Теоретичні засади формування інформаційної безпеки як інструменту забезпечення національної безпеки. *Бізнес Інформ*, 2025. №2. С. 163-170.

32. Топалов В. Забезпечення інформаційної безпеки суб'єктів підприємництва в умовах воєнного стану. Проблеми гарантування безпеки людини в умовах сучасних викликів: матеріали II Всеукраїнської науково-практичної конференції 29-30 квітня 2025 р. м. Луцьк: ЛНТУ, 2025. 114 с. С. 38-40.

33. Мачак Т., Дубина О., Юрченко С. Інформаційне забезпечення управління системою економічної безпеки підприємства та його удосконалення. *Економіка та суспільство*, 2024. № 61. DOI: <https://doi.org/10.32782/2524-0072/2024-61-66> (дата звернення: 18.09.2025).

34. Гнатенко В. Інформаційно-економічна безпека як фактор стабільного розвитку держави. *Публічне урядування*. 2020. №5 (25), С. 63-74.

35. Протидія дезінформації в умовах гібридної війни: український досвід. Центр стратегічних комунікацій та інформаційної безпеки. 2023. URL: <https://spravdi.gov.ua/> (дата звернення: 25.09.2025).

36. Босак А.О., Вержиковський В.П., Калінін І.Є., Максимів І.Д., Приступа Д.А., Ривак О.І. Засади формування інформаційної безпеки підприємства. *Міжнародний науковий журнал Інтернаука*. Серія: Економічні науки, 2023. № 11. DOI: <https://doi.org/10.25313/2520-2294-2023-11-9157> (дата звернення: 25.09.2025).

37. Марка Д., МакГоуен К. Методологія структурного аналізу та проектування SADT: пер. з англ. Київ: Діалектика, 1993. 240 с.
38. Ворохоб М.В. Моделі і методи вдосконалення політики інформаційної безпеки підприємства на основі методології Zero Trust. Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації». Київський університет імені Бориса Грінченка, МОН України, Київ, 2023. 164с.
39. Цілі інформаційної безпеки та їх значення. URL: <https://www.dqsglobal.com/uk-ua/navchajtesya/blog/cili-informacijnoyi-bezpeki-ta-yih-znachennya> (дата звернення: 25.09.2025).
40. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union. 2016. L119. P. 1-88.
41. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union. 2022. L333. P. 80-152.
42. European Commission. The EU Cybersecurity Strategy for the Digital Decade. Brussels, 2020. URL: <https://digital-strategy.ec.europa.eu> (дата звернення: 16.10.2025).
43. European Union Agency for Cybersecurity (ENISA). Guidelines for SMEs on the security of personal data processing. 2021. URL: <https://www.enisa.europa.eu> (дата звернення: 16.10.2025).
44. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing. V4.0. 2017. URL: <https://cloudsecurityalliance.org> (дата звернення: 16.10.2025).
45. ISO/IEC 27001:2022. Information technology. Security techniques. Information security management systems. Requirements. Geneva: International Organization for Standardization, 2022. 36 p.

46. European Cyber Security Organisation (ECSO). Public-Private Partnership (PPP) in Cybersecurity. ECSO White Paper. 2021. URL: <https://ecs-org.eu> (дата звернення: 16.10.2025).
47. OECD. Enhancing the Role of SMEs in the Digital Transformation. Paris: OECD Publishing, 2021. 124 p.
48. NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology, 2018. 55 p.
49. ISACA. COBIT 2019 Framework: Governance and Management Objectives. Schaumburg, IL: Information Systems Audit and Control Association, 2019. 136 p.
50. PCI Security Standards Council. Payment Card Industry Data Security Standard (PCI DSS). Version 4.0. March 2022. 360 p. URL: <https://www.pcisecuritystandards.org> (дата звернення: 16.10.2025).
51. Axelos. ITIL Foundation: ITIL 4 Edition. London: TSO (The Stationery Office), 2019. 240 p.
52. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union. 2022. L333. P. 1-102.
53. Center for Internet Security. CIS Controls v8. URL: <https://www.cisecurity.org/controls> (дата звернення: 16.10.2025).
54. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Official Journal of the European Union. 2016. L 119. P. 1-88.
55. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD: NIST, 2018. 55 p.
56. Конвенція про кіберзлочинність (Будапештська конвенція) від 23.11.2001. Рада Європи. ETS № 185.
57. Закон України «Про інформацію» від 02.10.1992 № 2657-XII Відомості Верховної Ради України. 1992. № 48. Ст. 650.

58. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI Відомості Верховної Ради України. 2010. № 34. Ст. 481.
59. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII Відомості Верховної Ради України. 2017. № 45. Ст. 403.
60. Положення Національного банку України з питань інформаційної безпеки для банківських установ. Київ: НБУ, 2021. 54 с.
61. Бедер Д., Цаль-Цалко Ю. Формування економічних індикаторів національної безпеки в умовах цифровізації бізнесу та змін в економіці. *Society and Security*, 2024. № 1(2). С. 3-13.
62. Рой Я. В., Мазур Н. П., Складанний П. М. Аудит інформаційної безпеки – основа ефективного захисту підприємства. *Кібербезпека: освіта, наука, техніка*, 2018. № 1. С. 86-93.
63. Тулуп'єв А. О., Кваша С. В. Методичні підходи до оцінювання рівня захищеності інформації в комп'ютерних системах. *Інформаційна безпека людини, суспільства, держави*, 2017. № 1. С. 15-22.
64. Мурашко О. В. Інформаційна безпека підприємства: системний підхід до управління ризиками. *Бізнес Інформ*, 2019. № 2. С. 150-155.
65. Шевченко Л. І., Ткачук Л. С. Методика аналізу ризиків інформаційної безпеки в малому бізнесі. *Економіка та держава*. 2020. № 9. С. 32-36.
66. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства. *Інформаційна безпека людини, суспільства, держави: науковий журнал*, 2020. № 1 (27). С. 34-41.
67. Живко М.О., Руда О.І., Живко З.Б. Управління інформаційним забезпеченням системи економічної безпеки підприємства. *Східна Європа: економіка, бізнес та управління*, 2019. Випуск 2 (19). С.137-143.
68. Земко А.М., Вавдіюк Н.С., Лук'янчук Ю.А. Штучний інтелект у публічному секторі: етичні принципи, стандарти безпеки та відповідальність державних службовців. *Актуальні проблеми сталого розвитку*, 2025. № 2 (3). С. 151-156.

69. Бегун А.В. Інформаційна парадигма безпеки економічної системи. *Моделювання та інформаційні технології в економіці*, 2011. № 83. С. 144-151.
70. Добринін І., Радивілова Т., Мальцева Н., Агєєв Д. Формалізація оцінювання ризиків інформаційної безпеки на основі байєсівських мереж. *Захист інформації*, 2019. № 2. С. 25-33.
71. Замлинський В. А., Волошина О. В., Степаненко С. В. Облікова політика і економічна безпека в системі управління підприємством. *Український журнал прикладної економіки та техніки*, 2024. Том 9. № 1. С. 56-61.
72. Alberts C., Dorofee A. OCTAVE-S Implementation Guide Version 1.0: Technical Report. Pittsburgh : Carnegie Mellon University, 2001. 110 p.
73. CRAMM: Information Security Risk Analysis Method. Version 5.0. CCTA, UK, 2003. 142 p.
74. Дейнега І. О., Пиртко М. С. Актуалізація інформації як елемента економічної безпеки підприємства. *Економіка і регіон*, 2025. № 3 (98). С. 216-224.
75. Варналій З.С., Васильців Т.Г., Лупак Р.Л. Регіональні особливості розвитку підприємництва в Україні: монографія. Львів: ІРД НАНУ, 2024. 378 с.
76. Державна служба статистики України. URL: <https://statzvit.ukrstat.gov.ua/> (дата звернення: 16.10.2025).
77. Діяльність суб'єктів господарювання в Україні: статистичний збірник Державна служба статистики України. Київ : Держстат України, 2023. 156 с.
78. Платформа Дія.Бізнес. Аналітичний звіт про ефективність освітніх програм для МСБ. Київ, 2024. 94 с.
79. Господарський кодекс України від 16.01.2003 № 436-IV. URL: <https://zakon.rada.gov.ua/laws/show/436-15#Text> (дата звернення: 16.10.2025).
80. Слюсарєва Л., Компанієць В. Національні та регіональні програми підтримки брендингу малого та середнього бізнесу в Україні. *Сталий розвиток економіки*, 2026. 2 (59). С. 407-415.
81. Мазаракі А.А., Лагутін В.Д., Герасименко А.Г. Конкурентоспроможність підприємств: методологія та механізми забезпечення. Київ: Київський національний торговельно-економічний університет, 2023. 452 с.

82. Федулова Л.І. Інноваційний розвиток малого та середнього підприємництва в Україні. *Економіка і прогнозування*, 2024. № 2. С. 87-104.
83. Annual report on European SMEs 2022/2023. Brussels: EU Publications Office, 2023. 112 p.
84. Structural business statistics overview Eurostat. 2023. URL: <https://ec.europa.eu/eurostat> (дата звернення: 16.10.2025).
85. Number of SMEs in the European Union (EU) from 2008 to 2024 Statista. 2024. URL: <https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size> (дата звернення: 16.10.2025).
86. Економічна активність населення та підприємництво в умовах воєнного стану Державна служба статистики України, 2024. URL: <http://www.ukrstat.gov.ua> (дата звернення: 16.10.2025).
87. SME and Entrepreneurship Outlook 2023: Ukraine Country Profile. Paris: OECD Publishing, 2023. 84 p.
88. Digital transformation and SME resilience in times of crisis UNDP Ukraine. Київ: Програма розвитку ООН в Україні, 2023. 66 с.
89. Нестеренко О.М., Захарін С.В. Регіональна політика підтримки малого та середнього бізнесу в Україні. *Регіональна економіка*, 2024. № 3 (113). С. 45-58.
90. Бабій І., Баксалова О., Остапчук О. Механізм формування конкурентної політики малого підприємництва в післявоєнний період. *Innovation and Sustainability*, 2022. № 2. С. 123-130.
91. Андрієвич В. Тенденції розвитку суб'єктів малого бізнесу в Україні. *Науковий вісник Полісся*, 2025. № 2 (31). С. 98-111.
92. Дейнега І.О., Пиртко М. Економічна безпека підприємства: зміна парадигми. *Цифрова економіка та економічна безпека*, 2025. № 4 (19). С. 124-130.
93. Геєць В.М. Суперечності та перспективи економічного зростання на інноваційній основі в Україні. *Економіка України*, 2024. Т. 67, № 11 (756). С. 3-28.

94. Амоша О.І., Саломатіна Л.М. Інноваційний розвиток промислових підприємств у регіонах: проблеми та перспективи. *Економіка України*. 2024. № 3 (664). С. 20-34.
95. Васильців Т., Шопська Ю. Методико-прикладні аспекти формування регіональної політики забезпечення фінансової безпеки сектора малого підприємництва. *Modeling the Development of the Economic Systems*, 2022. № 3. С. 115-120.
96. Гонtareва І.В., Євтушенко В.А., Михайленко Д.Г. Стан та особливості розвитку підприємництва в повоєнний період. *Economic Synergy*, 2023. Вип. 2(8). С. 148-158.
97. Vavdiiuk N.S., Konstankevych I.V., Horodniuk M.S. Evaluation of digital transformation processes in the organization of beauty salon activities. *Вісник НУБГП. Серія «Економічні науки»*, 2024. № 1 (105). С. 50-55.
98. Кошовий Б.-П.О. Концептуальні засади забезпечення інформаційної безпеки суб'єктів підприємництва в системі комплементарного поєднання маркетингової та логістичної стратегій. *Актуальні питання економічних наук*, 2026. № 20. DOI: <https://doi.org/10.5281/zenodo.20513681> (дата звернення: 06.10.2025).
99. Бунтова Н., Томашук Ю. Проблеми та перспективи розвитку суб'єктів малого підприємництва у сфері послуг. *Економіка та суспільство*, 2024. № 64. DOI: <https://doi.org/10.32782/2524-0072/2024-64-130> (дата звернення: 06.10.2025).
100. OECD Digital for SMEs Global Initiative. OECD. URL: <http://surl.li/lgftth> (дата звернення: 16.10.2025).
101. Використання інформаційно-комунікаційних технологій на підприємствах. Державна служба статистики України. URL: <https://www.ukrstat.gov.ua/> (дата звернення: 16.10.2025).
102. Цифровізація для відновлення України. OECD. URL: <http://surl.li/fqctpn> (дата звернення: 12.09.2025).
103. Digital Economy and Society Index (DESI). Digital Economy and Society Index 2018 Report. URL: <http://surl.li/hqxfbj> (date of access: 15.09.2025).

104. ОЕСР започаткувала Програму для України. Урядовий портал. URL: <http://surl.li/bvuseb> (дата звернення: 06.10.2025).

105. The Digital Markets Act. European Commission. URL: <http://surl.li/utkahp> (дата звернення: 16.10.2025)..

106. The Digital Services Act. European Commission. URL: <http://surl.li/lioxak> (дата звернення: 16.10.2025).

107. Топалов В.М. Розвиток системи інформаційної безпеки суб'єктів малого підприємництва. *Бізнес-навігатор*, 2025. № 4 (81). URL: https://business-navigator.ks.ua/journals/2025/81_2025/36.pdf (дата звернення: 16.10.2025).

108. Топалов В. Інформаційна безпека як фактор стійкості та конкурентоспроможності суб'єктів підприємництва. Актуальні проблеми управління соціально-економічними системами: матеріали XI Міжнар. наук.-практ. конф., Частина 1. Луцьк, 5 груд. 2025 р., Луцьк: Надстир'я, 2025. С.86-89.

109. Кравчук І.М. Сучасні тенденції в управлінні бізнесом: адаптація до цифровізації. *Економічні науки: збірник наукових праць Луцького національного технічного університету*. Серія «Регіональна економіка», 2024. Випуск 21 (83). Луцьк: ВІП ЛНТУ. С. 138-147.

110. Димитрієв В. Державна політика розвитку інформаційної сфери в Україні: дис. ... канд. наук з держ. упр.: 25.00.02 – механізми державного управління. Житомир, 2024. 200 с.

111. ENISA. Cybersecurity for SMEs: Challenges and Recommendations. European Union Agency for Cybersecurity, 2021. URL: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf> (дата звернення: 30.06.2025)

112. Deloitte Belgium. MXDR by Deloitte (Managed Extended Detection & Response). Брюссель: Deloitte Belgium, 2023. URL: https://eulisaroundtable.eu/eulisa_content/uploads/2023/06/Deloitte_IRJune23.pdf (дата звернення: 30.06.2025).

113. Carlos Rombaldo Jr., Ingolf Becker, Shane Johnson. Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. arXiv, 2023. URL: <https://arxiv.org/abs/2309.17186> (дата звернення: 30.06.2025)

114. Cybersecurity Budget as a Percentage of Revenue. Decypher Technologies URL: <https://decyphertech.com/cybersecurity-budget-as-a-percentage-of-revenue/> (дата звернення: 30.06.2025).

115. Does More Cyber Spending Mean More Cyber Security? Zeta Sky URL: <https://www.zetasky.com/post/does-more-cyber-spending-mean-more-cyber-security/> (дата звернення: 30.06.2025).

116. How Much Should Your SMB Budget for Cybersecurity? Business.com URL: <https://www.business.com/articles/smb-budget-for-cybersecurity/> (дата звернення: 30.06.2025)

117. Офіційний сайт YouControl. Повне досьє на кожну компанію України. URL: <https://youcontrol.com.ua/> (дата звернення: 16.10.2025).

118. Топалов В. Інформаційна безпека як фактор стійкості та конкурентоспроможності суб'єктів підприємництва. Актуальні проблеми управління соціально-економічними системами: матеріали XI Міжнар. наук.-практ. конф., Частина 1. Луцьк, 5 груд. 2025 р., Луцьк: Надстир'я, 2025. С.86-89.

119. Барабась Д., Панасюк О., Кривонос А. Формування цифрових конкурентних переваг компанії. *Mechanism of an Economic Regulation*, 2023. № 2 (100). Р. 12-18.

120. Ситник Н., Себестянович І. Цифровізація та її вплив на розвиток малого та середнього бізнесу. *Грааль науки*, 2022. № 11, С. 50-52.

121. Нікітенко В., Метеленко Н., Шапуров О. Концепція цифрової трансформації як чинник підтримки сталого екологічного, соціального та економічного розвитку. *Humanities studies: Collection of Scientific Papers*, 2022. № 12 (89). Р. 142-152.

122. Саврас І.З., Фединець Н.І. Цифровізація та інноваційний розвиток підприємства: тенденції, проблеми та перспективи. *Вісник Львівського*

торговельно-економічного університету. *Економічні науки*, 2023. № 74. С. 108-114.

123. Горохова Т. Стратегії використання цифрових інструментів у діяльності малого та середнього бізнесу під час економічної кризи. *Економіка та суспільство*, 2022. № 39. DOI: <https://doi.org/10.32782/2524-0072/2022-39-12> (дата звернення: 16.10.2025).

124. Кишакевич Б.Ю., Демедюк Б.Т., Сисюк В.І. Цифровізація малого та середнього бізнесу: виклики та перспективи. *Інвестиції: практика та досвід*, 2024. № 2. URL: <https://www.nayka.com.ua/index.php/investplan/article/view/2805> (дата звернення: 16.10.2025).

125. Струтинська І., Дмитроца Л., Сороківська О., Козбур Г. Особливості цифрового розвитку малого і середнього бізнесу України, країн Європи та G7. Трансформація бізнесу для сталого майбутнього: дослідження, цифровізація та інновації: колективна монографія, Тернопіль, 2024. С. 411-427.

126. Розвиток цифровізації обліку, оподаткування, аналізу і контролю в управлінні підприємствами: монографія: Р.Ф. Бруханський, П.Р. Пуцентейло [та ін.]. Тернопіль: ВПЦ «Університетська думка», 2021. 194 с.

127. Трубачева С., Мушка О., Замаскіна П. Особливості проектування освітнього середовища в умовах цифровізації суспільства під час воєнного стану в Україні. *Український Педагогічний журнал*, 2023. № 4. С. 46-52.

128. Візія Відновлення України: «Сильна європейська країна – магніт для іноземних інвестицій». План відновлення України. URL: <https://recovery.gov.ua/> (дата звернення: 28.07.2025).

129. Загальний регламент про захист даних (GDPR). GDPR Text, Translation and Commentary. URL: <https://gdpr-text.com/uk/> (дата звернення: 04.08.2025).

130. Alm R., Wissotzki M. TOGAF Adaption for Small and Medium Enterprises. University of Rostock, 2015. URL: https://www.wissdoc.com/uploads/alm_togaf_sme.pdf (дата звернення: 30.06.2025).

131. Hidayat R. S., Indrajit R. E., Dazki E. TOGAF's Approach in Developing an Enterprise Architecture for the Information Technology Security Industry. *Journal La Multiapp*, 2024. Vol. 5, P. 630-645.

132. The Open Group. The TOGAF Standard. Version 10. Reading (UK): The Open Group, 2022. URL: <https://pubs.opengroup.org/togaf-standard> (дата звернення: 30.06.2025).

133. The Open Group Security Forum. Integrating Risk and Security within a TOGAF Enterprise Architecture. The Open Group, 2016. URL: <https://publications.opengroup.org/w123> (дата звернення: 30.06.2025).

134. McClintock M., Falkner K., Szabo C., Yarom Y. Enterprise Security Architecture: Mythology or Methodology? Proceedings of the 15th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2020), 2020. P. 171-178.

135. Mayer N., Aubert J., Grandry E., Feltus C., Goettelmann E. An Integrated Conceptual Model for Information System Security Risk Management and Enterprise Architecture based on TOGAF, ArchiMate, IAF and DoDAF. arXiv.org, 2017. URL: <https://arxiv.org/abs/1704.08455> (дата звернення: 30.06.2025).

136. Tam T., Rao A., Hall J. Structuring the Chaos: Enabling Small Business Cyber-Security Risks & Assets Modelling with a UML Class Model. arXiv.org, 2024. URL: <https://arxiv.org/abs/2402.00190> (дата звернення: 30.06.2025).

137. Buriak I., Petchenko M. Analysis of the dilemmas of building an accounting system for the needs of future economic management. *Futurity Economics&Law*, 2021. № 1. P. 17-23.

138. Costa Melo D.I., Queiroz G.A., Alves Junior P.N., Sousa T.B., Yushimito W.F., Pereira J. Sustainable digital transformation in small and medium enterprises (SMEs): A review on performance. *Heliyon*, 2023. № 9(3), URL: <https://doi.org/10.1016/J.HELİYON.2023.E13908> (дата звернення: 30.06.2025).

139. Shah N., Zehri A. W., Saraih U. N., Abdelwahed N. A. A., Soomro B. A. The role of digital technology and digital innovation towards firm performance in a digital economy. *Kybernetes*, 2023. № 53(2), P. 620-644.

140. Rajala A., Hautala-Kankaanpää T. Exploring the effects of SMEs' platform-based digital connectivity on firm performance. The moderating role of environmental turbulence. *Journal of Business & Industrial Marketing*, 2022. № 38(13). P. 15-30.
141. Lemonakis C., Vassakis K., Tabouratzi E., Tsoukatos E. Determinants of technological and non-technological innovation in SMEs: The case of crete. *Global Business and Economics Review*, 2018. № 20 (5/6). P. 544.
142. Bagheri M., Mitchelmore S., Bamiatzi V., Nikolopoulos K. Internationalization orientation in SMEs: the mediating role of technological innovation. *Journal of International Management*, 2019. № 25(1). P. 121-139.
143. Naushad M., Sulphrey M. M. Prioritizing technology adoption dynamics among SMEs. *TEM Journal*, 2020. № 9(3). P. 983-991.
144. Thathsarani U.S., Jianguo W. Do digital finance and the technology acceptance model strengthen financial inclusion and SME performance? *Information*, 2022. № 13(8). P. 390.
145. The Digital Transformation of SMEs, OECD Studies on SMEs and Entrepreneurship, OECD Publishing, 2021. Paris, DOI: <https://doi.org/10.1787/bdb9256a-en> (дата звернення: 30.06.2025).
146. Klymchuk M. Methodology for managing investment processed of digitalization of the economy. *Innovation and Sustainability*, 2022. № 1. P. 20-33.
147. Методологія керування бізнесом в умовах цифровізації: монографія / А.П. Гринько, П.Л. Гринько, Н.Г. Ушакова, Т.В. Андросова, О.А. Кулініч, І.І. Помінова. Х.: Монограф, 2022. 199 с.
148. Кошовий Б.-П.О. Інформаційно-аналітичне забезпечення комплементарної маркетингово-логістичної стратегії логістичних підприємств в контексті діджиталізації та інформаційної безпеки. *Наукові записки Львівського університету бізнесу та права*, 2026. № 49. DOI: <https://doi.org/10.66556/2663-0117.49.koshovyi-b> (дата звернення: 30.06.2025).
149. Гавриленко Н.Г., Тарасенко І.О. Сучасні тенденції цифровізації економіки: проблеми та перспективи розвитку. *Міжнародний науковий журнал «Інтернаука». Серія: Економічні науки*. 2021. № 3 (47). Т. 1. С. 36-46.

150.Гражевська Н.І., Чигиринський А.М. Цифрова трансформація економіки в умовах посилення глобальних ризиків і загроз. *Економіка та держава*, 2021. № 8. С. 53-57.

151.Мельничук Г.С., Мамалига В.О. Цифровізація економіки: можливості та загрози для ефективного функціонування підприємств. *Приазовський економічний вісник*, 2020. № 2 (19). С. 125-130.

152.Струтинська І.В. Дефініції поняття «цифрова трансформація». Науково-практичний журнал *Причорноморські економічні студії*, 2019. Вип. 48 (2). С. 91-96.

153.Тульчинська С.О., Корзун Л.С. Цифровізація як засіб трансформації економіки України. *Сучасні проблеми економіки і підприємництва*, 2020. Вип. 25 С. 52-59.

154.Фролова Л.В., Бойко І.М. Трансформація підприємництва в умовах цифрової економіки. *Економіка: реалії часу*, 2021. № 2 (54). С. 47-56.

155.Воронкова В.Г., Нікітенко В.О. Цифрова трансформація промислового підприємства: науково-методичний посібник для здобувачів вищої освіти ступеня доктора філософії у галузі знань 07 «Управління та адміністрування» спеціальності 073 «Менеджмент». Запоріжжя : ЗНУ, 2023. 158 с.

156.Сороколіт М. Аудит інформаційної безпеки в умовах автоматизації облікових даних вітчизняних підприємств. *Herald of Khmelnytskyi National University. Economic Sciences*, 2025. № 3(2). С. 61-66.

157.Лахно В., Блозва А., Часновський Є., Криворучко О., Десятко А. Аудит інформаційної безпеки на основі застосування нейро-нечіткої системи. *Технічні науки та технології*, 2021. № 3. С. 125-137.

158.Хох В. Д. Автоматизована система проведення аудиту інформаційної безпеки комп'ютерних систем та мереж. *Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація*, 2018. Вип. 31. С. 174-181.

159. Хаджинова О., Хаджинова М. Аудит інформаційної безпеки. *Вісник Приазовського державного технічного університету*. Серія: Економічні науки, 2024. № 1 (40). С. 9-19.
160. Мазур Н.П., Рой Я.В. Аудит інформаційної безпеки – основа ефективного захисту підприємства. *Кібербезпека: освіта, наука, техніка*, 2018. № 1. С. 86-93.
161. Мурашко О.В. Інформаційна безпека в умовах цифровізації: виклики для малого бізнесу. *Економіка та держава*, 2021. № 6. С. 54-59.
162. Косінський П.М., Малишко С.О. Підвищення рівня інформаційної безпеки переробних підприємств в умовах «зеленого» розвитку економіки. *Здобутки економіки: перспективи та інновації*, 2026. № 29. DOI: <https://doi.org/10.5281/zenodo.20138139> (дата звернення: 16.10.2025).
163. Петров В. Інформаційна безпека підприємств: концептуальні засади та механізми забезпечення. *Економічна безпека в умовах цифрової трансформації*, 2020. Київ: Наукове видавництво. С. 112-125.
164. Іваненко О. Проблеми та перспективи інформаційної безпеки малого та середнього бізнесу. *Журнал інформаційних технологій та кібербезпеки*, 2018. №3 (15). С. 45-57.
165. Коваленко Н. Управління ризиками інформаційної безпеки в підприємницькій діяльності. *Сучасні інформаційні системи і технології*, 2021. Т. 5, №2. С. 87-99.
166. Григоренко Т. Захист інформаційних активів підприємств у цифровій економіці. *Інформаційна безпека та управління даними*, 2019. № 4 (22). С. 33-48.
167. Сидоренко Ю. Роль інформаційної безпеки у формуванні конкурентних переваг підприємств. *Стратегічні напрями розвитку цифрової економіки*, 2022. С. 55-70.
168. Акімова Н.С., Кирильєва Л.О., Наумова Т.А. Інформаційна безпека підприємств торгівлі в умовах становлення глобального інформаційного суспільства. *Підприємництво і торгівля*, 2023. № 35. С. 5-10.

169. Кір'ян О., Кононенко Я., Торяник Д. (2022). Інформаційна складова економічної безпеки організації. *Цифрова економіка та економічна безпека*, 2022. № 3. С. 79-84.

170. Косінський П.М., Малишко С.О. Теоретичні основи формування політики інформаційної безпеки підприємства в умовах «зеленої» трансформації. *Економіка та суспільство*, 2026. Вип. URL: <https://doi.org/10.32782/2524-0072/2026-85-172> (дата звернення: 16.10.2025).

171. Дмитренко А. Безпека інформаційного простору контролінгової інформації при здійсненні спільної діяльності. *Економіка та суспільство*, 2023. № 56. DOI: <https://doi.org/10.32782/2524-0072/2023-56-84> (дата звернення: 15.08.2025).

172. Топалов В.М. Забезпечення інформаційної безпеки бізнесу України в умовах сучасних загроз. *Цифрова економіка та економічна безпека*, 2024. № 6 (15). С. 157-161.

173. Рибальченко Л.В., Гребенюк А.М. Стандарти управління інформаційною безпекою. Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 22 листопада 2019 р. Одеса: ОДУВС, 2019. 108 с.

174. Топалов В. Напрями цифровізації сільськогосподарських підприємств. Цифрова трансформація: виклики та стратегії: матеріали Міжнародної науково-практичної конференції, 25 лютого 2025 р., м. Луцьк: ЛНТУ, 2025. С. 73-75.

175. Кицюк В.М., Пупинін О.С. Інформаційна безпека підприємства: теоретичний аспект. *Сучасний захист інформації*, 2024. № 2 (58), С. 103-108.

176. Лисецький Ю.М., Калбазов Д.Й. Підходи до забезпечення інформаційної безпеки. *Математичні машини і системи*, 2023. № 4. С. 26-32.

177. Старостін О.Ю. Забезпечення інформаційної безпеки як складової національної безпеки України. *Вісник Кримінологічної асоціації України*, 2026. № 31 (1). С. 466-474.

178. Бедер Д., Цаль-Цалко Ю. Формування економічних індикаторів національної безпеки в умовах цифровізації бізнесу та змін в економіці. *Society and Security*, 2024. 1 (2). С. 3-13.

179. Топалов В. Чинники впливу на забезпечення інформаційної безпеки суб'єктів малого підприємництва. Підприємництво та бізнес-адміністрування: відновлення, сталий розвиток та інновації у післявоєнний час: матеріали Міжнародної науково-практичної інтернет конференції, 1-28 лютого 2025 р. Харків. С. 167-168.

180. Данілова Е.І. Концепція системного підходу до управління економічною безпекою підприємства: монографія. Вінниця: Європейська наукова платформа, 2020. 342 с.

181. Ковальська Л., Голій О., Голій В. Економічна безпека підприємства: сутність, структура та механізм забезпечення. *Економічний форум*, 2023. Том 1. № 2. С. 126-137

182. Куркова К.М. Концептуальне розуміння національної безпеки у публічно-інформаційній сфері. *Наукові записки*, 2025. № 18. С. 343-347.

183. Шевчук М. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського Національного Університету*, 2023. Вип. 78. Ч. 2. С. 134-139.

184. Цимбалюк І.О., Павліха Н.В. Інклюзивна економіка: шлях до соціальної рівності та економічного розвитку: монографія. Луцьк : Вежа-Друк, 2023. 320 с.

185. Балабан П. Ю., Овсієнко А. М. Малий бізнес у сфері торгівлі: практико-орієнтована методика оцінки ефективності діяльності підприємств. *Науковий вісник Полтавського університету економіки і торгівлі. Серія: Економічні науки*, 2022. № 1 (105). С. 7-14.

186. Топалов В.М. Стратегічні орієнтири забезпечення інформаційної безпеки суб'єктів малого підприємництва. *Економіка та суспільство* № 75 *Економіка та суспільство*, 2025. № 75. DOI: <https://doi.org/10.32782/2524-0072/2025-75-92> (дата звернення: 16.10.2025).

187.Белянська Ю.В. Економічна сутність та значення інновацій в сучасних умовах господарювання. *Review of Transport Economics and Management*, 2020. № 4 (20). С. 55-65.

188.Бережницька У.Б. Інституціональне середовище розвитку малого та середнього підприємництва. *Review of Transport Economics and Management*, 2021. № 5 (21). С. 21-29.

189.Бортнік С.М. Функціонування малого і середнього підприємництва в Україні: сучасний стан та перспективи розвитку. *Економіка та суспільство*, 2022. № 36. DOI: <https://doi.org/10.32782/2524-0072/2022-36-46> (дата звернення: 15.08.2025).

190.Василець Н.М. Наукові підходи до розвитку малого бізнесу в умовах війни: монографія. Київ: *Науково-освітній інноваційний центр суспільних трансформацій*, 2022. С. 110-121.

191.Вітковський Ю.П., Смігунова О. В., Дудник О. В. Роль і значення малого підприємництва у формуванні стратегії розвитку економіки країни. *Український журнал прикладної економіки та техніки*. 2022. Т. 7, № 1. С. 107-113.

192.Гуцалюк О.М., Бондар Ю.А., Бойко О.В. Інноваційно-інтегрований розвиток монопрофільних виробничих структур транспортного ринку національної економіки. *Економічний вісник Донбасу*, 2024. № 3. С. 13-20.

193.Топалов В.М. Формування інституційної моделі забезпечення інформаційної безпеки бізнесу в регіоні. *Економічні науки: збірник наукових праць*. Серія Регіональна економіка, 2025. Випуск 22 (87). Редкол.: відп. ред. д.е.н., професор Л.Л. Ковальська. Луцьк : ВІП ЛНТУ. С.503-516.

194.Шовкун-Заблоцька Л.В. Формування ефективного механізму інноваційного менеджменту на підприємствах. *Вчені записки*. 2024. № 36 (3).

195.Ковтун Т. Зарубіжний досвід підтримки бізнесу в період криз та глобальних загроз. *Наукові перспективи*, 2022. № 9 (16). С. 11-23.

196.Соснов І.І., Іпполітов Є. М. Стратегічне забезпечення інформаційної безпеки підприємства. *Підприємництво і торгівля*, 2025. № 47. С. 141-149.

197.Задоя В.О. Інституційні та управлінські аспекти забезпечення економічної безпеки бізнесу в умовах цифрової економіки. *Ефективна економіка*. 2025. № 7. DOI: <https://doi.org/10.32702/2307-2105.2025.7.71%20> (дата звернення: 22.10.2025).

198. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. Київ, 2025. № 10. 166 с.

199. Терзі О. Принципи забезпечення інформаційної безпеки держави: досвід України та зарубіжних країн. *Право та державне управління*, 2024. № 3. С. 51-57.

200. Шовкун-Заблоцька Л.В. Механізм формування конкурентоспроможності підприємницьких структур у сфері агробізнесу. *Вчені записки*, 2023. № 33 (4). С. 178-195.

201. Котусєв С. Стандарт TOGAF, 10-те видання: Що нового? Мельбурн, Австралія: SK Publishing, 2023. 56 с.

202. OECD. Digital Security Policy for the Digital Transformation of SMEs: OECD Recommendation. Paris: OECD Publishing, 2021. 40 p.

203. ENISA. Cybersecurity Training for SMEs. – European Union Agency for Cybersecurity, 2020. URL: <https://www.enisa.europa.eu> (дата звернення: 22.10.2025).

204. ENISA. Public-Private Cooperation for Cybersecurity. *European Union Agency for Cybersecurity*, 2022. URL: <https://www.enisa.europa.eu> (дата звернення: 22.10.2025).

205. ENISA. Cybersecurity Standards and Guidelines. *European Union Agency for Cybersecurity*, 2023. URL: <https://www.enisa.europa.eu> (дата звернення: 22.10.2025).

206. Kshetri N. Cybersecurity Management for SMEs. In: *Cybersecurity for Small and Medium Enterprises*. Springer, 2019. P. 13-32.

207. European Commission. An SME Strategy for a Sustainable and Digital Europe. – Brussels: EC, 2021. 22 p.

208. Кравчук І. Управління інформаційною безпекою суб'єктів господарювання: сучасні підходи та інструменти. *Грааль науки*, 2026. № 68. С. 625-631.

209. Коробка С.В. Особливості релокації малого підприємництва в умовах війни. *Проблеми сучасних трансформацій. Серія: економіка та управління* 2023. № 7. DOI: <https://doi.org/10.54929/2786-5738-2023-7-04-14> (дата звернення: 22.10.2025).

210. Topalov V. Prospects for ensuring information security of business entities as a vector of their sustainable development. *Global Prosperity*, 2025. № 5 (3). URL: <https://gprosperity.org/index.php/journal/article/view/245>

ДОДАТКИ

**Інформація про суб'єкти малого підприємництва Волинської області,
які взяли участь у опитуванні щодо стану їх інформаційної безпеки**

Суб'єкти підприємництва	Сайти	Види діяльності
ТОВ «Espresso Lab»	https://espressolab.com.ua/	Продаж кавового обладнання
ТзДВ «Елтех»	https://www.eltech.com.ua/	Виробництво обладнання для намотки
ТОВ «Августіно»	https://avgustino.com.ua	Виробництво кондитерських виробів
ТОВ «Добра Кухня»	https://www.dobra-kukhnia.com.ua	Виробництво напівфабрикатів з натуральної сировини
ТОВ «Хімпласт»	https://himplast.lutsk.ua	Виробництво поліетиленової плівки
ТОВ «КаДар-Україна»	https://kadar.ua/	Виробництво взуття «КаДар»
ФОП «Райсон»	https://rayson.com.ua	Виробництво домашнього текстилю
ТОВ «Татрафан»	https://tatrafan.ua/	Виробництво полімерної гнучкої упаковки
ТОВ «СМ-хім»	https://smhim.com.ua	Виробництво засобів побутової хімії.
ПП «Артеспресо»	https://www.ukraine.com.ua/egrpou	Продаж кавового обладнання та його сервіс
ТОВ «Бест Бебі Комфорт»	https://deson.com.ua	Виробництво дитячих меблів
ТОВ «Атлант-Плюс»	https://www.atlantplus.com.ua	Виробництво металопластикових вікон, алюмінієвих конструкцій, корпусних меблів
ФОП «Стохід»	https://stohid.in.ua	Виробництво тактичного спорядження
ПП «Аква Прінт»	https://aqua-print.com.ua	Послуги зовнішньої реклами на вулицях, фасадах будівлі, транспорті.
ФОП «Creative Play»	https://creativeplay.com.ua	Виробництво дитячих ігрових та спортивних майданчиків
ТОВ «Віва»	https://chocoboom.com.ua	Виробництво кондитерських виробів
ПрАТ «ВГП»	https://www.ruta.ua	Виробництво продукції санітарно-гігієнічного призначення
ФОП «Black Mirror»	https://blackmirror.com.ua	Виробництво дзеркал
ПП «Гарна хата»	https://garnahata.ua	Послуги ремонту будівель (натяжні стелі)
ПП «Vinvest»	https://vinvest.top	Виробництво МАФів, кіосків, торгових причепів, ресепшинів та торгових острівків

Скільки приблизно ваш бізнес витрачає щорічно на інформаційну безпеку?

- ☐ Менше 10 000 грн
- ☐ 10 000 – 50 000 грн.
- ☐ 50 001 – 200 000 грн
- ☐ Понад 200 000 грн
- ☐ Не виділяємо окремого бюджету

Яка сума збитків вашого бізнесу, спричинена інформаційними атаками, за останні 5 років?

- ☐ 0 грн (жодних збитків)
- ☐ До 20 000 грн
- ☐ 20 001 – 100 000 грн
- ☐ Понад 100 000 грн
- ☐ Не знаю точно



Чи існує в компанії документовані політики інформаційної безпеки?

- ☐ Так, є затверджені політики й регулярно оновлюються
- ☐ Так, але застарілі та не оновлюються
- ☐ Ми тільки розробляємо такі політики
- ☐ Немає жодного документу

Як часто проводяться внутрішні аудити або перевірки інформаційної безпеки?

- ☐ Щоквартально
- ☐ Раз на пів року
- ☐ Раз на рік
- ☐ Лише у разі підозрілих інцидентів
- ☐ Ніколи не проводили

Чи є в компанії призначена відповідальна особа (або команда) за інформаційну безпеку?

- ☐ Так, у нас є спеціалізована служба/спеціаліст

продовження Додатку Б2

Чи є в компанії призначена відповідальна особа (або команда) за інформаційну безпеку?

- ☐ Так, у нас є спеціалізована служба/спеціаліст
- ☐ Призначена, але виконує обов'язки за сумісництвом
- ☐ Поки що плануємо призначити
- ☐ Ніхто конкретно не відповідає

Який рівень обізнаності співробітників щодо фішингових атак та соціальної інженерії?

- ☐ Ми регулярно проводимо тренінги та перевірки (наприклад, фейкові розсилки)
- ☐ Тренінги були одного разу, більше не проводили
- ☐ Співробітники поінформовані лише поверхнево
- ☐ Такого навчання взагалі не було

Які засоби захисту використовуються для захисту корпоративної мережі? (можна вибрати кілька)

- ☐ Фаєрвол (апаратний чи програмний)
- ☐ Антивірус/антикорупційне ПЗ
- ☐ Система виявлення та запобігання вторгненням (IDS/IPS)
- ☐ Віртуальні приватні мережі (VPN)
- ☐ Жодного зі згаданих

Чи використовує ваша компанія багатофакторну аутентифікацію (MFA) для доступу до критичних систем?

- ☐ Так, на всіх облікових записах
- ☐ Частково – лише для ключових співробітників
- ☐ Плануємо впровадити найближчим часом
- ☐ Ні, не використовуємо

продовження Додатку Б2

Як часто ви робите резервне копіювання критичних даних?

- ☐ Щоденно
- ☐ Щотижня
- ☐ Раз на місяць
- ☐ Лише за необхідності/рідко
- ☐ Не робимо зовсім

Де зберігаються резервні копії?

- ☐ Виключно локально (на внутрішніх серверах)
- ☐ Виключно у хмарі (SaaS/PaaS)
- ☐ Комбінація «локально + у хмарі»
- ☐ Інколи створюємо, але місце зберігання невизначене
- ☐ Не створюємо резервних копій

Чи проводили ви тестування на проникнення (пенетраційне

Чи проводили ви тестування на проникнення (пенетраційне тестування) чи зовнішній аудит інформаційної безпеки за останні 2 роки?

- ☐ Так, незалежними фахівцями (зовнішній аудит)
- ☐ Так, внутрішнім IT-відділом
- ☐ Плануємо найближчим часом
- ☐ Ніколи не проводили

Скільки часу займає у вас виявлення серйозного інциденту безпеки (приклад: злам, зловмисна активність)?

- ☐ Менше ніж 1 день
- ☐ 1–3 дні
- ☐ 4–7 дні
- ☐ Понад 7 днів
- ☐ Не проводили вимірювання

продовження Додатку Б2

Чи є у вас план реагування на інциденти (Incident Response Plan)?

- ☐ Так, документований і перевірений у практиці
- ☐ Є, але не тестувався на реальних кейсах
- ☐ Розробляється зараз
- ☐ Немає взагалі

Чи використовує компанія шифрування для захисту конфіденційних даних (на дисках чи при передачі)?

- ☐ Так, апаратне та програмне шифрування для всіх пристроїв
- ☐ Лише програмне шифрування на ноутбуках/флешках
- ☐ Тільки SSL/TLS для передачі даних
- ☐ Ні, не використовуємо шифрування



Чи застосовується у вас політика «принципу найменших привілеїв» (least privilege) для доступу співробітників до інформаційних систем?

Чи застосовується у вас політика «принципу найменших привілеїв» (least privilege) для доступу співробітників до інформаційних систем?

- ☐ Так, кожен співробітник має мінімально необхідний набір прав
- ☐ Частково – обмежуємо доступ лише до ключових систем
- ☐ Плануємо впровадити
- ☐ Ні, всі мають доступ до більшості ресурсів

Чи використовуєте ви систему страхування кіберризиків (cyber insurance)?

- ☐ Так, маємо поліс із покриттям основних ризиків
- ☐ Розглядаємо, але ще не оформляли
- ☐ Ми не вважаємо це за необхідне
- ☐ Не знаємо, що це таке



Як часто оновлюється програмне забезпечення (ОС, бізнес-застосунки)?

продовження Додатку Б2

Як часто оновлюється програмне забезпечення (ОС, бізнес-застосунки) на ваших робочих станціях і серверах?

- ☐ Автоматично, щойно виходить патч
- ☐ Раз на тиждень
- ☐ Раз на місяць
- ☐ Лише у разі критичних вразливостей
- ☐ Ніколи не оновлюємо систематично

Чи перевіряєте ви надійність і безпечність постачальників/підрядників, які мають доступ до ваших ІТ-систем або даних?

- ☐ Завжди вимагаємо підтвердження сертифікатів та звітів із аудиту
- ☐ Перевіряємо лише найбільших постачальників
- ☐ Перевіряємо після підозрілих інцидентів
- ☐ Не перевіряємо взагалі

Який інструмент чи сервіс ви використовуєте для захисту електронної пошти?

- ☐ Вбудовані антивірус/спам-фільтри провайдера
- ☐ Спеціалізований шлюз або хмарний сервіс (наприклад, Proofpoint, Mimecast)
- ☐ DMARC/DKIM/SPF без сторонніх сервісів
- ☐ Нічого окремо не використовуємо

На який рівень інвестицій в інформаційну безпеку ви готові збільшити витрати у наступному році, виходячи з потреб і ризиків?

- ☐ Не плануємо збільшувати (залишимо на тому ж рівні)
- ☐ До 10 % збільшення бюджету
- ☐ 10 % – 25 % збільшення бюджету
- ☐ Понад 25 % збільшення бюджету
- ☐ Ще не визначилися, залежить від ситуації в майбутньому



Принципи аудиту інформаційної безпеки підприємства

Принцип аудиту	Приклад реалізації	Практичні індикатори
Системність	Оцінювання усіх підсистем: ІТ-інфраструктури, політик, персоналу	Наявність аудиторських чек-листів для кожної сфери
Інтегрованість	Врахування взаємозв'язку між технічними і організаційними заходами	Звіт із взаємозв'язками між уразливостями та політиками
Пропорційність	Фокус на критичних зонах безпеки в умовах обмежених ресурсів	Зменшення витрат на аудит при збереженні ефективності
Актуальність	Використання актуальних стандартів (наприклад, ISO 27001:2022)	Наявність посилань на міжнародні стандарти в документації
Безперервність	Запровадження щорічного аудиту та моніторингу змін	Документовані результати повторних аудитів
Конфіденційність	Підписання угод про нерозголошення результатів аудиту	Контроль доступу до звітів та аудитних матеріалів
Незалежність	Залучення зовнішніх експертів, не пов'язаних із компанією	Акт перевірки, підписаний незалежною стороною
Практичність	Рекомендації з чітким планом впровадження та бюджетом	Кількість реалізованих рекомендацій у визначений термін
Орієнтація на ризики	Проведення оцінки на основі матриці ризиків	Звіт з ризик-матрицею з оцінками впливу/ймовірності
Залучення персоналу	Інтерв'ю та опитування персоналу під час аудиту	Рівень обізнаності персоналу (оцінено анкетуванням)



УКРАЇНА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

вул. Львівська, 75, м. Луцьк, 43018, тел.: +38(0332)74-61-03

e-mail: rector@lntu.edu.ua, web: www.lntu.edu.ua

код ЄДРПОУ 05477296

18.03.2026 р. № 805/01-14

на № _____ від _____

АКТ

про використання результатів дисертаційного дослідження аспіранта кафедри
 підприємництва, торгівлі та логістики

Луцького національного технічного університету

Топалова Романа Миколайовича

на тему: «**Цифрові трансформації логістичних систем підприємств**»
 представлена на здобуття наукового ступеня доктора філософії при виконанні
 науково-дослідних робіт кафедри підприємництва, торгівлі та логістики
 Луцького національного технічного університету

Цим актом підтверджується, що результати дисертаційного дослідження аспіранта Топалова Романа Миколайовича використано при виконанні науково-дослідних робіт кафедри підприємництва, торгівлі та логістики Луцького національного технічного університету «Оптимізація логістичних потоків під впливом воєнних дій в Україні» (номер державної реєстрації 0123U101523) та «Механізми публічного управління та адміністрування сталим розвитком територіальних громад» (номер державної реєстрації 0126U002918).

Зокрема, при виконанні цих науково-дослідних робіт Топаловим Р.М. здійснено обґрунтування моделі цифрової трансформації логістичної системи підприємства, впровадження якої дозволить забезпечити реалізацію етапів цифрової трансформації, оптимізувати логістичні потоки та логістичні бізнес-процеси на підприємстві; розроблено концепт здійснення цифрових трансформацій логістичної системи підприємства, реалізація якого сприяє підвищенню результативності її функціонування, а також сталості, безпечності та конкурентоспроможності територіальних громад.

Проректор
 з науково-педагогічної роботи
 та досліджень



Олена ЛЮТАК



УКРАЇНА

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**

вул. Львівська, 75, м. Луцьк, 43018, тел.: +38(0332)74-61-03

e-mail: rector@lntu.edu.ua, web: www.lntu.edu.ua

код ЄДРПОУ 05477296

18.03.2020р № 804/01-14

на № _____ від _____

АКТ

про використання результатів дисертаційного дослідження аспіранта кафедри підприємництва, торгівлі та логістики
Луцького національного технічного університету
Топалова Володимира Миколайовича
на тему: «**Забезпечення інформаційної безпеки суб'єктів підприємництва**»
представленої на здобуття наукового ступеня доктора філософії при виконанні науково-дослідних робіт кафедри підприємництва, торгівлі та логістики Луцького національного технічного університету

Цим актом підтверджується, що результати дисертаційного дослідження аспіранта Топалова Володимира Миколайовича використано при виконанні науково-дослідних робіт кафедри підприємництва, торгівлі та логістики Луцького національного технічного університету «Потенціал синергії управління, логістики та інновацій як основа розвитку кросрівневої підприємницької діяльності» (номер державної реєстрації 0126U002654).

Зокрема, при виконанні цієї науково-дослідної роботи Топаловим В.М. здійснено обґрунтування алгоритму аналізу та оцінки інформаційної безпеки суб'єктів підприємницької діяльності, що дозволяє виявити рівні її забезпечення; визначення можливих ризиків порушення інформаційної безпеки підприємства та кореляційної залежності обсягів доходів суб'єктів підприємництва та рівня витрат на забезпечення інформаційної безпеки, що сприятиме виявленню ролі інформаційної безпеки у зміцненні конкурентоспроможності малого бізнесу в умовах цифрової трансформації та загроз зовнішнього середовища.

Проректор
з науково-педагогічної роботи
та досліджень



Олена ЛЮТАК



ВОЛИНЬСЬКА ОБЛАСНА РАДА

майдан Київський, 9, м. Луцьк, 43027, тел. (0332) 778 300,
e-mail: post@volynrada.gov.ua, web: https://new.volynrada.gov.ua, код ЄДРПОУ 00022444

08.05.2026 № 431/51/2-26 на № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження аспіранта кафедри
підприємництва, торгівлі та логістики
Луцького національного технічного університету
Топалова Романа Миколайовича
на тему: «Цифрові трансформації логістичних систем підприємств»

Довідка видана здобувачу наукового ступеню доктора філософії Топалову Р.М. в тому, що наукові положення дисертаційного дослідження було враховано в процесі здійснення цифрових трансформаційних змін на підприємствах Волинської області. Зокрема, цікавим є підхід автора щодо розробки механізму здійснення цифрових трансформацій логістичних систем підприємств, в основу якого покладено рівень цифрової зрілості (оцифрування, цифровізація, оптимізація, інтеграція, трансформація, зрілість) та рівень ефективності функціонування їх логістичних систем. Це дозволило підприємствам здійснити діагностику цифрової трансформації логістичної системи підприємства, застосувати диференційований підхід до вибору цілей та стратегії цифрової трансформації логістичної системи підприємства.

Голова



Григорій НЕДОПАД



ВОЛИНЬСЬКА ОБЛАСНА РАДА

майдан Київський, 9, м. Луцьк, 43027, тел. (0332) 778 300,
e-mail: post@volynrada.gov.ua, web: https://new.volynrada.gov.ua, код ЄДРПОУ 00022444

08.05.2026 № 729/51/2-26 на № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження аспіранта кафедри підприємництва, торгівлі та логістики
Луцького національного технічного університету
Топалова Володимира Миколайовича
на тему: «Забезпечення інформаційної безпеки суб'єктів підприємництва»

Довідка видана здобувачу наукового ступеню доктора філософії Топалову В.М. в тому, що наукові положення дисертаційного дослідження було враховано в процесі розробки заходів по забезпеченню інформаційної безпеки суб'єктів підприємництва в умовах воєнного стану. Зокрема, цікавим є підхід автора щодо розробленої моделі забезпечення інформаційної безпеки суб'єктів підприємництва, що дозволить інтегрувати процеси ідентифікації, аналізу, попередження і нейтралізації загроз по забезпеченню інформаційної безпеки, а також забезпечити стійкість та адаптацію підприємств до динамічних умов розвитку цифрового суспільства.

Голова



Григорій НЕДОПАД



ТОВ "Еурістік", Україна, 79029, м. Львів, вул. Кульпарківська, буд. 59, корпус 42

Код ЄДРПОУ: 41212702

+380 63 840 35 60

hello@euristiq.com | euristiq.com

Вих. №1-20.03.26 від 20 березня 2026 року
Для пред'явлення за місцем вимоги

ДОВІДКА

про впровадження результатів дисертаційного дослідження аспіранта кафедри
підприємництва, торгівлі та логістики
Луцького національного технічного університету
Топалова Володимира Миколайовича
на тему: «Забезпечення інформаційної безпеки суб'єктів підприємництва»

Довідка видана здобувачу наукового ступеню доктора філософії Топалову В.М. в тому, що наукові положення дисертаційного дослідження є прикладними у роботі ТОВ "Еурістік". Зокрема, враховано підхід автора щодо запропонованого алгоритму дослідження процесу забезпечення інформаційної безпеки суб'єктів підприємництва. Запропонований підхід дозволяє оцінити загрози та вразливості зовнішнього середовища, які зумовлюють порушення інформаційної безпеки суб'єктами підприємництва, сформувати порогові значення забезпечення інформаційної безпеки, порівняти фактичні значення показників, які характеризують інформаційну безпеку із нормативними значеннями, та на цій основі виявити рівень забезпечення інформаційної безпеки суб'єктом підприємницької діяльності.

Директор ТОВ «Еурістік»



Бричук Ірина Олександрівна

Euristiq LLC, 59 Kulparkivska Str. 59, unit 42 79029 Lviv, Ukraine

Registration number: 41212702

+380 63 840 35 60

hello@euristiq.com | euristiq.com

ТОВ "Еурістік", вул. Кульпарківська, 596 корпус 42 79029, Львів, Україна

Код ЄДРПОУ: 41212702

+380 63 840 35 60

hello@euristiq.com | euristiq.com



ТОВ "Еурістік", Україна, 79029, м. Львів, вул. Кульпарківська, буд. 59, корпус 42

Код ЄДРПОУ: 41212702

+380 63 840 35 60

hello@euristiq.com | euristiq.com

Вих. №2-23.03.26 від 23 березня 2026 року
Для пред'явлення за місцем вимоги

ДОВІДКА

про впровадження результатів дисертаційного дослідження аспіранта кафедри
підприємництва, торгівлі та логістики
Луцького національного технічного університету
Топалова Романа Миколайовича
на тему: «Цифрові трансформації логістичних систем підприємств»

Довідка видана здобувачу наукового ступеню доктора філософії Топалову Р.М. в тому, що наукові положення дисертаційного дослідження є прикладними у роботі ТОВ "Еурістік". Зокрема, враховано підхід автора щодо запропонованого алгоритму аналізу та оцінки цифрових трансформацій логістичної системи підприємства, що дозволяє виявити рівень його цифрової зрілості (оцифрування, цифровізація, інтеграція, оптимізація, трансформація, зрілість), а також відповідність тенденцій розвитку суб'єкта господарюванням викликам цифрового середовища. Такий підхід у подальшому дозволить обрати стратегічну альтернативу здійснення цифрових трансформацій відповідно до рівня цифрової зрілості логістичної системи підприємства.

Директор ТОВ «Еурістік»



Бричук Ірина Олександрівна

Euristiq LLC, 59 Kulparkivska Str. 59, unit 42 79029 Lviv, Ukraine

Registration number: 41212702

+380 63 840 35 60

hello@euristiq.com | euristiq.com

ТОВ "Еурістік", вул. Кульпарківська, 596 корпус 42 79029, Львів, Україна

Код ЄДРПОУ: 41212702

+380 63 840 35 60

hello@euristiq.com | euristiq.com



УКРАЇНА

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**

вул. Львівська, 75, м. Луцьк, 43018, тел.: +38(0332)74-61-03

e-mail: rector@lntu.edu.ua, web: www.lntu.edu.ua

код ЄДРПОУ 05477296

18.03.2026р. № 206/01-14

на № _____ від _____

ДОВІДКА

про впровадження в навчальний процес результатів досліджень та розробок,
одержаних при виконанні дисертаційної роботи

Топалова Володимира Миколайовича**«Забезпечення інформаційної безпеки суб'єктів підприємництва»**

Науково-методичні розробки та результати досліджень Топалова Володимира Миколайовича, подані на здобуття ступеня доктора філософії галузі знань 07 «Управління та адміністрування» за спеціальністю 076 «Підприємництво, торгівля та біржова діяльність», сприяють якісній підготовці здобувачів та поглибленому оволодінні ними теоретичних знань та практичних навиків з освітніх компонент ОП «Логістика», ОП «Підприємництво та бізнес-адміністрування», ОП «Менеджмент».

Положення сформульовані в дисертації, а саме: понятійний апарат, який характеризує інформаційну безпеку підприємства, її функції та принципи; розроблена модель системи управління інформаційною безпекою підприємства; формування концептуальних засад забезпечення інформаційної безпеки підприємства – використано при розробці навчально-методичних матеріалів, а також викладанні освітніх компонент «Інформаційна безпека», «Інформаційно-комунікаційні технології в підприємстві та торгівлі», «Економічна безпека» на факультеті бізнесу та права Луцького національного технічного університету.

Проректор
з науково-педагогічної роботи
та досліджень



Олена ЛЮТАК



УКРАЇНА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

вул. Львівська, 75, м. Луцьк, 43018, тел.: +38(0332)74-61-03

e-mail: rector@lntu.edu.ua, web: www.lntu.edu.ua

код ЄДРПОУ 05477296

18.03.2016/р. № 804/01-14

на № _____ від _____

ДОВІДКА

про впровадження в навчальний процес результатів досліджень та розробок,
 одержаних при виконанні дисертаційної роботи

Топалова Романа Миколайовича**«Цифрові трансформації логістичних систем підприємств»**

Науково-методичні розробки та результати досліджень Топалова Романа Миколайовича, подані на здобуття ступеня доктора філософії галузі знань 07 «Управління та адміністрування» за спеціальністю 076 «Підприємництво, торгівля та біржова діяльність», сприяють якісній підготовці здобувачів та поглибленому оволодінні ними теоретичних знань та практичних навиків з освітніх компонент ОП «Логістика», ОП «Економіка».

Положення сформульовані в дисертації, а саме: понятійний апарат «логістична система», «трансформація», «цифрова трансформація», «цифрова трансформація логістичних систем підприємств», розроблена модель цифрової трансформації логістичної системи підприємства, запропонований алгоритм аналізу та оцінки цифрової трансформації логістичної системи підприємства, обґрунтування системи показників для оцінки ефективності функціонування логістичної системи підприємства, запропонований підхід до вибору стратегії цифрової трансформації логістичної системи підприємства – використано при розробці навчально-методичних матеріалів, а також викладанні освітніх компонент «Логістичні системи підприємницьких структур», «ІТ-рішення в логістиці», «Цифрова економіка», «Інформаційно-комунікаційні технології в логістиці» на факультеті бізнесу та права Луцького національного технічного університету.

Проректор
 з науково-педагогічної роботи
 та досліджень



Олена ЛЮТАК



ЛЬВІВСЬКА ОБЛАСНА РАДА

вул. Винниченка, 18, м. Львів, 79008 тел. (032) 2 999 800 факс (032) 2 999 810
www.lvivoblrada.gov.ua e-mail: info@lvivoblrada.gov.ua
 код ЄДРПОУ 22340506

№ _____ На № _____ від _____

ДОВІДКА

**про впровадження результатів дисертаційного дослідження
 аспіранта кафедри підприємництва, торгівлі та логістики
 Луцького національного технічного університету
 ТОПАЛОВА Володимира Миколайовича
 на тему: «Забезпечення інформаційної безпеки суб'єктів підприємництва»**

Виконавчим апаратом Львівської обласної ради проаналізовано положення, які репрезентовані у дисертаційному дослідженні Володимира Топалова на тему: «Забезпечення інформаційної безпеки суб'єктів підприємництва».

Тематика дисертаційного дослідження має високий рівень актуальності та практичної значимості в умовах забезпечення інформаційної безпеки країни в період воєнного стану. Зокрема, автором запропоновано підхід до обґрунтування вибору стратегії забезпечення інформаційної безпеки суб'єктів малого підприємництва.

Вважаємо, що за таким підходом, вибір стратегії забезпечення інформаційної безпеки дозволить отримати достатній рівень захищеності суб'єктів господарювання, а також протистояти сучасним інформаційним загрозам та інтегрувати інформаційну безпеку в загальну бізнес-стратегію як чинника конкурентної переваги досліджуваних підприємств.

Керуючий справами

Ярослав ГАСЯК



Львівська обласна рада
 №02-вих-523 від 24.03.2026
 КЕП: Гасяк Я. В. 24.03.2026 07:34
 382367105294AF970400000073AFC6005FD9AE04