ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця

на правах рукопису

КАПЕЛЮШНА ТЕТЯНА ВІКТОРІВНА

УДК 330.34:004.89:005.4:621.39(043.3)

ДИСЕРТАЦІЯ

УПРАВЛІННЯ БЕЗПЕКОЮ ПІДПРИЄМСТВ: ТЕОРІЯ ТА МЕТОДОЛОГІЯ

Спеціальність: 08.00.04 – економіка та управління підприємствами
(за видами економічної діяльності)

Подається на здобуття наукового ступеня доктора економічних наук

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

_____Т.В. Капелюшна

Науковий консультант: Легомінова Світлана Володимирівна, доктор економічних наук, професор

Київ – 2024

АНОТАЦІЯ

Капелюшна Т.В. *Управління безпекою підприємств: теорія та методологія. – Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня доктора економічних наук за спеціальністю 08.00.04 – економіка та управління підприємствами (за видами економічної діяльності). – Державний університет інформаційно-комунікаційних технологій Міністерства освіти і науки України, Київ, 2024.

У дисертаційній роботі обґрунтовано теоретико-методологічний базис управління безпекою підприємств, розвинуто наукові погляди до його сутності. Критичний аналіз існуючих уявлень та наукових знань щодо безпеки підприємства дозволив обґрунтувати безпеку як стан стійкого функціонування й потенціальної спроможності його розвитку за умови відсутності небезпек (викликів, ризиків, загроз), а у разі їх появи – захищеності, що гарантує досягнення цільових безпекових результатів діяльності. З'ясовано, що контекст безпеки не змінюється з часом, її осередком традиційно вбачається відсутність небезпек, захист від негативного впливу чинників об'єктів безпекозабезпечення (фінансових ресурсів, інформації, персоналу, майна та ін.), проте нові парадигми суспільно-економічного розвитку продукують виклики, які формують перспективи і, одночасно, небезпеки для підприємства й наштовхують на врахування в управлінні підприємством станів безпеки та небезпеки з виокремленням ділянок перебування підприємства за показниками у зоні викликів, ризиків, загроз. Констатовано, що динамічність соціально-економічних систем, невизначеність актуалізують безпекові питання та потребують вирішення в частині упередження ризиків і загроз, що продукуються змінами й впливають на цільові результати діяльності, що визначені як цільові безпекові орієнтири підприємтва (здатність до розвитку, конкурентоспроможність, стійкість, платоспроможність, прибутковість та рентабельність, гармонізація інтересів стейкхолдерів). Зважаючи на складність,

множину елементів безпеки, їх взаємозв'язок з результатами діяльності, сформовано систему безпекових складових: фінансову, техніко-технологічну, виробничу, енергетичну, ринкову, інтелектуального капіталу, інтерфейсну (репутаційну), інформаційну, фізичну (силову)), політико-правову, екологічну, інвестиційно-інноваційну та, запропоновану електронно-комунікаційну як відповідь на стрімкий розвиток інформаційно-комунікаційних технологій, які знаходяться у тісному зв'язку, взаємодоповнюються та використовуються у безпекозабезпеченні цільових безпекових результатів. Відзначено, що цільові безпекові орієнтири досягаються через управління як безперервний процес в динамічних умовах функціонування господарюючих суб'єктів, якому притаманна складність через множину елементів безпеки як об'єктів управління (активів захисту) та суб'єктів, що керують процесом, враховуючи чинники впливу, передумови виникнення невизначеностей, ризики та загрози, тобто через сукупно охоплену площину безпеки чи небезпеки. Підкреслено, що у невизначених умовах існує декілька варіантів щодо прийняття рішень внаслідок впливу явищ, чинників з невідомою ймовірністю їх настання, тобто через неможливість отримання даних про об'єкт захисту та передбачень щодо появи негативного результату через події, що відбуваються (відсутність інформації для аналізу та попередніх припущень щодо наслідків дії чинників). Доведено, що ризик передбачає прийняття рішення із множини варіантів, за попередньо відомою ймовірністю отриманого результату, що спрощує процес управління, однак ризик існує перманентно разом із функціонуючим підприємством, тісно пов'язаний із отриманням прибутку, тому його не можна повністю уникнути. Виклики оточують підприємство, можуть нести, як позитивні, так і негативні зрушення, за певних обставин формують воронку можливостей для підприємства. Науково обґрунтовано фрагментацію виразності ідентифікації ризиків та загроз у середовищах визначеності та невизначеності з резистентністю чи нерезистентністю безпекової площини підприємства до їх впливу/дії та розгалуженням управлінських заходів безпеки у напрямку розвитку, відновлення функціонування у разі протидії загрозам, або

ж, ліквідації підприємства – у разі неризистентності до загроз. Аргументовано доцільність використання VUCA та BANI-аналізу викликів для підприємств та характеристики невизначеностей у разі низької поінформованості щодо оточення. Відзначено стейкхолдер-орієнтованість та цільову безпекову спрямованість управління підприємством у відповідь на перехід від економіки знань до креативної цифрової економіки, доцільність прийняття рішень гармонізовано до інтересів стейкхолдерів.

Окреслено ризики, що ідентифікується за показниками діяльності у репелерній точці (нестійкість у межах допустимих значень метрик), а також у біфуркаційні точці – загрози (неоднозначність, нестійкість, суттєві відхилення метрик), що дозволяє визначити безпекові площини перебування підприємства за даними точками, а також сформовано концепт-погляд траєкторії площин станів безпеки під дією тривекторного синергетичного управління, який ґрунтується на захисті складових, якими формуються цільові результати безпеки підприємства.

Запропоновано концепт-методологію управління безпекою, яка ґрунтується на попередньо окресленій площині безпеки, в осередку якої – цільові результати діяльності підприємства, що визначаються складовими та метриками, які в залежності від зміни їх параметрів перебувають у діапазоні ризику із фіксацією реперної точки та переходом у діапазон загрози у біфуркаціній точці, якими окреслюється стан безпеки підприємства й, відповідно, рух у площинах безпеки та небезпеки підприємства під впливом ризиків та дії загроз, що скеровує до цілеспрямованого використання підходу до управління безпекою підприємства в залежності від конструкту безпекової площини підприємства. Проаналізовано ринок постачальників електронних комунікаційних послуг та відзначено сприятливе підґрунтя для розвитку та функціонування підприємств-постачальників електронних комунікаційних послуг за ініціації на інституційному рівні розбудови цифрової держави. Проаналізовано безпекові показники, диференційовано підходи до управління безпекою підприємства з урахуванням сумарних втрат за цільовими результатами

від ризиків, загроз та ризик-апетиту. Зважаючи на результати визначення стійкості підприємства до ризиків та загроз й враховуючи нелінійність процесів (за використання методу моделювання Ляпунова для окреслення стійкості та рівня (стану) безпеки підприємства, керуючись відхиленнями цільових безпекових орієнтирів від нормативних значень (критичних меж, якими визначаються репелер точки та точки біфуркації)), беручи до уваги безпекові відхилення метрик. запропоновано варіативно обирати підходи до управління безпекою підприємства.

Розглянуто та узагальнено виклики екзогенного характеру, перед якими постали підприємства-постачальники електронних комунікаційних послуг за умов невизначеності. Виклики повномасштабного вторгнення та початок воєнних дій в країні проаналізовано за допомогою VUCA та BANI аналізу, матричним методом SPOD визначено сильні сторіни, проблеми, можливості та невизначеності, окреслено оточення. Запропоновано можливі чотири сценарії розвитку підприємств-постачальників електронних комунікаційних послуг, визначено ентропію невизначеності для прогнозування вірогідного отримання прибутку (за інертним сценарієм, песимістичним сценарієм, позитивним сценарієм). Запропоновано план-стратегію управління підприємством в умовах невизначеності, низької прогностичності та емерджентності, що дозволило враховувати вірогідні сценарії з ентропією системи діагнозів для забезпечення безпеки підприємства та управління нею.

Ключові слова: управління, безпека підприємства, економічна безпека, підприємства, електронні комунікаційні послуги, цільові безпекові орієнтири, ризики, загрози, виклики, невизначеність умов, стани безпеки

ABSTRACT

Kapeliushna T.V. Enterprises security management: theory and methodology. – Qualifying scientific work on manuscript rights.

The thesis for receiving a scientific degree of the Doctor of Economics on specialty 08.00.04 – Economics and company management (by economic activities).

– State University of Information and Communication Technologies, The Ministry of Education and Science of Ukraine, Kyiv, 2024.

In the dissertation substantiates the theoretical and methodological basis of enterprise security management, develops scientific views on its essence. A critical analysis of the existing ideas and scientific knowledge about enterprise security allowed to substantiate security as a state of stable functioning and potential development capability of an enterprise – in the absence of hazards, security – in case of their occurrence, and guaranteed achievement of target performance results. It is found that the context of security does not change over time, its core is traditionally seen as the absence of dangers, protection from the negative impact of factors of security objects (financial resources, information, personnel, property, etc.), but new paradigms of socio-economic development produce challenges that form prospects and, at the same time, dangers for an enterprise and prompt to take into account the security and danger states in the enterprise management with allocation of areas of the enterprise's location by indicators in the zone of threats and risks.

It is stated that the dynamism of socio-economic systems raises security issues and requires their solution in terms of preventing risks and threats generated by changes and affecting the target performance results, which are defined as the target security guidelines of an enterprise (ability to develop, competitiveness, sustainability, solvency, profitability and profitability, harmonisation of stakeholders' interests). Given the complexity of security, the concentration of elements, and the relationship with performance results, the author has formed a system of its components: financial, technical and technological, production, energy, market, intellectual capital, interface (reputation), information, physical, political and legal, environmental, investment and innovation, and, as proposed, electronic and communication in response to the rapid development of information and communication technologies, which are closely related, interconnected and used.

It is noted that the target security benchmarks are achieved through management as a continuous process in the dynamic conditions of functioning of economic entities, which is inherent in complexity due to the multitude of security

elements as objects of management, (protection assets) and entities managing the process, taking into account the factors of influence, prerequisites for uncertainties, risks and threats, i.e. the total coverage of the hazard plane. It is emphasised that in uncertain conditions there are several options for decision-making due to the impact of phenomena, factors with an unknown probability of their occurrence due to the impossibility of obtaining data on the object and the probability of a negative outcome due to the events taking place, i.e. their absence for analysis and preliminary assumptions about the consequences. It is proved that risk involves making a decision from a set of options, based on the previously known probability of the result, which simplifies the management process, but it permanently exists with a functioning enterprise, is associated with making a profit, so it cannot be completely avoided. Challenges surround the enterprise, can bring both positive and negative changes, and under certain circumstances form a funnel of opportunities for the enterprise.

The fragmentation of the severity of identification of risks and threats in the environments of certainty and uncertainty with the resistance or non-resistance of the enterprise security plane to their impact/action and the branching of security management measures in the direction of development, restoration of functioning in case of counteracting threats, or liquidation of the enterprise – in case of non-resistance to threats – is scientifically substantiated. The expediency of using VUCA and BANI-analysis of challenges for enterprises and characterisation of uncertainties in case of low awareness of the environment is substantiated. The article emphasises the stakeholder-orientation and targeted security orientation of enterprise management in response to the transition from the knowledge economy to the creative digital economy, the expediency of decision-making harmonised with the interests of stakeholders.

The risks identified by the performance indicators at the repulsor point (instability within the permissible values of the indicators) and threats at the bifurcation point (ambiguity, instability, significant deviations of the indicators) are outlined, which allows to determine the security planes of the enterprise at these points, and also to form a conceptual view of the trajectory of the security planes

under the influence of the three-vector synergistic management, based on the protection of components that form the target results of the enterprise.

A concept-methodology of security management is proposed, based on a previously defined security plane, in the centre of which are the target results of enterprise activity, determined by components and indicators, which, depending on changes in their parameters, are in the risk range with fixing the reference point and transition to the threat range at the bifurcation point, which will determine the state of enterprise security and, accordingly, the movement in the security and danger planes of the enterprise under the influence of risks and threats, which leads to the targeted use of an approach to enterprise security management depending on the structure of the security plane of the enterprise. The market of electronic communication service providers is analysed and a favourable basis for the development and functioning of enterprises providing electronic communication services is noted, given the initiation of the development of a digital state at the institutional level.

The security components are analyzed, approaches to enterprise security management are differentiated, taking into account the total losses by target results from risks and threats and risk appetite, according to deviations, it is proposed to choose approaches to enterprise security management variably, taking into account the results of determining the enterprise's resistance to risks and threats and taking into account the nonlinearity of processes (using the Liapunov modelling method to determine the stability and level (state) of enterprise security, guided by deviations in the target security goals).

It has been analysed and summarised the challenges faced by the enterprises-providers of electronic communication services of exogenous nature: full-scale invasion of the country's territory and the beginning of hostilities with the help of VUCA and BANI analysis, the SPOD matrix method for analysing strengths, problems, opportunities and uncertainties, outlining the environment, four scenarios for the development of enterprises-providers of electronic communication services have been proposed, the entropy of uncertainty has been determined to predict the probable profit for inertia.

Key words: management, enterprise security, economic security management, electronic communication services, target security guidelines, risks, threats, challenges, uncertainty of conditions, security states.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Kapeliushna T., Lehominova S., Goloborodko A., Lysetskyi Yu., Nosova T. Methodological approaches to enterprise security management: traditional and transformed to the conditions of functioning. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024. No. 3. P. 204-209. URL: https://doi.org/10.33271/nvngu/2024-3/204. *(0,99 д.а., авторський внесок 0,2 д.а., полягає в аналізі методичних підходів до управління безпекою підприємства).*

2. Kapeliushna T., Goloborodko A., Nesterenko S. Bezhenar I., Matviichuk B. Analysis of digitalization changes and their impact on enterprise security management under uncertainty. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2023. No. 4. P. 150–156. URL: https://doi.org/10.33271/nvngu/2023-4/150. *(1,01 д.а., авторський внесок 0,21 д.а., полягає в обґрунтуванні врахування трансформаційних змін, що викликані діджиталізацією в управлінні безпекою).*

3. Kapeliushna T., Dymenko R., Safonov Yu. Kachmala V., Borshch V., Sheremet O. Digital tools for effective student learning and training online in conditions of uncertainty. *Financial and Credit Activity Problems of Theory and Practice*. 2022. Vol. 6, No. 47. P. 469–479. URL: https://doi.org/10.55643/fcaptp.6.47.2022.3817. *(0,9 д.а., авторський внесок 0,15 д.а., полягає в означенні електронних комунікаційних послуг та технологій, як основи забезпечення безпечного функціонування господарюючих одиниць за умов невизначеності).*

4. Kryshtal H., Kapeliushna T., Kalina I., Shuliar N., Martynenko M. Trends of development of financial and economic activity of entrepreneurial structures during the period of quarantine restrictions. Naukovyi *Visnyk Natsionalnoho Hirnychoho Universytetu*. 2022. No. 1. P. 139–144. URL: https://doi.org/10.33271/nvngu/2022-1/139. *(0,74 д.а., авторський внесок 0,14 д.а., полягає в аналізі трендів безпеки та можливостей забезпечення безперебійної роботи підприємства в умовах пандемії).*

5. Zghurska O., Dymenko R., Semkina T., Kapeliushna T. Diversification Strategy of Entrepreneurial Activity in Conditions of European Integration. *International Journal of Innovative Technology and Exploring Engineering*. 2019. Vol. 9, no. 1. P. 4809–4815. URL: https://doi.org/10.35940/ijitee.j9443.119119. *(0,7 д.а., авторський внесок 0,14 д.а., полягає в формуванні безпекових орієнтирів у функціонуванні підприємств в умовах євроінтеграції).*

6. Капелюшна Т. В. Управління безпекою підприємства в умовах невизначеності: система контролю загроз. Відбудова для розвитку: зарубіжний досвід та українські перспективи: міжнародна колективна монографія. Київ : ДУ "Ін-т екон. та прогнозув. НАН України", 2023. С. 474-486. URL: http://ief.org.ua/wp-content/uploads/2023/08/Reconstruction-for-development.pdf *(0,69 д.а.).*

7. Yakymenko Yu., Rabchun D., Kapeliushna T. Use of methodological approaches of system analysis to ensure information security of critical infrastructure objects. *Challenges and threats to critical infrastructure : Collective monograph.*. Detroit : NGO Institute for Cyberspace Research, 2023. P. 46-51. URL: https://conference.cyberspace.org.ua/wp-content/uploads/2023/06/Monograph-09-06-2023.pdf#page=46 *(0,36 д.а., авторський внесок 0,12 д.а., в частині пропозицій проведення системного аналізу безпеки функціонування підприємств).*

8. Капелюшна Т. В. Методологічний концепт управління безпекою підприємства. *Інвестиції: практика та досвід.* 2024. № 10. С. 69-74. URL: https://doi.org/10.32702/2306-6814.2024.10.69 *(0,4 д.а.)*

9. Капелюшна Т. В. Формування площини безпеки підприємства під дією ризиків і загроз. *Бізнес інформ.* 2024. Т. 3, № 554. С. 255–262. URL: 10. https://doi.org/10.32983/2222-4459-2024-3-255-262 *(0,42 д.а.)*

10. Капелюшна Т. В. Безпека даних підприємства у хмарному середовищі: аналіз загроз. *Облік і фінанси*. 2023. № 4(102). С. 97-104. URL: https://afj.org.ua/ua/journals/2023/4/ *(0,49 д.а.)*

11. Капелюшна Т. В., Голобородько А. Ю. Врахування інформаційних викликів при управлінні безпекою підприємств у сьогоденних невизначених

умовах. *European Journal of Economics and Management.* 2023. Т. 9, № 1. С. 12-21. URL: https://doi.org/10.46340/eujem.2023.9.1.2 *(0,61 д.а., авторський внесок 0,31 д.а. полягає в обґрунтуванні врахування інформаційних викликів в управлінні безпекою підприємства).*

12. Капелюшна Т. В. Врахування впливу загроз соціальної інженерії при управлінні безпекою підприємства. *Інвестиції: практика та досвід*. 2023. № 8. С. 125-130. URL: https://www.nayka.com.ua/index.php/investplan/article/view/1374/1384 *(0,36 д.а.)*

13. Капелюшна Т. В. Захист безпечного функціонування телекомунікаційних підприємств в умовах цифровізації та невизначеності. *Агросвіт*. 2023. No 7-8. С. 115-123. URL: https://www.nayka.com.ua/index.php/agrosvit/article/view/1351/1361 *(0,42 д.а.)*

14. Голобородько А. Ю., Капелюшна Т. В. Формування цифровізації інтегративного розвитку економіки та підприємств, як її елементів. *European Journal of Economics and Management.* 2022. Т. 8, № 6. С.5-13. URL: https://doi.org/10.46340/eujem.2022.8.6.1 *(0,88 д.а., авторський внесок 0,08 д.а., полягає в обґрунтуванні імперативів цифровізації економіки та розвитку підприємств).*

15. Капелюшна Т. В. Розширення базових складових економічної безпеки підприємства з урахуванням умов невизначеності. *Ефективна економіка*. 2022. № 10. URL: https://www.nayka.com.ua/index.php/ee/article/view/675/683 *(0,42 д.а.)*

16. Капелюшна Т. В., Пильнова В. П., Полякова А. О., Купрієнко Є. О. Роль електронної комерції в умовах формування цифрової держави та інформатизації суспільства. *Економіка. Менеджмент. Бізнес.* 2021. № 4. С. 68-75. URL: http://nbuv.gov.ua/UJRN/ecmebi_2021_4_13 *(0,45 д.а., авторський внесок 0,18 д.а., полягає в відзначенні потреби посилення захисту та безпеки підприємств, що представляють товари та послуги на електронних комерційних платформах).*

17. Капелюшна Т. В., Дименко Р. А. Експертна оцінка щодо надання телекомунікаційних послуг. *Ефективна економіка*. 2021. № 8. URL: http://www.economy.nayka.com.ua/?op=1&z=8811 *(0,7 д.а., авторський внесок 0,36 д.а., полягає в пропозиції визначення ключових показників якості для формування позитивного сприйняття постачальника послуг та захисту від втрати економічних вигід).*

18. Капелюшна Т. В., Кришталь Г. О., Ващенко О. О. Огляд та аналіз розвитку ринку державних боргових цінних паперів в Україні. *Ефективна економіка*. 2021. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=8811 *(0,7 д.а., авторський внесок 0,24 д.а., полягає в визначенні пріоритетних напрямів вкладення коштів в державні боргові цінні як найбільш безпечні з точки зору ризиків фінансових втрат).*

19. Капелюшна Т. В., Пильнована В. П., Овсійчук В. Я., Красник О. А. Місце інноваційних ризиків у системі економічної безпеки підприємства. *Економіка. Менеджмент. Бізнес.* 2021. № 4. С. 61-68. URL: http://nbuv.gov.ua/UJRN/ecmebi_2021_4_12 *(0,41 д.а., авторський внесок 0,19 д.а., полягає в дослідженні ризиків та визначенні їх місця в системі економічної безпеки підприємства).*

20. Капелюшна Т. В., Гавриш О. М. Проблеми неформального інвестування інноваційного підприємництва в Україні. *Ефективна економіка.* 2020. № 12. URL: http://nbuv.gov.ua/UJRN/efek_2020_12_69 *(0,68 д.а., авторський внесок 0,36 д.а., полягає в обґрунтуванні доцільності інвестування ризикових інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).*

21. Пильнова В. П., Гавриш О. М., Капелюшна Т. В. Організація експорту товарів суб'єктами малого та середнього бізнесу. *Агросвіт.* 2020. № 24. С. 29–36. URL: http://www.agrosvit.info/pdf/24_2020/5.pdf *(0,8 д.а., авторський внесок 0,26 д.а., полягає в обґрунтуванні доцільності експорту як заходу захисту та убезпечення підприємства від зменшення продажів на внутрішньому ринку).*

22. Пильнова В. П., Гавриш О. М., Капелюшна Т. В. Формування системи управління підприємницькими ризиками. *Інвестиції: практика та досвід.* 2020. № 24. С. 51-57. URL: http://www.investplan.com.ua/?op=1&z=7258&i=6 *(0,38 д.а., авторський внесок 0,13 д.а., полягає в обґрунтуванні доцільності інвестування ризикових інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).*

23. Гавриш О. М, Згурська О. М., Капелюшна Т. В., Мартиненко М. О. IT-послуги як об'єкт міжнародної торгівлі. *Міжнародний науковий журнал "Інтернаука". Серія:"Економічні науки".* 2020. № 11. URL: https://www.inter-nauka.com/ua/issues/economic2020/11/6585 *(0,7 д.а., авторський внесок 0,16 д.а., полягає в формуванні безпекових засад надання IT послуг на зовнішніх ринках).*

24. Капелюшна Т. В., Гавриш О. М., Пильнова В. П. Діагностика та тенденції розвитку міжнародної торгівлі в Україні. *Ефективна економіка.* 2020. № 11. URL: http://www.economy.nayka.com.ua/?op=1&z=8379 *(0,65 д.а., авторський внесок 0,23 д.а., полягає в означення загроз безпеці підприємств з урахуванням тенденцій розвитку міжнародної торгівлі).*

25. Капелюшна Т. В., Гавриш О. М., Дименко Р. А. Новації оподаткування підприємницької діяльності. *Інфраструктура ринку*. 2020. № 49. URL: http://www.market-infr.od.ua/uk/49-2020 *(0,75 д.а., авторський внесок 0,27 д.а., полягає в визначенні перспектив та ризиків в оподаткуванні для підприємств).*

26. Гавриш О. М., Пильнова В. П., Капелюшна Т. В. Планування торговельної діяльності підприємств на міжнародних ринках. *Підприємництво і торгівля*. 2020. № 27. С. 21-25. URL: http://journals- lute.lviv.ua/index.php/pidpr-torgi/article/view/699/664. *(0,68 д.а., авторський внесок 0,23 д.а., полягає в обґрунтуванні доцільності інвестування ризикових інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).*

27. Пильнова В. П., Гавриш О. М., Капелюшна Т. В., Лобань О. О. Інтернет-торгівля: особливості реалізації товару за допомогою інтернету. *Економіка. Менеджмент. Бізнес.* 2020. № 1. С. 122–130. URL:

http://journals.dut.edu.ua/index.php/e_mb/article/view/2394 *(0,51 д.а., авторський внесок 0,19 д.а., полягає в обґрунтуванні доцільності інвестування ризикових інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).*

28. Kapeliushna T. Organizational Mechanism for the Formation of an Innovative Enterprise in the Conditions of a New Technological Structure. *Science and Education a New Dimension.* 2019. Vol. VII, Is. 213, №. 35. P. 16-19. URL: https://doi.org/10.31174/send-hs2019-213vii35-03 *(0,42 д.а.)*

29. Капелюшна Т. В. Аналіз та тенденції розвитку фондового ринку в Європейському регіоні та Україні. *Бізнес Інформ.* 2019. Т. 12. № 503. С. 290-296. URL: https://doi.org/10.32983/2222-4459-2019-12-290-296 *(0,41 д.а.)*

30. Капелюшна Т. В. Роль інноваційного підприємства в умовах нового технологічного укладу. *Економіка. Менеджмент. Бізнес.* 2019. № 3(29). С. 71-77. URL: https://doi.org/10.31673/2415-8089.2019.037177 *(0,42 д.а.)*

31. Kryshtal H., Kapeliushna T. Synergy of the banking sector and socio-economic under the influence of the state regulator. *Підприємництво та інновації*. 2019. № 9. С.147-152. URL: https://doi.org/10.37320/2415-3583/9.24 *(0,63 д.а., авторський внесок 0,31 д.а., полягає в обґрунтуванні доцільності синергії фінансового сектора із соціально-економічним для безпечного функціонування та стабільності роботи підприємницьких структур під наглядом регулятора).*

32. Дименко Р. А., Капелюшна Т. В., Лобань О. О. Ризики впровадження та проблеми правового регулювання цифрової валюти в Україні. *Економіка. Менеджмент. Бізнес.* 2019. № 2(28). С. 72-79. URL: https://journals.dut.edu.ua/index.php/emb/article/view/2153 *(0,68 д.а., авторський внесок 0,22 д.а., полягає в аналізі ризиків впровадження та безпеки цифрової валюти).*

33. Капелюшна Т. В., Згурська О. М. Динаміка розвитку інтернет-речей та їх вплив на управління підприємствами. *Економіка. Менеджмент. Бізнес.* 2018. № 3(25). С. 79-86. URL: https://journals.dut.edu.ua/index.php/emb/article/view/1943 *(0,41 д.а., авторський*

внесок 0,21 д.а., полягає в дослідженні ризиків, додаткових можливостей та безпеки використання інтернет-речей в управлінні підприємствами).

34. Капелюшна Т. В. Оцінювання ефективності механізму управління сталим розвитком підприємства з використанням статико-динамічного підходу. *Економіка. Менеджмент. Бізнес.* 2016. № 3(17). С. 69-74. URL: https://journals.dut.edu.ua/index.php/emb/article/view/758 *(0,36 д.а.).*

35. Капелюшна Т. В. Підхід до оцінки ефективності механізму управління підприємством в контексті сталого розвитку. *Економіка. Менеджмент. Бізнес*. 2016. № 2(16). С. 62-68. URL: https://journals.dut.edu.ua/index.php/emb/article/view/650 *(0,37 д.а.).*

Опубліковані праці апробаційного характеру:

36. Капелюшна Т. В. Пропозиції щодо упередження ризиків інформаційних активів задля захисту репутації підприємства. *Перспективи та проблематика інтелектуальних систем* : зб. наук.-практ. конф., м. Київ, 31 трав. 2024 р. Київ, 2024. С. 54-55. *(0,1 д.а.).*

37. Капелюшна Т. В. Заходи щодо захисту інформаційного середовища підприємства. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу* : матеріали IV всеукр. наук.-практ. конф., м. Київ, 28 лют. 2024 р. Київ, 2024. С.105-108. *(0,15 д.а.).*

38. Капелюшна Т. В., Стріканов Д. О. Інформаційна безпека підприємства: важливість дотримання міжнародних стандартів безпеки. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу* : матеріали IV всеукр. наук.-практ. конф., м. Київ, 28 лют. 2024 р. Київ, 2024. С. 277-280. *(0,16 д.а., авторський внесок 0,12 д.а., полягає в дослідженні стандартів управління інформаційною безпекою підприємства).*

39. Капелюшна Т. В. Актуалізація питань інформаційної та кібернетичної безпеки підприємства в діджитал-умовах. *Глобалізаційні процеси та їх вплив на соціально-економічний та правовий розвиток України* : зб. матеріалів II всеукр. наук.-теор. конф., Київ 20 груд. 2023 р. Київ, 2023. С.92-93. *(0,1 д.а.).*

40. Капелюшна Т. В. Іванов Д. А. Врахування репутаційних ризиків при управлінні інформаційною безпекою компанії. *Актуальні проблеми кібербезпеки* : матеріали всеукр. наук.-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 125-127. URL: https://duikt.edu.ua/uploads/p_2626_52007398.pdf#page=125. *(0,16 д.а., авторський внесок 0,12 д.а., полягає в дослідженні впливу репутаційних ризиків на безпеку підприємства).*

41. Капелюшна Т. В. Чернявський І. Р. Проблема безпеки даних підприємства при використанні хмарних сервісів. *Актуальні проблеми кібербезпеки* : матеріали всеукр. наук.-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 134-135. URL: https://duikt.edu.ua/uploads/p_2626_52007398.pdf#page=134 *(0,1 д.а., авторський внесок 0,08 д.а., полягає в дослідженні проблематики забезпечення безпеки даних підприємства при їх розміщенні у хмарних сервісах).*

42. Капелюшна Т. В. Багаторівневий захист даних підприємств критичної інфраструктури задля зменшення поверхонь атак. *"Забезпечення кібероборони держави" Національного університету оборони України:* матеріали IV наук.-практ. вебінару, *м. Київ,* 10 лист. 2023 р. Київ, 2023. С. 62-65. URL: https://drive.google.com/file/d/1VpULkcweKcyZ-KR8EvxtxQSGYbyS1JSq/view *(0,16 д.а.).*

43. Kapeliushna T. Enterprise security management under uncertainty: a threat control system. *Міжнародний історичний досвід повоєнної реконструкції економіки: уроки для України* : матеріали міжнар. наук.-практ. конф., м. Київ, 27 квіт. 2023 р. Київ, 2023. С. 90. URL: Mizhnar-istor-dosvid-povojen-reconstrukcii-uroky-dla-Ukrainy.pdf (ief.org.ua) *(0,06 д.а.).*

44. Капелюшна Т. В., Голобородько С. О. Безпека функціонуючих господарюючих суб'єктів в сучасних умовах за систематизованого управління ризиками. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу :* матеріали всеукр. наук.-практ. Інтернет-конф., м. Київ, 23 лют. 2023 р.

Київ, 2023. С. 40-42. *(0,13 д.а. авторський внесок 0,09 д.а., полягає в дослідженні стандартів управління інформаційною безпекою підприємства).*

45. Капелюшна Т. В. Упередження від кібернетичних загроз підприємств критичної інфраструктури за використання систем їх контролю. *Шкідливі програми як загроза об'єктам критичної інфраструктури в умовах кібервійни* : зб. матеріалів міжвідомчого круглого столу, м. Київ, 21 лют. 2023 р. Київ, 2023. С. 63-66. URL: https://drive.google.com/file/d/1VpULkcweKcyZ-KR8EvxtxQSGYbyS1JSq/view *(0,17 д.а).*

46. Капелюшна Т. В. Забезпечення безпечного функціонування підприємств за сьогочасних викликів. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку :* матеріали IV міжнар. наук.-практ. конф., м. Київ, 17 лют. 2023 р. Київ, 2023. С. 97-99. *(0,15 д.а.).*

47. Капелюшна Т. В. Інформаційна складова в управлінні економічною безпекою діяльності підприємства. *Актуальні проблеми кібербезпеки :* матеріали всеукр. наук.-практ. конф., м. Київ, 27 жовт. 2022 р. Київ, 2022. С.171-172 –URL: https://dut.edu.ua/uploads/p_2121_20358827.pdf#page=171 *(0,1 д.а.).*

48. Капелюшна Т. В. Врахування впливу інформаційних атак на персонал задля безпеки підприємства. "*Telecommunication: problems and innovation"* : зб. тез всеукр. наук.-практ. конф. Київ, 2022. С.122-123. URL: https://dut.edu.ua/uploads/p_2121_16069800.pdf#page=122 *(0,1 д.а.).*

49. Капелюшна Т. В. Системи управління бізнесом – невід'ємна складова оптимізації бізнес-процесів. *Нові інформаційні технології управління бізнесом* : матеріали VI всеукр. наук.-практ. конф., м. Київ, 16 лют. 2022 р. Київ, 2022. С. 113-116. URL: http://unionba.com.ua/osvita *(0,15 д.а.).*

50. Капелюшна Т. В., Хуторна А. В. Формування товарного асортименту на підприємствах. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку :* матеріали III міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 37- 40. *(0,17 д.а., авторський внесок 0,12 д.а., полягає в дослідженні конкрентоспроможності як*

орієнтиру безпеки підприємства за рахунок клієнтоорієнтованого асортименту).

51. Капелюшна Т. В., Сіненко А. О. Формування соціально-психологічних компетенцій підприємця для досягнення ефективних результатів діяльності. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку:* матеріали ІІІ міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 35-37. *(0,12 д.а., авторський внесок 0,08 д.а., полягає в дослідженні впливу соціально-психологічних компетенцій підприємця на результати діяльності підприємства).*

52. Капелюшна Т. В., Берегова В. О. Переваги ведення підприємницької діяльності в інтернет за сучасних невизначених умов. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку:* матеріали ІІІ міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 132-139. *(0,28 д.а., авторський внесок 0,2 д.а., полягає в дослідженні переваг провадження підприємством своєї діяльності у глобальній мережі за невизначених умов функціонування).*

53. Капелюшна Т. В., Воробей К. О. Метрики визначення оптимізації управління запасами на підприємствах. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали ІІІ міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 32-35. *(0,18 д.а., авторський внесок 0,14 д.а. полягає у деталізації метрик оптимізації управління запасами підприємства для гарантування безпеки постачання й забезпечення безперебійного функціонування підприємств).*

54. Капелюшна Т. В., Дерев'янко Б. О. Дієві методи реклами в сучасних умовах функціонування підприємств. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку :* матеріали ІІІ міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 177-180. *(0,13 д.а. авторський внесок 0,1 д.а. полягає у моніторингу впливу реклами на результати діяльності підприємства та обґрунтування доцільності вкладень у рекламу).*

55. Капелюшна Т. В. Інноваційні інструменти інтернет-реклами в умовах інформатизації та цифровізації суспільства. *Розвиток економіки та бізнес-адміністрування: наукові течії та рішення* : матеріали III міжнар. наук.-практ. конф., м. Київ, 20–25 трав. 2022 р. Київ, 2022. С. 55-57. *(0,14 д.а.).*

56. Капелюшна Т. В., Новикова І.В. Умови ефективного провадження е-торгівлі. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку:* матеріали II міжнар. наук.-практ. конф., м. Київ, 11–12 лют. 2021 р. Київ, 2021. С. 35- 40. *(0,14 д.а., авторський внесок 0,09 д.а. полягає у дослідженні податкових новацій та їх впливу на результати діяльності підприємства).*

57. Капелюшна Т. В., Мізецький М. М. Підхід до забезпечення економічної стійкості у бізнес-процесах підприємства. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали II міжнар. наук.-практ. конф., м. Київ, 11–12 лют. 2021 р. Київ, 2021. С. 28- 31. *(0,13 д.а., авторський внесок 0,1 д.а. полягає у дослідженні підходів до забезпечення економічної стійкості підприємств як гарантій безпеки функціонування підприємства та його розвитку).*

58. Капелюшна Т. В., Ткаченко І. С. Private label як дієвий захід формування товарного асортименту. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали II міжнар. наук.-практ. конф., м. Київ, 11–12 лют. 2021 р. Київ, 2021. С. 189-193. *(0,17 д.а, авторський внесок 0,13 д.а. полягає у формуванні власної товарної марки для гарантування й забезпечення інтересів споживачів).*

59. Капелюшна Т. В. Податкові новації в умовах сьогоднішньої невизначеності. *Модернізація економіки: сучасні реалії, прогнозні сценарії та перспективи розвитку* : матеріали II міжнар. наук.-практ. конф., м. Херсон, 28 квіт. 2020 р. Херсон, 2020. С.701-703 *(0,12 д.а.).*

60. Капелюшна Т. В., Лисогор М. Л., Купрієнко Є. О. Фінансовий механізм забезпечення розвитку та конкурентоспроможності торговельного підприємства. *Підприємницька, торговельна, біржова діяльність: тенденції,*

проблеми та перспективи розвитку : матеріали І міжнар. наук.-практ. конф., м. Київ, 11 лют. 2020 р. Київ, 2020. С. 32-35. *(0,13 д.а., авторський внесок 0,1 д.а. полягає у дослідженні дієвих механізмів забезпечення розвитку та конкурентоспроможності підприємств).*

61. Капелюшна Т. В., Татаринський Г. О. Фіскальні інструменти як стимул для розвитку підприємств. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали І міжнар. наук.-практ. конф., м. Київ, 11 лют. 2020 р. Київ, 2020. С. 35-36. *(0,08 д.а., авторський внесок 0,06 д.а. полягає у дослідженні стимулювання розвитку підприємства за рахунок фіскальних інструментів).*

62. Капелюшна Т. В. Проблеми та перспективи розвитку фондового ринку України. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку*: матеріали І міжнар. наук.-практ. конф., м. Київ, 11 лют. 2020 р. Київ : ДУТ, 2020. С. 220-223. *(0,15 д.а., авторський внесок 0,13 д.а. полягає у розгляді проблемних питань для компаній з управління активами на організованих ринках капіталу).*

63. Капелюшна Т. В. Практична підготовка фахівців з використанням програмних продуктів для автоматизації бізнесу в процесі навчання. *Нові інформаційні технології управління бізнесом* : матеріали ІІІ всеукр. наук.-практ. конф., м. Київ, 12 лют. 2020 р. Київ, 2020. С. 85-86. *(0,09 д.а.).*

64. Капелюшна Т. В. Роль технологій у розбудові фондового ринку. *Телекомунікаційний простір XXI сторіччя: ринок, держава, бізнес* : матеріали І міжнар. наук.-прак. конф., м. Київ, 18-19 груд. 2019 р. Київ, 2019. С. 33-38. *(0,2 д.а.).*

65. Капелюшна Т. В. Концепція міжнародного управління в сучасних умовах. *Сучасні тенденції розвитку світової економіки* : зб. тез доп. Х міжн. наук.-практ. конф., м. Харків, 18 трав. 2018 р. Харків, 2018. С. 130. *(0,09 д.а.).*

66. Капелюшна Т. В. Аналіз державного боргу та оцінка механізму його управлінням. *Сучасні тенденції розвитку світової економіки* : зб. тез доп. ІХ

міжн. наук.-практ. конф., м. Харків, 26 трав. 2017 р. Харків, 2017. С. 73. *(0,09 д.а.)*

67. Капелюшна Т. В. Оцінювання динаміки рівня сталості розвитку підприємств. *Актуальні проблеми управління та економічного розвитку в умовах інформатизації суспільства*: матеріали наук.-практ. конф., м. Київ, 20 груд. 2016 р. Київ, 2016. С. 48-49. *(0,1 д.а.).*

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Виклики та невизначеність середовища функціонування підприємств позначаються на їх стійкості та результатах діяльності, що сповільнює розвиток та провокує порушення їхньої безпеки. Актуальності набуває питання управління безпекою підприємства, що пояснюється зміною індустріальних епох, технологій та підходів до процесів виробництва, зростанням конкуренції й умовами невизначеності функціонування підприємства. Підвищуються вимоги до безпеки, яка нині не зосереджується суто на економічних аспектах, а має враховувати екологічні, енергетичні проблеми. Вагомим залишається питання забезпечення результативності управління безпекою підприємства, яке залежить від чіткості визначення цілей безпеки (орієнтирів), які скеровуватимуть управління до захисту підприємства від ризиків, загроз, викликів за невизначених умов.

Множинний спектр викликів, перед яким постають підприємства, з одного боку продукує ризики та загрози, а з іншого – може слугувати тригером для нових можливостей розвитку, тому обидва випадки потребують ретельного дослідження та розв’язання проблем забезпечення та управління безпекою підприємств. За умов технологічної та інформаційно-комунікаційної залежності суспільства та господарюючих суб’єктів, підприємства, що постачають електронні комунікаційні послуги й відносяться до критичної інфраструктури, потребують посиленого перманентного захисту та гарантій безпечного функціонування.

Теоретичні та практичні аспекти управління безпекою підприємств з урахуванням високотехнологічних змін широко висвітлено в працях вітчизняних та закордонних учених: О. Ареф’євої, Б. Буркинського, В. Вахлакової, В. Волошина, В. Вороніної, В. Геєця, В. Грищенко, Е. Данілової, Б. Дуб, Г. Єфімової, З. Живко, Т. Зубко, С. Ілляшенко, О. Кучмєєва, О. Ляшенко, Т. Меліхової, С. Мельника, І. Мойсеєнко, І. Отенко,

В. Пильнової, Ю. Погорелова, Н. Пойда-Носик, С. Покропивного, Ю. Работіна, М. Сопікової, Т. Ткаченко, Ф. Фішера, М. Фрідмана, С. Хаддона, В. Чубаєвського, Г. Швиданенко, І. Шевченко, О. Шуміло та інших. Значний внесок у дослідження питань управління підприємствами-постачальниками електронних комунікаційних мереж та послуг зробили вітчизняні вчені: Т. Васильців, М. Верескун, О. Виноградова, О. Гудзь, О. Гусєва, К. Жадько, О. Згурська, І. Зеліско, Н. Євтушенко, О. Карпенко, І. Князєва, О. Ковшова, С. Легомінова, І. Охріменко, О. Сосновська та інші.

Вагомі напрацювання науковців надали можливість сформувати ґрунтовний теоретико-методологічний базис управління безпекою підприємств. Однак, у працях вчених увага переважно фокусується на управлінні ризиками, як ймовірних небезпеках підприємства, без розмежування потенційних та наявних загроз. Діалектика між теоретичним базисом та вирішенням практичних питань щодо управління безпекою підприємств потребує подальших досліджень у частині диференціації підходів до управління в залежності перебування підприємства у зоні ризиків та загроз, а також проведення пошуку стратегічних напрямів управління безпекою підприємствами за важкопрогнозованості майбутніх подій. Невизначеність умов господарювання підприємств спрямовує до поглиблення досліджень проблематики управління безпекою підприємств з урахуванням посилення загроз і ризиків та актуалізує розв’язання безпекових питань для функціонуючих підприємств і визначає мету, постановку завдань, логіку та послідовність їх дослідження.

Зв’язок роботи з науковими програмами, планами, темами, грантами. Дисертаційну роботу виконано відповідно до напрямів науково-дослідних робіт Державного університету інформаційно-комунікаційних технологій за темами: “Кадрові технології в управлінні інформаційною безпекою підприємства” (№ держ. реєстрації 0222U005067), де особисто автором запропоновано теоретико-методологічну концепцію управління безпекою підприємств, що ґрунтується на моделюванні безпекової площини за

цільовими безпековими орієнтирами й диференціації підходів до управління безпекою (у частині провадження управління за рівнями: перший – розробка планів, розпоряджень та рішень, стратегічних напрямів щодо управління безпекою; другий – розробка політики управління безпекою підприємств; третій – задачі, операційні картки, інструкції, розподіл на підпроцеси за станами безпеки та небезпеки підприємства); "Інноваційні засади розвитку телекомунікаційних підприємств" (№ держ. реєстрації 0120U100021), де автором обґрунтовано пріоритезацію: відновлення інфраструктури за використання технологій пасивних оптичних мереж; гарантування забезпечення безпеки підприємств у контексті сталого розвитку за використання еко-лізингу електричного та електронного обладнання (ЕЕО) й покращення управління відходами електричного та електронного обладнання (WEEE), зважаючи на інтеграцію національної енергосистеми з європейською мережею операторів системи передачі електроенергії; "Конкурентна розвідка як складова забезпечення інформаційної безпеки підприємства" (№ держ. реєстрації 01181U00058), де автором проведено розрахунок інформаційної складової безпеки підприємств ПЕКМП та запропоновано науково-параметричну діагностику безпеки підприємства, що ґрунтується на використанні підходу з урахуванням ентропії та дозволяє кількісно виміряти невизначеність; "Запобігання і протидія методам соціальної інженерії у забезпеченні інформаційної безпеки підприємства" (№ держ. реєстрації 0123U100743), де автором проведено аналіз кіберінцидентів на урядові, оборонні, високотехнологічні компанії, запропоновано розробку політики безпеки підприємств із планом стійкості до витоків даних та контролем на підприємствах за комунікаціями та ланцюгами постачання.

Мета і завдання дослідження. Метою роботи є обґрунтування теоретико-методологічних засад і розроблення практичних рекомендацій щодо вдосконалення управління безпекою підприємств за сучасних невизначених умов функціонування.

Досягнення цієї мети зумовило необхідність постановки й вирішення таких основних завдань:

– розглянути термінологічний базис щодо управління безпекою підприємства;

– проаналізувати понятійно-категоріальну площину елементів управління безпекою підприємства;

– визначити складові безпеки підприємства та множину чинників впливу на безпеку підприємства;

– розглянути ризики та загрози як рушії небезпеки в управлінні підприємством у визначеному та невизначеному середовищі;

– проаналізувати трансформаційні зміни управління безпекою підприємств в умовах невизначеності та втрати прогностичності;

– розглянути еволюцію поглядів щодо управління безпекою підприємств, обумовленою змінами підходів до виробництва та управління безпекою підприємства;

– сформувати науково-онтологічний базис методології управління безпекою підприємств;

– запропонувати концепт траєкторії площин станів безпеки підприємств;

– розробити методологію управління безпекою підприємств за невизначених умов функціонування;

– проаналізувати стан ринку постачання електронних комунікаційних мереж та послуг;

– провести моніторинг безпекової площини українських підприємств-постачальників електронних комунікаційних послуг;

– сконструювати модель управління безпекою підприємств-постачальників електронних комунікаційних послуг;

– проаналізувати виклики управління безпекою підприємств;

– провести науково-параметричну діагностику безпеки підприємств за умов невизначеності;

– запропонувати стратегічні напрями розвитку підприємств, як підґрунтя для управління безпекою підприємств у повоєнний час.

Об'єкт дослідження – сукупність процесів та явищ управління безпекою підприємств за умов невизначеності.

Предмет дослідження – теоретико-методологічні та прикладні засади управління безпекою підприємств-постачальників електронних комунікаційних послуг за невизначених умов функціонування.

Методи дослідження. Теоретичним і методологічним підґрунтям дослідження слугували положення економічної теорії, менеджменту, теорії фірм, теорії прибутків, еволюційної теорії, інноваційної теорії, теорії нестабільного розвитку (теорія дисипативних структур), теорії інформації, теорії сталого розвитку, загальної теорії систем, теорії ризиків, теорії стійкості систем, теорії структурного функціоналізму. Використовувався системний підхід загальнонаукових та спеціальних методів, зокрема: логічного, історичного та морфологічного аналізу для уточнення понятійно-категоріального апарату, а саме сутності, змісту управління безпекою підприємств; компаративного аналізу для структурування досліджуваних явищ та процесів ризикології підприємств; структурно-функціонального аналізу – для розкриття елементів та складових управління безпекою підприємств; аналізу та синтезу – для вивчення сутності управління безпекою, визначення цільових безпекових орієнтирів підприємств та їх впливу на стійкість безпеки функціонування підприємств; наукової абстракції – для розроблення підходу до управління безпекою з виокремленням метрик безпеки; методи узагальнення, формалізації, групування, систематизації; економіко-математичний та статистичний методи (ряди динаміки, аналіз даних, прогнозування) застосовувалися для моніторингу виявлення взаємозалежностей, впливу складових безпеки, ризиків і загроз на цільові безпекові орієнтири підприємств. Метод функцій Ляпунова застосовано для дослідження стану стійкості підприємств та визначення точок нестійкості (біфуркації, репелер), станів безпеки підприємств й моделювання безпекових площин управління

підприємствами. Індукції, дедукції – для визначення ключових показників безпеки та виокремлення вагомих у формуванні цільових безпекових орієнтирів; діалектичний аналіз, наукова абстракція, матричний метод SPOD, аналіз VUCA, BANI – для теоретичного узагальнення визначальних напрямів безпеки та розвитку підприємств в умовах воєнного стану та повоєнний період. Метод аналогії використовувався для обґрунтування вірогідних сценаріїв умов функціонування підприємств, метод ентропії для визначення ступеня невизначеності викликів й прогнозування прибутку за інертного управління безпекою та за вірогідними сценаріями розв'язання конфлікту в країні й, відповідно, запропонованими стратегічними напрямами управління підприємством за невизначених умов. Графічний метод для відображення теоретичного і методологічного матеріалу роботи.

Інформаційною базою дослідження слугували: законодавчі та нормативно-правові акти України; офіційні дані міністерств та відомств України; Державної служби статистики України; офіційні матеріали Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку; звіти Міжнародного союзу електрозв'язку; статистична та фінансова звітність; звіти про якість надання послуг підприємствами-постачальниками електронних комунікаційних мереж та послуг (ПЕКМП); наукові публікації, розробки, монографії вітчизняних та зарубіжних учених; матеріали періодичних видань і міжнародних оглядів; інші довідково-інформаційні джерела; матеріали з офіційних сайтів, а також результати власних досліджень автора.

Наукова новизна отриманих результатів

вперше:

– науково обґрунтовано концепт цільових безпекових орієнтирів, що включає: здатність до розвитку, стійкість, платоспроможність, конкурентоспроможність, прибутковість і рентабельність, а також гармонізацію інтересів стейкхолдерів у контексті ризиків і загроз сучасних викликів;

– доведено взаємозв’язок ризиків, загроз і невизначеностей, на перетині яких посилюється синергетизм турбулентного середовища функціонування підприємства з визначенням у точках: ризик – репелерна точка (нестійкість у межах допустимих значень індикаторів), загроза – біфуркаційна точка (неоднозначність, нестійкість, значні відхилення метрик), що дозволяє скоординувати управління зміщенням площини безпеки або її цілковитою трансформацією (переходом у новий стан);

– побудовано модель управління безпекою підприємств-постачальників електронних комунікаційних послуг з визначенням безпекових відхилень у безпечно-небезпечній площині дотичності репелерних точок впливу ризиків і біфуркаційних точок дії загроз, а також вибором відповідного підходу до управління безпекою підприємства для досягнення цільових показників діяльності;

– запропоновано науково-методичний підхід до оцінки викликів за невизначених умов функціонування підприємств, який ґрунтується на матричному аналізі сильних сторін, проблем, можливостей, невизначеностей (SPOD) та комбінації VUCA, BANI-аналізу для виявлення дестабілізуючих факторів в умовах високої ентропії, на основі якого побудовано вірогідні сценарії розвитку підприємств сфери електронних комунікацій (стабілізація конфлікту та поступове відновлення; ескалація та тривалі невизначеності; часткове врегулювання зі збереженням незначної невизначеності; позитивне розв’язання конфлікту, відбудова, інтенсивне відновлення);

– запропоновано науково-параметричну діагностику безпеки підприємства за умов невизначеності та динамічності, яка базується на використанні підходу з урахуванням ентропії та дозволяє кількісно виміряти невизначеність, визначити вплив викликів (з урахуванням їх ймовірності) на прибуток підприємств, що надає змогу аналізувати поведінку функціонуючого підприємства як системи, можливості його розвитку (за умови, що його стійкість як системи не надто “жорстка”), або ж навпаки, неспроможності до подальшого розвитку, нових впроваджень та динамічних змін;

удосконалено:

– методологію управління безпекою підприємства, яка, на відміну від існуючих, грунтується на безпековій площині, осередком якої слугують цільові результати діяльності підприємства, що визначаються метриками, які в залежності від зміни їх параметрів перебувають у діапазоні ризику з фіксацією репелерної точки та переходом у діапазон загрози у біфуркаційній точці, що дозволяє враховувати динамічність та невизначеність безпекової площини підприємства;

– стратегічні напрями управління підприємством в умовах невизначеності, низької прогностичності та емерджентності, які, на відміну від існуючих, враховуватимуть ймовірні сценарії з ентропією системи діагнозів для забезпечення безпеки підприємства та управління нею;

– науково-методичний підхід до екстраполяції процесу управління безпекою в умовах невизначеності, що полягає у забезпеченні керівництва максимально можливим обсягом інформації, отриманим за використання VUCA та BANI-аналізу викликів для підприємств й, відповідно, характеристик невизначеностей, який, на відміну від традиційних підходів, спрямований на створення умов для забезпечення стабільного функціонування підприємства й упередження від втрати прогнозованості процесу управління;

дістало подальшого розвитку:

– теоретичне обґрунтування розуміння безпеки підприємства як стану стійкого функціонування й потенційної спроможності його розвитку за умови відсутності небезпек (викликів, ризиків, загроз), а у разі їх появи – захищеності, що гарантує досягнення цільових результатів діяльності;

– наукове обґрунтування ознак небезпеки в контексті безпечно-небезпечного функціонування підприємства, що, на відміну від існуючих підходів, передбачає розмежування між ризиком і загрозою. Ризик розглядається як імовірність переходу підприємства до нестійкого стану функціонування, прояви якого включають ймовірність призупинення розвитку, втрату конкурентоспроможності, стійкості, платоспроможності, рентабельності

та прибутковості, а також порушення інтересів стейкхолдерів. Загроза розглядається як реальна дія, що призводить до негативних змін у цільових результатах діяльності підприємства, з проявами, такими як: гальмування розвитку, втрата конкурентних переваг, порушення стійкості, зростання витрат, скорочення темпів приросту прибутку, рентабельності, а також дегармонізація інтересів стейкхолдерів;

– диференціація безпекової площини управління підприємством за рівнями безпеки та небезпеки відповідно до ймовірності виникнення ризиків і реальної дії загроз як окремих елементів впливу на цільові орієнтири. Запропоновано доповнити традиційні стани безпеки підприємства станами небезпеки в залежності від розташування підприємства на конкретній небезпечній ділянці за зональною градацією: відносний стан, передкризовий стан, кризовий стан, критичний стан;

– обгрунтування доцільності доповнення існуючих складових безпеки підприємства (фінансова, техніко-технологічна, виробнича, енергетична, ринкова, інтелектуального капіталу, репутаційна, інформаційна, фізична, політико-правова, екологічна, інвестиційно-інноваційна) електронно-комунікаційною безпековою складовою у відповідь на зростаючу роль електронних комунікаційних послуг в умовах діджиталізації суспільства, визначаючи електронно-комунікаційну складову як ключовий орієнтир для забезпечення функціонування та розвитку підприємства;

– теорія ризиків, наукове обґрунтування впливу ризику та загрози в середовищі визначеності та невизначеності з урахуванням резистентності або нерезистентності безпекової площини підприємства, що дозволяє ідентифікувати їх ступінь впливу на вибір підходів до управління безпекою та повернення підприємства до резистентності;

– наукове обґрунтування динамічно-ситуативного підходу до управління безпекою підприємства в контексті еволюції промислових революцій та економічних змін від індустріальної епохи до економіки знань і цифрової економіки, що, на відміну від існуючих підходів, фокусується на змінах у

поглядах щодо управління безпекою з урахуванням невизначеностей, орієнтованості на стейкхолдерів та цільової спрямованості безпеки підприємства за попередньо визначеними складовими (ринкової, виробничої, інноваційно-інвестиційної, техніко-технологічної, фінансової, енергетичної, електронно-комунікаційної, екологічної, кадрової, інформаційної, інтерфейсної, політико-правової);

– науково-онтологічний базис методології управління безпекою підприємства, який включає теоретичний блок, що містить цільові орієнтири підприємства як вектор руху до прийнятного стану безпеки за умов виникнення ризиків та дії загроз у визначеному та невизначеному середовищі функціонування з акцентом на практичний блок (завдання, критерії, метрики моніторинг ризиків і загроз, а також визначення рівнів безпеки (небезпеки));

– наукове обґрунтування адаптації традиційних управлінських підходів до умов невизначеності, їх взаємної інтегрованості та зв'язку з об'єктом управління, що дозволило сформувати концепцію траєкторії станів безпеки підприємства під впливом тривекторного синергетичного управління: захист складових, що формують цільові результати підприємства; гармонізація інтересів стейкхолдерів; захист від небезпек (ризиків, загроз);

– критичне осмислення та аналіз інституційних змін щодо впровадження цифрових інновацій та розширення переліку надання е-послуг на шляху до євроінтеграції;

– конструктивне бачення значущості енергоефективного підключення споживачів за технологією xPON, обґрунтоване надзвичайними умовами функціонування підприємств-постачальників електронних комунікаційних послуг та інтеграцією національної енергосистеми з європейською мережею операторів системи передачі електроенергії;

– моніторинг безпекового стану українських підприємств ПЕКМП за запропонованою методикою розмежування ризиків і загроз, а також визначення безпекових проблем розвитку ПрАТ "Київстар", ПрАТ "ВФ Україна", АТ "Укртелеком", ПрАТ "Датагруп", ТОВ "Лайфселл" у динаміці для пошуку

підходів до прийняття ризиків або до управління безпекою підприємства у разі його високої чутливості до умов функціонування.

Практичне значення одержаних результатів. Розроблена в дисертаційній роботі методологія управління безпекою підприємств є теоретичною та практичною основою для впровадження результатів, рекомендацій, методів та методик, які можуть бути використані органами законодавчої і виконавчої влади під час підготовки проєктів нормативно-правових актів, які пов'язані з регулюванням діяльності підприємств-постачальників електронних комунікаційних мереж та послуг України, а також підприємствами під час формування, вибору та впровадження релевантних організаційно-економічних системних механізмів управління діяльністю підприємств-постачальників електронних комунікаційних мереж та послуг, що сприятимете їх ефективному, безпечному функціонуванню та розвитку. Одержані практичні результати схвалені та прийняті до впровадження у роботі Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку (довідка № 06-4065/103 від 12.06.2024 р., довідка № 06-4169/103 від 17.06.2024 р.), основні науково-практичні розробки впроваджено в діяльність таких підприємств, як: ТОВ "ПРОКОМ" (довідка № 3345 від 05.06.2024 р.); ДП "Ес Енд ТІ Україна" (акт від 28.05.2024 р.); ТОВ "НВО "Інформаційні технології" (довідка № 259-24 від 15.05.2024 р.); ТОВ "Євростратос" (акт від 27.05.2024 р.); ТОВ "АМ "АРТ-ПРОЄКТ" (довідка № 57 від 18.05.2024 р.), ТОВ "ІТ Спеціаліст" (довідка № 965 від 28.05.2024 р.). Рекомендації та основні наукові теоретично-методологічні напрацювання дисертаційної роботи використовуються в освітньому процесі Державного університету інформаційно-комунікаційних технологій під час викладання дисциплін: "Економічна безпека діяльності підприємства", "Управління інформаційною безпекою банків", "Організація проведення наукових досліджень", для написання курсових та кваліфікаційних робіт (акт від 07.06.2024 р.).

Особистий внесок здобувача. Дослідження виконано особисто здобувачем, усі наукові положення, результати дисертаційної роботи, що виносяться на захист, належать автору та відображені у наукових публікаціях. З наукових праць, які опубліковані у співавторстві, використано лише ті положення, ідеї та висновки, які є результатом власного дослідження здобувача. Наукові результати кандидатської дисертації не використано.

Апробація результатів дисертації. Основні теоретичні положення та результати дисертаційної роботи апробовано на 32 міжнародних науково-методичних і науково-практичних конференціях, семінарах, вебінарах: “Перспективи та проблематика інтелектуальних систем” (Київ, 2024 р.); “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” (Київ, 2023 р.; 2024 р.); “Глобалізаційні процеси та їх вплив на соціально-економічний та правовий розвиток України” (Київ, 2024 р.); “Міжнародний історичний досвід повоєнної реконструкції економіки: уроки для України” (Київ, 2023 р.); “Забезпечення кібероборони держави” (Київ, 2023 р.); “Шкідливі програми як загроза об’єктам критичної інфраструктури в умовах кібервійни” (Київ, 2023 р.); “Актуальні проблеми кібербезпеки” (Київ, 2022 р.; 2023 р.); “Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку” (Київ, 2020 р.; 2021 р.; 2022 р.; 2023 р.); “Розвиток економіки та бізнес-адміністрування: наукові течії та рішення” (Київ, 2022 р.); “Telecommunication: problems and innovation” (Київ, 2022 р.); “Нові інформаційні технології управління бізнесом” (Київ, 2020 р.; 2022 р.); “Модернізація економіки: сучасні реалії, прогнозні сценарії та перспективи розвитку” (Херсон, 2020 р.); “Телекомунікаційний простір XXI сторіччя: ринок, держава, бізнес” (Київ, 2019 р.); “Сучасні тенденції розвитку світової економіки” (Харків, 2017 р.; 2018 р.); Актуальні проблеми управління та економічного розвитку в умовах інформатизації суспільства” (Харків, 2017 р.); “Актуальні проблеми економіки та права: теорія та практика” (Київ, 2016 р.).

Публікації. За результатами дослідження опубліковано 67 наукових праць загальним обсягом 24,8 друк. арк. (з них 13,8 друк. арк. належить

особисто автору), а саме: дві колективні монографії обсягом 1,05 друк. арк. (з них 0,81 друк. арк. авторські), п’ять статей у наукових періодичних виданнях, проіндексованих у базах даних Web of Science Core Collection (одна) та Scopus (чотири), три статті у періодичних виданнях ЄС, двадцять одна стаття у наукових фахових виданнях України категорії “Б”, чотири статті в інших наукових періодичних виданнях обсягом 19,45 друк. арк. (з них 9,26 друк. арк. авторські), 32 публікації тез доповідей за матеріалами міжнародних наукових і науково-практичних конференцій обсягом 4,3 друк. арк. (з них 3,73 друк. арк. авторські).

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, п’яти розділів, висновків, списку використаних джерел з 418 найменувань, 4 додатків. Загальний обсяг роботи – 485 сторінок комп’ютерного тексту, з них 365 сторінок основного тексту (22,8 друк. арк.), містить 111 рисунків, 46 таблиць (10 сторінок – рисунки і таблиці, які повністю займають площу сторінки).

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

ARPU (Average Revenue per User) – середній дохід на одного користувача

BANI – Brittle (крихкий), Anxious (тривожний), Nonlinear (нелінійний), Incomprehensible (незрозумілий)

CEI (Cost Efficiency Index) – показник ефективності витрат

CR (Churn Rate) – відтік клієнтів

EBITDA (Earnings before Interest, Taxes, Depreciation and Amortization) – показник обсягу прибутку до вирахування витрат за відсотками, сплати податків та амортизаційних відрахувань

MAU (Mobile App Users) – користувачі мобільних додатків

NIST (The National Institute of Standards and Technology) – Національний інститут стандартів і технологій

NPS (Net Promoter Score) – індекс підтримки споживача

PON (Passive Optical Network) – пасивна оптична мережа

ROIC (Return on Invested Capital) – рентабельність вкладеного капіталу

ROMI (Return on Marketing Investment) – повернення маркетингових інвестицій

SPOD – матриця сильніх сторіни (S), проблем (P), можливостей (O) та невизначеностей (D)

VUCA – Volatility (волантильність, нестабільність), Uncertainly (невизначеність), Complexity (складність), Ambiguity (неясність, двозначність)

АТ – акціонерне товариство

ЕК – електронні комунікації

МСЕ – Міжнародний союз електрозв’язку

НКЕК – Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та поштового зв’язку

ПЕКМП – постачальник електронних комунікаційних мереж та послуг

ПрАТ – приватне акціонерне товариство

ТОВ – товариство з обмеженою відповідальністю

ЦРБ – цільові результати безпеки

ШСД – широкосмуговий доступ

ШСМ – широкосмугові мережі

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ БЕЗПЕКОЮ ПІДПРИЄМСТВА

1.1. Термінологічний базис понятійного апарату в управлінні безпекою підприємства

Наріжність питань гарантій безпеки, відслідковування викликів, упередження ризиків та усунення загроз постає перед людством та світом у всіх аспектах та напрямах існування. Всесвітні організації, спільноти, уряди держав, корпорації, підприємства й населення активно обговорюють шляхи уникнення поширення загроз, що нині постають та чинять руйнівний вплив на їх функціонування крім того, несуть невідворотні глобальні проблеми з негативними наслідками для всього світу. Проводяться форуми, зібрання, обговорення, створюються спільні міжнародні проєкти, програми, дорожні карти щодо подолання кризових явищ, викликаних загрозами безпеці.

Нині поняття “безпека” формує абсолютно новий погляд на її гарантування та управління нею, при чому на всіх рівнях – локальному і глобальному; мікро- макро; індивіда-суспільства. Усе більша увага привернута до питань еко-безпеки, яка включає не лише економіку, а ще й соціум, екологію, тобто зачіпаються питання сталого розвитку суспільства, територій, світу. Влучно висловлювався у формулюванні ризиків, глобального їх сприйняття У. Бек [21], який вважав, що теперішнє століття характеризується поєднанням ризиків: ядерного, фінансового; терористичного; біохімічного; військового; екологічного та інформаційного. Перераховані науковцем ризики притаманні всім функціонуючим економічним одиницям на теренах нашої держави, оскільки країна перебуває у стані війни. Тому питання безпеки, пошук шляхів її забезпечення із урахуванням низки подій та явищ, появи непередбачуваних дестабілізуючих чинників, які виникають в результаті ведення бойових дій на

території нашої країни, є надважливими та потребують нагального, якісно продуманого та ретельно спланованого вирішення. Тому слід детально, послідовно та методично досліджувати питання безпеки, її змісту, ролі, значення, зміни у поглядах її розуміння з урахуванням динамічного розвитку всіх сфер в умовах цифровізації, інформатизації та переходу роботи підприємств у новий вимір функціонування із використанням технологій, нанотехнологій, квантових комп'ютерів, штучного інтелекту й, зрозуміло, умовами невизначеності, що нині огортають Україну та світ.

Безпека, як ключовий орієнтир у розвитку всього живого, формує політики, напрями руху, програми розвитку і, безперечно, вважається важливою складовою, яка має гарантуватися в економічній сфері, починаючи від мікрорівня – підприємств, поступово рухаючись у напрямку до глобального – корпорацій, міжнародних та світових організацій. Для забезпечення належного рівня безпеки на підприємствах та ефективного управління нею необхідно ґрунтовно володіти категоріальним апаратом із безпекозабезпечення, орієнтуватися у підходах до управління безпекою, методології оцінки, концептуальних засадах її гарантування.

Термінологічний базис розуміння безпеки нашаровується із часом та надиктовується новими умовами: технологічними революціями, змінами технологічних укладів, політичними, економічними, екологічними зрушеннями. Звісно ж, що не слід оминати і питання економічних циклів, їх вихід на нові рівні, які формують нео-погляди у науці та розумінні вже відомих понять. На сьогодні слід розібратися із тим, що представляє собою безпека від макрорівня до мікрорівня її забезпечення.

Графічна інтерпретація безпеки за змістовним, об'єктним, територіальним вимірами та виміром небезпек, яка згадувалася у праці C. Daase, демонструє взаємозалежність та взаємовплив безпек (рис. 1.1).

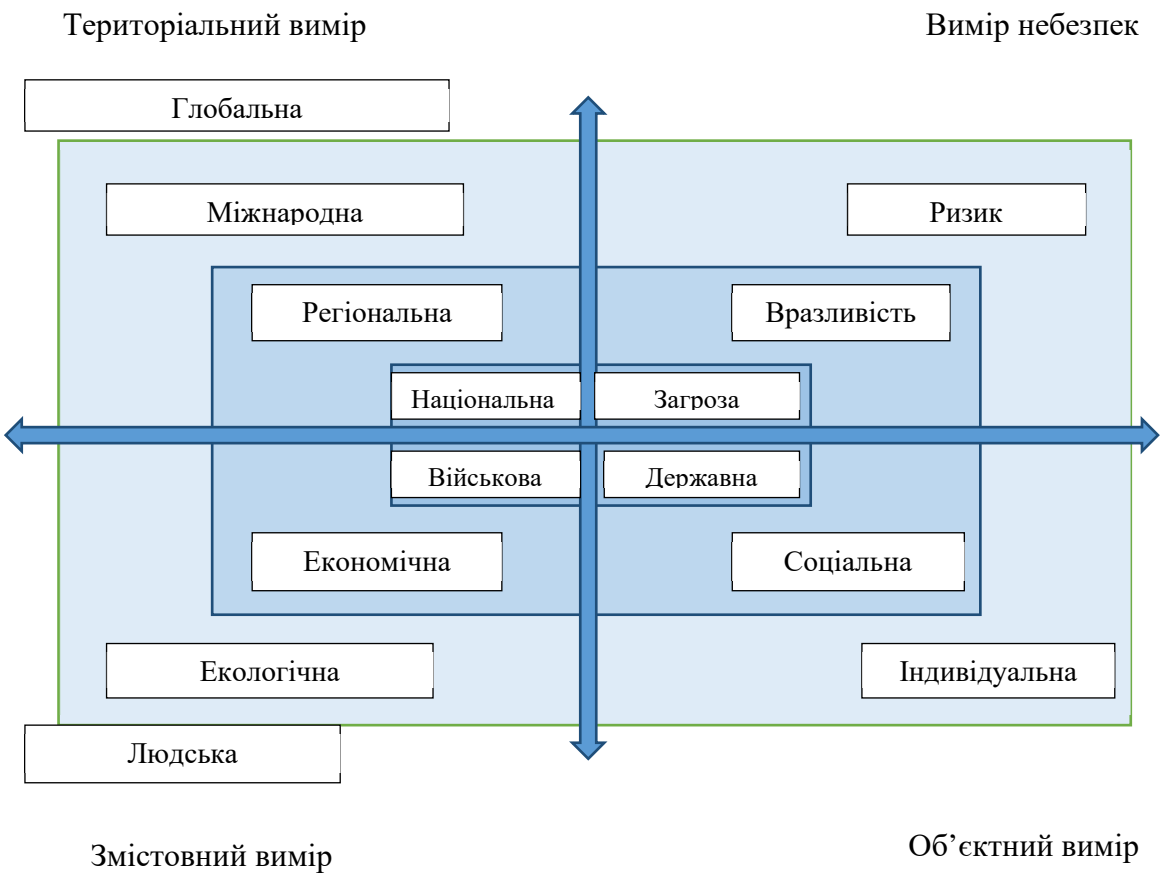


Рис. 1.1. Зовнішня архітектура метрик безпеки
(складено автором за [22])

Не можна не погодитись, що глобалізаційні процеси призвели до потреби узгодження безпеки на глобальному рівні, оскільки інтернаціоналізація, міжнародна торгівля, міграція робочої сили, альянси та міжнародні угоди щодо торгівлі та напрямків розвитку країн, появи союзів економічних сил потребують єдиного погляду на безпеку, та управління нею, координацію щодо її забезпечення, формування засад безпекозабезпечувальної діяльності за всіма згаданими вимірами. Крім того, взаємозалежність військової та економічної безпеки є очевидним фактом, оскільки напад на Україну з боку країни-агресора чітко дав зрозуміти, що продовольча безпека у світі під загрозою через військову небезпеку, яка нависла над Україною, що може призвести до непоправних наслідків для країн, які потребують товарів та продуктів харчування для населення та задоволення їх фізіологічних потреб – у продуктах

харчування. Нині прослідковується посилення взаємозв'язку військової та економічної безпеки, тому захист міжнародних потоків товарів, послуг, транснаціональних сполучень є важливим та привертає все більше уваги світової спільноти [315].

Об'єктний вимір безпеки зосереджується навколо держави, соціуму та індивіда, більшістю науковців за об'єктами здійснюються поділ безпеки за рівнями її забезпечення.

Вимірюються небезпеки за C. Daase загрозами, вразливостями, ризиками, однак у подальшому в результаті дослідження нами буде уточнено, якими елементами формується площина безпеки, причини порушення станів безпеки, коли підприємство опиняється у стані небезпеки (вибудується послідовність станів за пересуванням по вектору "виклик – ризик – загроза".)

Запропонований автором вимір безпеки актуальний і нині, може розглядатися як базовий для нашарування за змістом, територіальним охопленням та об'єктом.

Рис. 1.2. Класифікаційні ознаки безпеки за об'єктами захисту та рівневим забезпеченням

(складено автором за [24; 26; 27; 30; 31; 45])

Нині широко використовується розуміння безпеки в співвідношенні об’єкта захисту та рівня забезпечення (рис. 1.2).

Питання безпеки підприємства бере свій початок із забезпечення безпеки індивіда та завершується безпекою на глобальному рівні – міждержавному, тобто повністю охоплює рівні функціонування об’єктів безпеки.

Слід наголосити, що Маслоу А. (за теорією мотивації, вчений представив піраміду потреб людини, в якій безпека, на рівні із фізіологічними потребами (їжа, одяг), є однією із основних потреб” [47]) включив безпеку до базових потреб людини, як розуміємо, без неї індивід не в змозі перейти до більш високих потреб, формувати своє світобачення та мотивуватися до подальшого розвитку (на рис. 1.2 має місце у об’єктному вимірі, як безпека індивіда, клієнта). Знову ж таки без безпеки індивіда, людської безпеки не можна перейти до безпеки на мікрорівні – підприємств, оскільки найбільшу цінність у формуванні ланцюга виробництва відіграє людина: людина формує підприємницьку ідею, організовує виробництво, управляє виробничо-збутовими процесами з метою отримання прибутку, персонал безпосередньо виконує операційну діяльність, в кінцевому результаті – поповнюється державний бюджет податковими надходженнями для забезпечення соціального рівня розвитку та гарантій безпеки за всіма вимірами її формування в суспільстві.

Питання безпеки, стратегічного управління нею розглядаються у працях Ситника Г.П., який розглядає її як систему, що складається із різних категорій, таких як: “кадрова безпека”, “продовольча безпека”, “техногенна безпека”, “транспортна безпека”, “водна безпека” тощо. Науковець вважає, що безпека починається із індивіда: “Певною мірою такий підхід обґрунтований, оскільки він обумовлений процесами гуманізації суспільства і держави, в основу яких покладена зміна уявлень про сферу національної безпеки. Ця зміна відбувається в напрямі забезпечення передусім безпеки особи, яку необхідно розглядати в контексті сучасних тенденцій до глобалізації, розвитку інформаційних технологій, зміни традиційних уявлень про державний суверенітет,

національну ідентичність тощо" [24]. Із цим судженням важко не погодитись, адже у сучасному світі нами обговорюються питання людиноцентризму, студентоцентризму, для підприємства – клієнтоорієнтованості, як підґрунтя до отримання прибутку через задоволення потреб споживача за врахування його вподобань щодо товарів та послуг [248].

Розглядаючи місце безпеки підприємства загалом за масштабом її забезпечення, зрозуміло, що на мікрорівні безпека є узгодженим комплексом заходів щодо її досягнення на всіх рівнях задля досягнення підприємством запланованих результатів діяльності [23]. Тобто, має забезпечуватися безпека на наднаціональному рівні (актуально, якщо підприємство провадить свою діяльність і поза межами країни), в цілому в країні, якій зареєстроване підприємство, безпека на галузевому рівні (притримуватися, взаємоузгоджувати норми та стандарти безпеки у галузі), для окремого підприємства (враховуючи його особливості функціонування, ресурси, можливості, потужності), а також на рівні індивіда, (безпека клієнта, який є важливим суб'єктом при формуванні клієнтоорієнтованого підходу для формування планів виробництва та асортименту, переліку послуг відповідно до вподобань споживачів щодо товарів (послуг)). Цілковито безпека підприємства забезпечується за досягнення її на всіх рівнях.

Нестабільність економіки, невизначені умови, що були викликані пандемією, яка ширилася світом, а наразі воєнним станом, що введений в Україні через повномасштабне вторгнення країни-агресора, призводить до дестабілізації функціонування підприємств, порушення безпеки та появи біфуркаційних явищ. Наразі під загрозою знаходиться національна безпека, що у свою чергу призводить до порушення безпеки загалом економічних одиниць, тому питання її забезпечення потребує вирішення на всіх рівнях із урахуванням масштабів її порушення та впливу на індивідів та суб'єктів господарювання.

Науковицями Зеліско І.М., Захаржевською А.А. відзначено посилення глобалізаційних процесів, підвищення взаємозалежності країн, формування складних, нелінійних позитивних і негативних взаємозворотних зв'язків між

елементами економічних систем та підсистем будь-якого рівня. Як результат збільшується кількість факторів впливу, чутливість поведінки суб'єктів господарювання до внутрішніх і зовнішніх збурень будь-якої природи й появи біфуркаційності (багатоваріантності) процесів розвитку [25].

За Законом України "Про національну безпеку України" національна безпека визначається як: захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [27]. Розглядаючи поняття "безпека підприємства", доцільно розпочати із етимології поняття "безпека", що дозволить зрозуміти її сутність, що вбачалося під безпекою із часів появи терміну, сенс якого не змінюватиметься в різних сферах використання. Тож, вважається, що слова "безпека" походить від французької та латинської мов.

Вживання цього терміну латинською мовою можна знайти в різних історичних текстах, слово "sēcūritās" (походить від поєднання "se", що означає "без" і "cura" – "турбота") [49, с.583] перекладається, як: безтурботність, відсутність небезпеки, впевненість, спокій, свобода від тривоги чи турботи, свобода від небезпеки, захист. Французькою "securité" впевненість, спокій [97; 98].

Тобто розуміємо поняття наступним чином: бути захищеним від небезпеки або у спокої.

Перші згадки про безпеку містяться й у письменах Греції, вислів "бути у безпеці", означав "володіти ситуацією".

На івриті слово "безпека" має кілька значень: 1) a'sfalh – твердий, непохитний, непорушний, міцний; 2) ei'rh/ nh – мир, спокій [50, с.178]. В англомовному вжитку термін "security" з'явився дещо пізніше, у оксфордському словнику "securyte" згадується приблизно у 15 сторіччі, написання його дещо відрізнялося від сучасного "security" [98].

Концепція безпеки, в сенсі захисту і свободи від небезпеки або ризику, має давнє походження і є фундаментальною для людських суспільств. Хоча сам термін не використовувався в його сучасній англомовній версії аж до 17

століття, концепція, що лежить в його основі, була присутня впродовж всієї історії, оскільки люди шукали способи захистити себе, свої громади і своє майно.

Можемо зробити припущення, що безпека є керованою, оскільки йдеться про "володіння ситуацією", а також станом спокою з відсутністю небезпек.

Питання безпеки завжди було і залишається нагальним, дослідження категорії має широкий спектр для подальшого розгляду та рефлексій. Проаналізуємо визначення категорії, що дозволить зрозуміти її суть й чітко визначати вихідні елементи, які враховуватимуться при управлінні безпекою підприємства (складові, елементи і т.д.).

Науковцею Зубко Т.Л. [28, с. 9] та науковцем Денисовим О.Є. [29, с. 46-47] зазначається, що в економічному розумінні "безпека" згадується ще у доробку філософа Платона "Політея", як "ідеальної держави", що перебуває у безпеці. Держава з високим рівнем достатку вважається захищеною, оскільки у протилежному випадку, за надлишкових потреб, виникає низка проблем, країни опиняються на шляху їх вирішення, розв'язуючи війни за ресурси, яких вони потребують. Тобто безпека, на думку Платона, вбачається у перебуванні країни у стані економічної безпеки (як згадувалося вище "ідеальної держави").

Переважною більшістю науковців вказується, що початково поняття "безпека" згадується у словнику Гроссетеста Робера 1190 року і визначається, як спокійний стан духу людини, за якого вона відчуває захищеність від будь-якої небезпеки, проте таке визначення обмежується суто людським чинником, її внутрішньою силою, але аж ніяк тим, що формує її, тобто складовими та чинниками впливу.

Економічного сенсу поняття "безпека" набуло через потребу виходу із кризи, яка виникла у фінансовій сфері впродовж 1929-1933 рр., коли здійснювався пошук шляхів стабілізації економічної та соціальної ситуації. Саме у цей період у положеннях Франкліна Делано Рузвельта економічна безпека окреслилася, як економічна категорія та передбачалася у захисті соціально-економічних прав: гідне житло, якісна освіта, належний рівень

зайнятості населення, соціальний захист, дохід співставний для обміну на продукцію, тобто – у захисті базових благ, яких потребує суспільство [35].

Із плином часу, розвитком суспільства, поділом країн на економічні зони за рівнем доходу, активізації зовнішньої торгівлі, глобалізаційних процесів та економічних трансформацій під впливом науково-технічного, технологічного прогресу, зміни промислових революцій та епох прогресу, сутність поняття "безпека" залишалася незмінною, а його змістовне наповнення збагачується.

Загалом безпека вбачається у відсутності небезпек, захищеності від внутрішніх і зовнішніх руйнівних впливів та наповнюється ще розумінням її забезпечення через систему безпеки від глобального до мікрорівня, окремого індивіда. Науковцями Мелих О. [30, с.266], Зубко Т.Л. [28, с. 9], Гуляєвою Н.М., Камінським С.І. [31, с.140], Швиданенко Г.О. [32, с. 8], Язлюком Б.О. [33, с. 150] та ін.) безпека підприємства полягає у захищеності від небезпек, обумовлених зовнішніми впливами.

Науковиця Зубко Т.Л. розуміє економічну безпеку, як захищеність суб'єктів соціально-економічних відносин усіх рівнів: від держави – до суб'єктів господарювання, підприємств, кожного окремого громадянина [28, с.15]. Вважає одним із елементів захисту національної безпеки економічну безпеку підприємства Ламберт Д. [50], який стверджує, що для забезпечення безпеки треба рухатися по вертикалі безпеки: від найнижчого (мікро-) до найвищого (макро-) рівня.

Досить чітко надано визначення поняття "безпека" у словнику-довіднику за редакцією Ситника Г.П., підтверджуючи, важливість захисту всіх сфер діяльності та об'єктів захисту: "це стан системи, за якого вона зберігає свою цілісність, стійкість (стабільність), здатність до ефективного функціонування та стійкого розвитку, а на їх основі – можливість надійного захисту усіх її елементів (підсистем, сфер, об'єктів) від будь-яких деструктивних внутрішніх та зовнішніх дій" [24], що дозволяє виокремити ключові елементи безпеки: стійкість, розвиток, захист елементів від змін. Досліджуючи визначення поняття безпека підприємства, ми впевнимося, що згадані елементи будуть

базовими, крім того, безпека підприємства осмислена, з економічної точки зору, із огляду мети створення підприємства – отримання прибутку, який отримується шляхом задоволення потреб споживачів, що підкріплені їх платоспроможністю.

Економічна безпека підприємства є таким станом його функціонування, що забезпечує захист соціально-економічних інтересів, формування адаптивних здібностей для можливості функціонування підприємства за всіх можливих економічних умов, а також утримання конкурентних переваг у довгостроковій перспективі [33, с.6]. Кучмєєв О.О. економічну безпеку підприємств оптової торгівлі характеризує, як здатність підприємства організовувати свою діяльність таким чином, щоб охопити закупівельну, збутову, складську, управління запасами та замовленнями, транспортну, інформаційну логістику, логістичну інфраструктуру, організаційно-управлінську діяльність для створення та управління цією системою з метою надійного захисту від негативних внутрішніх, зовнішніх чинників впливу або ж усунення наслідків та проявів загроз і небезпек, а також адаптації до умов з мінімальними затратами [34; 37, с. 4].

У своїй концепт-моделі місця захисту корпоративної інформації в забезпеченні ефективного функціонування підприємства Чабаєвський В.І. вбачає інформаційну безпеку, як складову економічної безпеки підприємства і визначає останню як стан захищеності інтересів підприємства, який забезпечує ефективне використання пулу ресурсів [38, с. 13]. Зубко Т.Л. в основу побудови системи економічної безпеки підприємства в умовах євроінтеграції заклала розуміння її, як сукупності економічних відносин для захищеності підприємства від негативних впливів та спроможності формування можливості розвитку [39, с.13].

З урахуванням умов невизначеності, що нині спостерігаються, доцільно дослідити визначення поняття економічна безпека підприємства саме у цьому контексті. На думку Нестерова Ю.О. захищеність від катастрофічного впливу дестабілізуючих чинників зовнішнього середовища, що реалізується шляхом

спрямування наявних ресурсів в першу чергу на своєчасне діагностування і прогнозування негативного впливу зовнішніх чинників на різні аспекти його економічної та виробничої діяльності [40, с.3].

У дисертаційному дослідженні Сосновська О.О. зосереджується на загрозах, які виникають в умовах невизначеності та зазначає, що: "рівень економічної безпеки та стійкість функціонування підприємства будуть залежати від його здатності своєчасно й ефективно мінімізувати потенційні загрози як спосіб уникнення чи мінімізації негативних економічних наслідків діяльності в результаті існування небезпеки та виникнення ризиків під впливом дестабілізуючих чинників внутрішнього і зовнішнього середовища" [41, с. 27].

Економічну безпеку підприємств, як соціально-економічну систему, що включає складові й визначається станом захищеності підприємств від внутрішніх і зовнішніх загроз, характеризується властивістю до адаптації змінам умов функціонування, здатністю протистояти загрозам, визначено вченою Шуміло О. С. [42, с. 8]. Науковиця акцентує увагу на двоспрямованості безпеки: перший напрям – досягнення цілей підприємства та забезпечення стану захищеності, другий – стосується чинників зовнішнього та внутрішнього впливу, тобто знову ж таки пов'язаний з умовами функціонування підприємства, його оточенням.

Спираючись на розуміння активних трансформаційних змін в економіці, невизначеності та мінливості оточуючого середовища функціонування господарюючих суб'єктів, доволі нетрадиційно формулює визначення економічної безпеки підприємства Тютченко С.М., а саме: чітко структурованої системи гарантування резистентності, ризикоредукції й економічної сукцесії підприємств [43, с.13].

Аналогічної думки Ліщенко А.В., вважаючи, що економічна безпека підприємств являє собою стан захищеності від загроз, ризиків, небезпек, що визначається їх адаптаційною здатністю до зміни зовнішніх економічних умов та постійною готовністю до їх погіршення, умінням вчасно створити нові економічні можливості, прийняти адекватні рішення [44, с. 5]. Досить змістовно

наповненим є визначення надане Ткачук Г.Ю., якою вказано, що запланованого рівня економічної безпеки у довгостроковій перспективі підприємство може досягти шляхом реалізації економіко-організаційних, адміністративних та правових методів, форм та засобів впливу керуючої системи на систему економічної безпеки підприємства з метою мінімізації можливих втрат та досягнення стану його захищеності [46, с.56].

Часто зустрічаються визначення, в яких економічна безпека пов'язання із управлінням, оскільки йдеться про керованість та контрольованість процесу її забезпечення. До прикладу, Ляшенко О.М. економічну безпеку розглядає як міру економічної свободи підприємства, що досягається внаслідок керованого процесу взаємоузгодження економічних інтересів стейкхолдерів як зовнішнього, так і внутрішнього середовища підприємства, який має на меті протистояння загрозам економічній безпеці підприємства та потребує необхідних для такого протистояння ресурсів [51, с. 60]. Єфімова Г.В. вважає, що економічна безпека підприємства характеризує умови функціонування підприємства, не контрольовані або контрольовані ним, що забезпечують йому певний рівень стабільності та стійкості, можливість самореалізації та розширеного самовідтворення шляхом протистояння зовнішнім загрозам і запобігання внутрішнім при наявності відповідних ресурсів [45, с. 12].

За результатами пошуку джерел, у яких згадується безпека впродовж 2018 – 2021 рр., найчастіше зустрічаються праці науковців, із характеристиками, уточненнями та удосконаленнями визначення понять "безпека підприємства", "економічна безпека підприємства". Починаючи з 2022 року, більшість робіт присвячено безпеці на національному рівні, питанням продовольчої безпеки, енергетичної безпеки. Проте, безпека господарюючих суб'єктів не має залишатися осторонь, а навпаки, потребує розгляду на одному щаблі із безпекою інших рівнів, оскільки, безпека підприємства є багатосторонньою, базисною для формування цілковитої безпеки, як згадувалося раніше.

Подальші дослідження етимології безпеки підприємства підтверджують думку, що це є стан, забезпеченість, потенційні можливості, протидія загрозам, врахування інтересів підприємства та середовища.

Безпека, за визначенням Ткаченко Т.П., стан, що обмежений в часі, при якому об'єкт, система чи процес, здатні повністю захистити себе від небезпеки [99, с.22]. Вчений Чуприн Є.С. характеризує економічну безпеку підприємства, як стан захисту підприємства від впливу зовнішніх та внутрішніх дестабілізуючих чинників, що характеризується стабільністю господарської діяльності та дотриманням інтересів підприємства [69]. Вівчар О.І. категоріально визначає економічну безпеку підприємства, як стан корпоративних ресурсів (ресурсів капіталу, персоналу, інформації і технології, техніки та устаткування, прав) і підприємницьких можливостей, за якого гарантується найбільш ефективне їх використання для стабільного функціонування та динамічного науково-технічного і соціального розвитку, запобігання внутрішнім і зовнішнім негативним впливам та загрозам [49].

Сосновською О.О. детально розглядаються ризики безпечного функціонування підприємства, зокрема ідентифікуються кадрові загрози зовнішнього і внутрішнього середовища функціонування підприємства, врахування яких, на думку, авторки сприятиме підвищенню адаптивності організаційної структури, покращенню якості управління кадровим потенціалом та створенню унікальної організаційної культури для досягнення безпечного стану кадрової підсистеми й організаційно управлінської стійкості підприємств зв'язку [58].

На думку вченої Євтушенко Н.О., ефективним інструментом управління підприємством в умовах невизначеності та ризику є планування. За даних умов менеджмент підприємства має приймати обґрунтовані управлінські рішення щодо заходів не тільки з мінімізації економічних ризиків, а проводити прогнозування можливих втрат у майбутньому з урахуванням цілей: нормування витрат ресурсів підприємства (матеріальних та трудових), набору

професійних компетенцій менеджерів та інформаційного забезпечення (його рівень, якість) [63].

Огляд інструментів для формування стратегії забезпечення безпеко-орієнтованого розвитку підприємства представлено у роботі Отенко І.П. [67], а безпека підприємства, знову ж таки, вбачається станом ефективного використання ресурсів і можливостей, що забезпечує динамічний розвиток в умовах виникнення зовнішніх і внутрішніх погроз.

На думку Шкребеня Р.П., економічна безпека спрямована на досягнення цілей підприємства, тому це – невід'ємна складова процесу управління розвитком і лише аналіз умов функціонування та можливостей надає змогу проводити відбір та розробку дієвих заходів щодо безпеки підприємства [68].

У низці робіт прослідковується важливість інституційного забезпечення економічної безпеки для розвитку підприємства, до уваги беруться інтереси екзогенного оточення господарюючого суб'єкта, а саме держави, конкурентів, кредиторів, споживачів, постачальників, інвесторів, партнерів, за їх вподобаннями вибудовується модель поведінки для забезпечення стійкості конкурентної позиції підприємства на ринку. Подібний погляд у Кучеєва О.О., який вважає оточення, як найбільш впливовий елемент у прийнятті рішень для безпечного функціонування підприємства [70].

Вартує уваги праця Герасименко О.М., в якій йдеться про функціонування підприємства в умовах інформаційної економіки, а також концептуально обґрунтовано особливості функціонування системи економічної безпеки підприємства за даних умов [71].

Можемо припустити, що система включатиме елементи, складники, які захищаються на підприємстві для ефективної роботи підприємства, сам захист вбачається у протидії зовнішнім загрозам або ж стійкому "імунітету" до дії зовнішніх чинників, боротьбі із зовнішніми подразниками. Цікаво, що наразі підприємство розглядається також як система, а саме соціально-економічна система з притаманними їй рисами: цілісності (взаємне поєднання елементів), організованості (процес управління змінами у системі взаємного поєднання

елементів, системи зв'язків між ними), керованості (дія на чинники, досягнення результату), цілеспрямованості (усвідомленість завдання та їх виконанням для досягнення цілей).

У результаті вивчення питань щодо змісту безпеки прослідковується, що поняття "безпека" нашарувало розуміння його від суто фізичного (силового) до економічного, політичного, правового, екологічного, соціального, технологічного сенсів за сучасних умов.

Семантика пошуку серед наукових джерел тлумачень та визначень вченими понять "безпеки", "безпеки підприємства", надає змогу зробити висновок, що безпека підприємства є комплексним поняття, яке включене у загальне поняття безпеки, тому її забезпечення можливе не лише за врахування можливостей подолання на мікрорівні, а й на рівні національному, так як без захисту із-зовні державою неможливо убезпечити внутрішню безпеку підприємства (рис. 1.3)

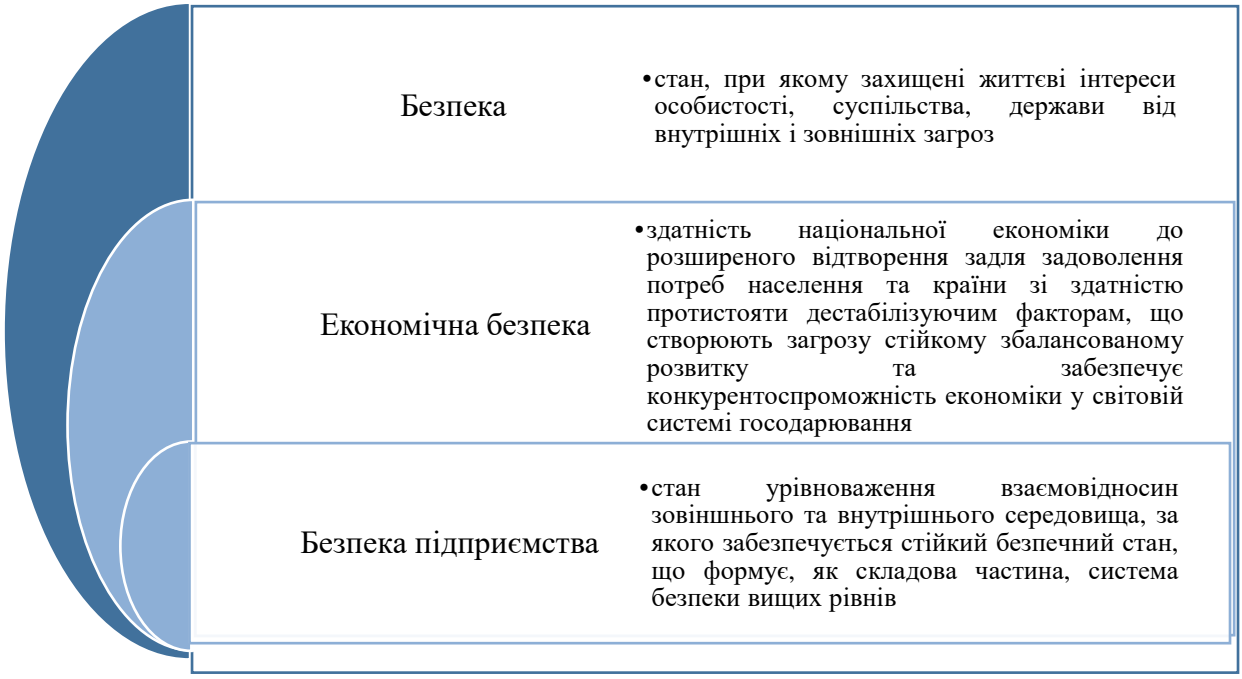


Рис. 1.3. Економічна безпека підприємства як комплексне поняття безпеки

(узагальнено та складено автором)

За своєю суттю економічна безпека є багатоаспектною, досягти стану безпеки підприємство спроможне при гарантуванні її державою шляхом: протистояння дестабілізуючим чинникам; створення відповідних умов для розширеного відтворення з метою задоволення потреб населення; забезпечення умов для ефективного господарювання; створення умов для формування конкурентного середовища функціонування економічних одиниць, як у національній, так і світовій системі господарювання.

Безпека тісно пов'язана з інтересами, так, об'єктом економічних інтересів для власників, інвесторів виступають результати діяльності підприємства (доходи, прибуток), для споживачів, з метою задоволення їх потреб, – результати операційної діяльності у вигляді виробленого продукту або наданої послуги. Саме інтереси є рушієм взаємовідносин, як у повсякденному житті між людьми, так і у бізнесі між підприємством та суб'єктами внутрішнього та зовнішнього середовища, з якими співпрацюють.

Ньюбоулдом Г. та Луффманом Г. було здійснено поділ зацікавлених сторін на чотири групи:

– стейкхолдери, якими здійснюється фінансування (можуть бути інвестори, акціонери, засновники);

– стейкхолдери, які представляють менеджмент (менеджери);

– стейкхолдери, які працюють на підприємстві (безпосередньо зацікавлені в досягненні цілей);

– стейкхолдери, які є економічними партнерами (покупці, постачальники).

Стейкхолдерами вважаються особи або групи осіб, які, здатні вплинути на досягнення господарюючим суб'єктом своїх цілей або на роботу організації в цілому, чий внесок (робота, капітал, ресурси, купівельна спроможність, розповсюдження інформації про компанію, тощо) є базою для успіху підприємства [94].

Отже, від врахування інтересів оточення залежать результати діяльності підприємства, тому при управлінні підприємством та захисті цільових результатів діяльності (прибутку) підприємство має рухатися у напрямку їх задоволення, в протилежному випадку виникатиме конфлікт інтересів, взаємонеузгодженість та непорозуміння, що призведе до дестабілізації відносин із оточенням підприємства, що порушуватиме його безпеку.

Варто зазначити, що переважній кількості визначень, що наведена згаданими авторами, притаманна ідентичність, а саме, економічна безпека підприємства являє собою захищеність від загроз.

На думку Ареф'євої О.В, Мягких І.М., Шкоди М.С. економічна безпека підприємства полягає у постійному, щоденному та цілеспрямованому забезпечення стабільної та ефективної роботи і має включати захисні заходи через побудовану систему безпеки для усунення загроз та дії різних чинників, які чинять вплив на підприємство [54, с.11]. Економічна безпека підприємства та особистості Захарченком В. І., Меркуловим М. М., Ширяєвою Л. В. визначається, як стан юридичних, виробничих відносин і організаційних зв'язків, матеріальних та інтелектуальних ресурсів, за нявності яких забезпечується надійність і стабільність функціонування, фінансово-комерційний успіх, прогресивний науково-технологічний та соціальний розвиток [55, с.50].

Не зовсім зрозумілим є визначення надане Філипповою С.В., Нізяєвою С.А., якими безпека розуміється як відкрита, штучна підсистема існуючої системи "підприємство", яка потребує відповідної регламентації, оцінки й управління [53 с. 11], однак, етимологія поняття "безпека" вказує, що безпека є природно утвореним поняттям і потреба у ній відчувається на всіх рівнях господарювання. Тому вважати її "штучною", тобто набутою не природнім шляхом, ніби вигаданою, не варто, вона є базовою й затребуваною усіма суб'єктами господарювання, не залежно від виду економічної діяльності, галузевої приналежності.

Виникає питання щодо припущення Ляшенко О.М., що економічна безпека підприємства досягається при узгодженості інтересів, що формують економічну свободу, а сам інтерес пов'язаний із діяльністю, яка виступає рушієм започаткування підприємства, його функціонування та розвитку. Головним у визначенні виступає економічна свобода та інтерес, однак, задоволення інтересів стейкхолдерів, оточення недостатньо, мають комплексно підлягати захисту всі елементи виміру наповненості, що формують безпеку підприємства. Науковиця доволі критично ставиться до розуміння безпеки, як стану або характеристики, вважаючи, що управління ними є некоректним з точки зору теорії та практики.

Із таким твердженням важко погодитися, з огляду дослідження напрацювань вчених, нами було з'ясовано, що безпека полягає у розвитку саме через те, що ним передбачається зміна станів. Підприємство постійно перебуває у пошуках покращення результатів діяльності, тяжіє до позитивних динамічних змін, тому його бажання до розвитку має захищатися. У визначенні, наданою Філипповою С.В., економічна безпека підприємства розглядається саме як динамічний процес, а не застигле явище, передбачає маневрування у відповідь на виявлені та приховані загрози середовища існування [91, с.19].

Характеристики безпеки, надані Мельником С.І., вбачаються також у розвитку та розгляді безпеки, як стану. Так науковцем визначення "фінансова безпека підприємства" представлено, як стан, при якому через ефективне використання всіх наявних ресурсів та прийняття адекватних, у кожній конкретній ситуації, управлінських рішень, формується рівновага, підтримується стійкість та стабільність, забезпечується надійність для досягнення поставлених цілей та завдань, реалізації стратегії розвитку шляхом застосування заходів своєчасного розпізнавання викликів, уникнення/зменшення ризиків, протидії/адаптації до негативного впливу загроз [93, с.27].

У науковому світі розвиток вбачається процесом, за якого відбуваються кількісно-якісні зміни, що призводять до стабільного функціонування

підприємства, а також виживання його складних, мінливих ринкових умовах, адаптації його до оточення, покращення економічного стану, зростання потенціалу. Узагальнено та перелічено елементи визначення розвитку підприємства Дундою С.П., як: кількісні та якісні зміни, процесний характер, сукупність процесів, адаптація до зовнішнього середовища, здатність протидіяти негативним впливам чинників зовнішнього середовища, поліпшення, довготривалість, зростання потенціалу підприємства, внутрішня інтеграція, підвищення життєздатності підприємства [52].

Приходимо до висновку, що безпека безперечно торкається питань розвитку, який є динамічністю станів з тяжінням до покращення результативних показників підприємства, його адаптування до чинників, змін, що виникають у ринковому середовищі та невизначених умовах сьогодення.

Загалом, функціонуючи підприємство стикається з безліччю невизначеностей, так вважав і М. Крозьє, якому належить вислів, що у підприємства море невизначеностей із острівцями визначеностей. Дана теза вкотре підкреслює важливість дослідження даної категорії через розуміння якої вибудовуватиметься підхід до управління безпекою. Безперечно управляти безпекою підприємства не просто, так оточення, стейкхолдери, в умовах нестабільних умовах можуть проявляти себе непередбачувано, виникає проблема керованості процесу і без того складного процесу управління.

Невизначеність оточення економічного середовища, наслідки руйнувань критично важливих об’єктів, підприємств, організацій формує нові бачення безпеки, в залежності від умов його функціонування. Категорія зберігає динамічність, формується інноваційно, проходить рефракцію через призму сприйняття оточення та змін, загроз, трансформацій, глобалізації та цифровізації, посилення інтернаціоналізації світових зв’язків.

Опрацювання (за семантичним пошуком) наукових доробків вчених щодо визначення поняття “безпека підприємства” дало змогу виокремити його визначники (табл. 1.1), які слугують маркерами сутнісної ідентифікації категорії.

Таблиця 1.1

Маркери безпеки підприємства за семантикою визначень науковцями поняття “безпека підприємства”

Визначення та маркери безпеки підприємства	Праці вчених
Захищеність від небезпек та зовнішніх впливів	Мелих О., Язлюк Б.О Камінський С.І., Швиданенко Г.О.,
Стійкість, розвиток, захист елементів від змін	Ситник Г.П.
Здатність організовувати діяльність, охоплюючи усі напрями, надійний захист від негативних внутрішніх, зовнішніх чинників впливу, усунення наслідків небезпек, адаптація до умов з мінімальними затратами	Кучмєєв О.О.
Захищеність від катастрофічного впливу дестабілізуючих чинників зовнішнього середовища за допомогою наявних ресурсів	Нестеров Ю.О.
Здатність своєчасно й ефективно мінімізувати потенційні загрози як спосіб уникнення чи мінімізації негативних економічних наслідків діяльності в результаті існування небезпеки та виникнення ризиків під впливом дестабілізуючих чинників середовища	Сосновська О.О.
Соціально-економічна система, що включає складові й визначається станом захищеності підприємств від внутрішніх і зовнішніх загроз, характеризується властивістю до адаптації змінам умов функціонування, здатністю протистояти загрозам	Шуміло О. С.
Чітко структурована система гарантування резистентності, ризикоредукції й економічної сукцесії підприємства	Тютченко С.М
Стан захищеності від загроз, ризиків, небезпек, що визначається їх адаптаційною здатністю до зміни зовнішніх економічних умов та постійною готовністю до їх погіршення, умінням вчасно створити нові економічні можливості, прийняти адекватні рішення	Ліщенко А.В
Економіко-організаційні, адміністративні та правові методи, форми та засоби впливу керуючої системи з метою мінімізації можливих втрат та досягнення стану його захищеності	Трачук Г.Ю
При узгодженості інтересів, що формують економічну свободу, а сам інтерес пов’язаний із діяльністю, яка виступає рушієм започаткування підприємства, його функціонування та розвитку	Ляшенко О.М.,
Характеризує умови функціонування підприємства, не контрольовані або контрольовані ним, що забезпечують йому певний рівень стабільності та стійкості, можливість самореалізації та розширеного самовідтворення шляхом протистояння зовнішнім загрозам і запобігання внутрішнім при наявності відповідних ресурсів	Єфімова Г.В.
Стан захисту підприємства від впливу зовнішніх та внутрішніх дестабілізуючих чинників, що характеризується стабільністю господарської діяльності та дотриманням інтересів підприємства	Чуприн Є.С.
Стан корпоративних ресурсів і підприємницьких можливостей, за якого гарантується найбільш ефективне їхнє використання для стабільного функціонування та динамічного науково-технічного і соціального розвитку, запобігання внутрішнім і зовнішнім негативним впливам та загрозам	Вівчар О.І.
Стан ефективного використання ресурсів і можливостей, що забезпечує динамічний розвиток в умовах виникнення зовнішніх і внутрішніх погроз	Отенко І.П.
Складова процесу управління розвитком при здійсненні аналізу умов функціонування та можливостей, відбір та розробку дієвих заходів для її забезпечення	Шкребень Р.П.
Оточення, як найбільш впливовий елемент у прийнятті рішень для безпечного функціонування підприємства	Кучеєва О.О

продовження таблиці 1.1

Постійне, щоденне та цілеспрямоване забезпечення стабільної та ефективної роботи і має включати захисні заходи через побудовану систему безпеки для усунення загроз та дії різних чинників, які чинять вплив на підприємство	Ареф'єва О.В, Мягких І.М, Шкода М.С.
Стан юридичних, виробничих відносин і організаційних зв'язків, матеріальних і інтелектуальних ресурсів, при яких забезпечується надійність і стабільність функціонування, фінансово-комерційний успіх, прогресивний науково-технологічний та соціальний розвиток	Захарченко В. І., Меркулов М. М., Ширяєва Л. В.
Відкрита, штучна підсистема існуючої системи "підприємство", яка потребує відповідної регламентації, оцінки і управління	Філипова С.В., Нізяєва С.А.

(складено автором за [30;32; 37;57;58;41;40;42-46;51;53;65;67;68;70])

Критичний аналіз визначення поняття "економічної безпеки підприємства" та виокремлення його визначників (маркерів) надає змогу сформулювати авторську дефініцію поняття "безпека підприємства" як стану стійкого функціонування й потенціальної спроможності його розвитку за умови відсутності небезпек (викликів, ризиків, загроз), а у разі їх появи – захищеності, що гарантує досягнення цільових безпекових результатів діяльності.

Можемо зробити висновок, що забезпечується безпека підприємства через побудову системи безпеки від глобального до мікрорівня з врахуванням потреб окремого індивіда й складових, які виступатимуть об'єктами захисту. Сама по собі система економічної безпеки підприємства представляє собою складну комбіновану цілісність із взаємопов'язаних між собою підсистем, окремих елементів, які існують окремо, але формують єдине ціле. Схематичне представлення поняття "безпека підприємства" (рис. 1.4) дозволить чітко виділити ключові вихідні елементи, що його формують.

Представлена на рис. 1.4 площина елементів, які формують розуміння безпеки потребує детального розгляду, оскільки їх розуміння та дослідження є базисом, так званою точкою відліку формування загальної безпеки підприємства. Засвідченням факту вагомості питань безпеки для підприємств є формулювання його цілей за існуючими теоріями фірм. Так, за системно-інтеграційною теорією фірми ціллю важливим аспектом у функціонуванні підприємства є стабільний розвиток підприємства.

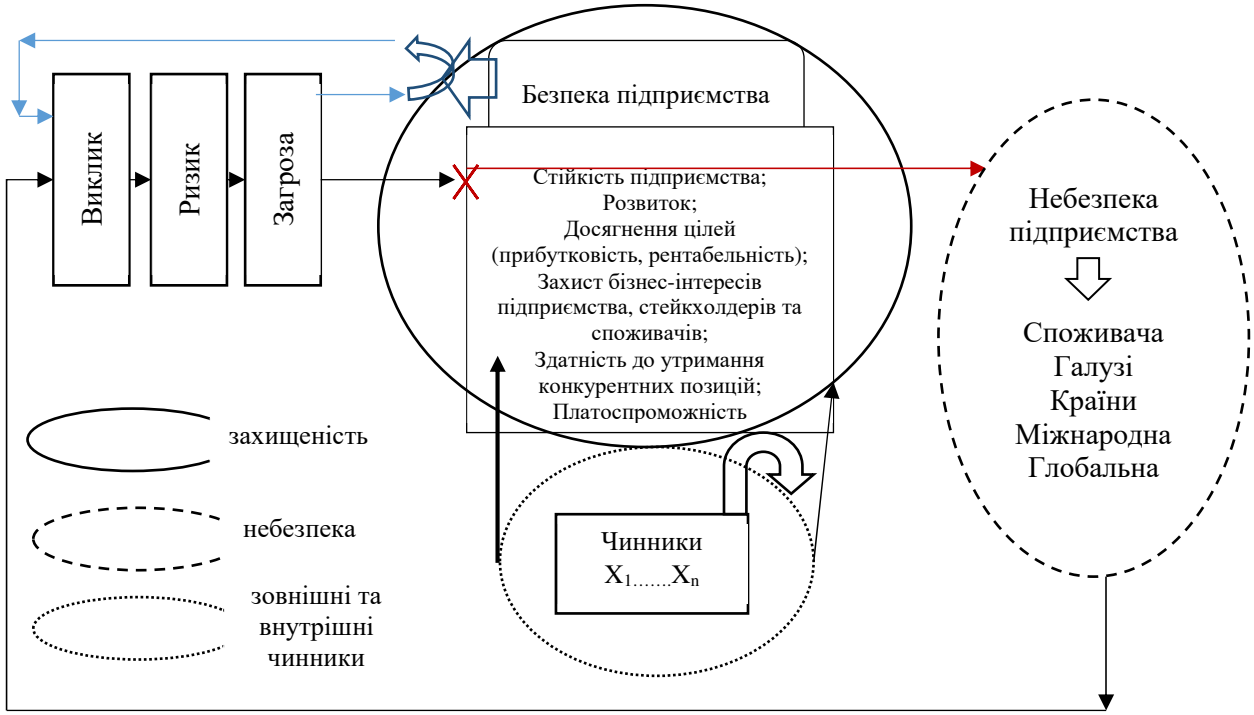


Рис. 1.4. Критеріальні параметри вимог безпеки підприємства

(авторська розробка)

Вивчення сутнісних особливостей безпеки, безпеки підприємства надало змогу висунути гіпотезу щодо окреслення цільових безпекових орієнтирів підприємства (результатів безпеки) із встановленням кореляції їх із попередньо розмежованими ризиками та загрозами, якими визначатиметься площина управління безпекою підприємства.

Відображення важливості безпеки знаходимо у традиційній та управлінській теоріях, де метою є максимізація прибутку, збільшення обсягів продажів та доходу, які характеризують безпечність його функціонування через отримання позитивних результатів діяльності. Із результатами діяльності пов'язана і теорія транзакційних витрат, за якою прагнення фірм концентрувалися навколо мінімізації витрат, тим самим збільшуючи прибуток та витрати. Поведінкова теорія вбачалася у гармонізації інтересів фірми та стейкхолдерів (зацікавлених осіб), підприємницька – в організації виробничого процесів задля задоволення потреб підприємця та забезпечення

конкурентоспроможності, а еволюційна теорія – в сталому розвитку. Тобто в теоріях чітко прослідковується схожість із безпековими питаннями в частині прибутків, зацікавленості сторін (інтересах), сталому розвитку, конкурентоспроможності. Аналіз теорій фірм, цілей створення підприємств дозволив виокремити маркери, які вказують на безпекові аспекти, які представлено на рис. 1.5.

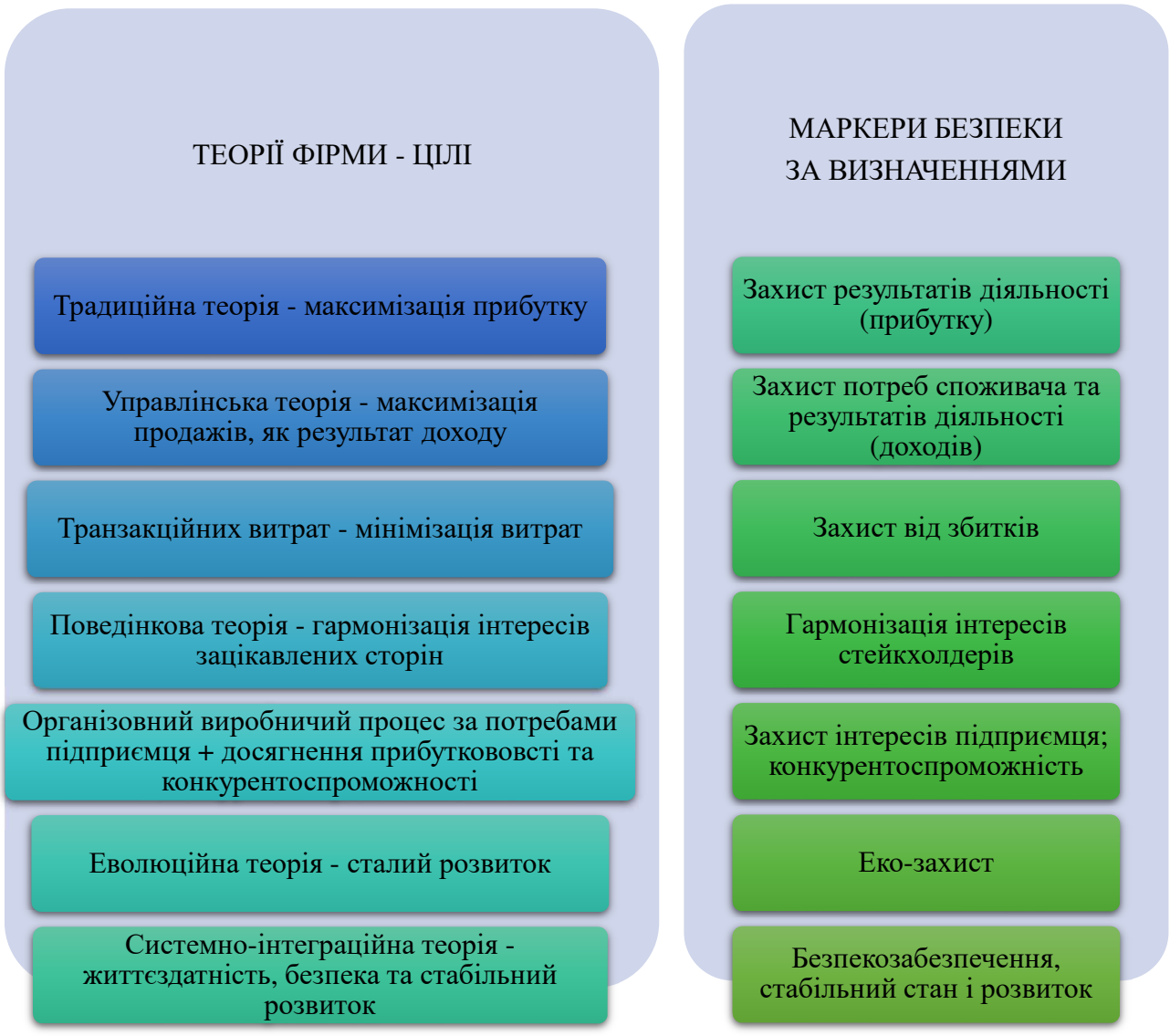


Рис. 1.5. Маркери безпеки підприємства відповідно до цілей створення підприємства за теоріями фірм

(складено автором за [95; 96; 97, с.84-85])

Нині підприємства тісно співпрацюють із оточенням, зосереджуються не лише на власних інтересах, а й на інтересах зацікавлених сторін, долучаючи їх до вирішення питань щодо постачання, купівель, пошуку нових каналів збуту. Як нами з'ясовано, гармонізація інтересів підприємства із оточенням, науковцями вважається важливим питанням для безпеки підприємства.

Гарантує економічну безпеку, сприяє забезпеченню економічного відновлення в умовах війни галузева спеціалізація національної економіки країни, яка має гармонійно узгоджувати фінансово-економічні інтереси стейкхолдерів та підприємств різних сфер [101].

Змінюється бачення оточення підприємства з часом, доповнень зазнала концепція стейкхолдерів. У середині 1970-х рр. Р. Акофф разом із групою дослідників [102], окрім персоналу, постачальників, покупців, інвесторів, кредиторів, державних інституцій, запропонували розширити коло зацікавлених сторін – майбутніми поколіннями. Зміни вбачалися у врахуванні інтересів людства в перспективі, прийнятті управлінських рішень підприємствами з врахуванням можливості вибору для наступних поколінь, що притаманно сталому розвитку в баченні екотріади розвитку (тривимірний захист інтересів поколінь у майбутньому: екологія, економіка, соціум).

Підсумовуючи, приходимо до висновку, що поняття безпеки, все ще нашаровується, змінюється з урахуванням глобалізаційних та трансформаційних змін, і найчастіше розглядається з позицій: стійкості (стабільності), захищеності (запобігання загроз); потенціалу, конкурентоспроможності, ступеня гармонізації економічних інтересів; використання ресурсів [103].

Більшість контекстів визначення безпеки втрачають її основу, яка полягає у саме у відсутності небезпек чи загроз, відкидати їх не варто, оскільки змінюється осередок її суті, що призводить до штучної модифікації науковцями його генези. При дослідженні безпеки в центрі уваги мають бути загрози, небезпеки, що існують для підприємства, шляхи їх усунення.

Отже, динамічні зміни, викликані глобалізацією, діджиталізацією, інтеграційними процесами, формування нових парадигм суспільного та економічного розвитку, поява нових викликів, які формують для підприємства як перспективи, так і небезпеки, потребують досліджень безпекових питань, на що варто реагувати підприємствам. Зміни безумовно призводять до перетворень, потребують нових поглядів та рішень в управлінні безпекою заради пристосування, адаптації та життєздатності підприємства у відповідь на виклики сучасності. З'ясовано, що нині формується новий погляд щодо змістовного наповнення поняття "безпека підприємства" в умовах геополітичного напруження та протиборства, дослідження безпекових питань потребує нових поглядів та фокусу не лише на прибутках підприємства як цілі, але й врахування інтересів стейкхолдерів, якими задається розвиток.

Проблематика безпеки, пошук шляхів її забезпечення із урахуванням низки подій та явищ, появи непередбачуваних дестабілізуючих чинників, які виникають в результаті ведення бойових дій на території нашої країни, є надважливими та потребують нагального, якісно продуманого та ретельно спланованого вирішення. Тому слід детально, послідовно та методично досліджувати питання безпеки, її змісту, ролі, значення, зміни у поглядах її розуміння з урахуванням динамічного розвитку всіх сфер в умовах цифровізації, інформатизації та переходу роботи підприємств у новий вимір функціонування із використанням технологій, нанотехнологій, квантових комп'ютерів, штучного інтелекту й, зрозуміло, з урахуванням невизначеностей, що нині огортають Україну та світ.

1.2. Понятійно-категоріальна площина елементів управління безпекою підприємства

Для ефективного та стабільного функціонування підприємства треба дбати про його безпеку, яка вбачається, як нами з'ясовано, у забезпеченні розвитку через протистояння зовнішнім впливам та загрозам, свободи від небезпеки або ризику. Безпека підприємства включає множину елементів, складових, тому, щоб захистити підприємство необхідно провести їх аналіз, зрозуміти їх значущість та потребу приділення уваги при управлінні безпекою підприємства.

Безпека, будучи складною категорією за своєю суттю, передбачає формування розуміння процесу управління. У даному контексті система передбачатиме множину елементів, взаємну узгодженість, взаємозв'язок між ними, що дозволить забезпечити управління безпекою підприємств.

Чітке визначення цих елементів надасть змогу окреслити площину безпеки, чим детальніше буде проведено їх опис та наданий перелік, тим правильніше окреслиться безпека підприємства. Елементи безпеки розглядатимуться як основа забезпечення безпеки, формують відлікові точки для управління безпекою, звісно, що первиною для цього слугуватимуть суб'єкти та об'єкти безпеки, вхідні, вихідні ресурси підприємства.

Узгодженість економічних інтересів між суб'єктами безпеки (з позиції підприємства) представлено на рис. 1.6. Суб'єктами безпеки підприємства зазвичай виступають особи; підрозділи, служби; органи; відомства та установи. Із боку держави питаннями захисту підприємства займаються законодавчі органи, виконавчі органи, судові органи, правоохоронні органи, науково-дослідні інститути, митні органи. Прослідковується взаємозалежність між суб'єктами, вони мають взаємоузгоджувати безпекові питання, починаючи від клієнта, закінчуючи організаціями, підприємствами світового рівня.

Рис. 1.6. Фокуси концентрації економічних інтересів між суб'єктами безпеки *(авторська розробка)*

Між підприємством і споживачами мають вирішуватися безпекові питання щодо задоволення потреб у товарах, роботах, послугах; безпечності продуктів, товарів, робіт послуг; підвищення рівня якості продукції, товарів, послуг та попиту на неї. Безпосередньо господарюючі суб'єкти мають забезпечувати безпечність виготовлення товарів, робіт, послуг; захист усіх ресурсів; гарантувати безпеку роботи персоналу; економічна безпеку як ціль; розвиток, розширення виробництва з метою отримання прибутку та примноження капіталу. Оскільки підприємство є тією ланкою серед економічних одиниць, що формують найбільшу частину дохідної частини бюджету, держава має створювати сприятливі умови для функціонування господарюючих суб'єктів через: захист товаровиробників, надавачів послуг; уникнення залежності від експорту комплектуючих (власне виробництво);

фінансова підтримка (податкові знижки, преференції); захист конкуренції. Інтереси підприємство-світ вбачаються у забезпеченні сталого розвитку, як напрямку безпеки; дотриманні міжнародних стандартів безпеки щодо товарів, робіт, послуг; захист експортно-імпортних операцій; сприянні міжнародних дружніх економічних зв'язків.

Суб'єкти безпеки можна розділити на дві групи, перша – ті, хто безпосередньо відносяться до підприємства (служба економічної безпеки, відділ якості, охорона, пожежна служба, відділ інформаційної безпеки, персонал та керівництво), друга – відноситься до зовнішніх суб'єктів (державу й законодавчі органи, виконавчі органи, судові, правоохоронні, митні органи, установи освіти та науки, дослідницькі інститути), конкурентів, постачальників, органи місцевої влади (територіальні громади), покупців, суб'єктів ринкової інфраструктури, міжнародні організації, країни-партнери.

Об'єкти і суб'єкти знаходяться у постійній взаємодії, в управлінні безпекою вони відіграють ключову роль, тому що саме їх захист від невизначеностей та чинників впливу є першочерговим. Суб'єкт постійно діє на об'єкт і його складові, є невіддільним від нього, обидва вони підлягають впливу чинників та невизначеністю середовища (рис. 1.7).

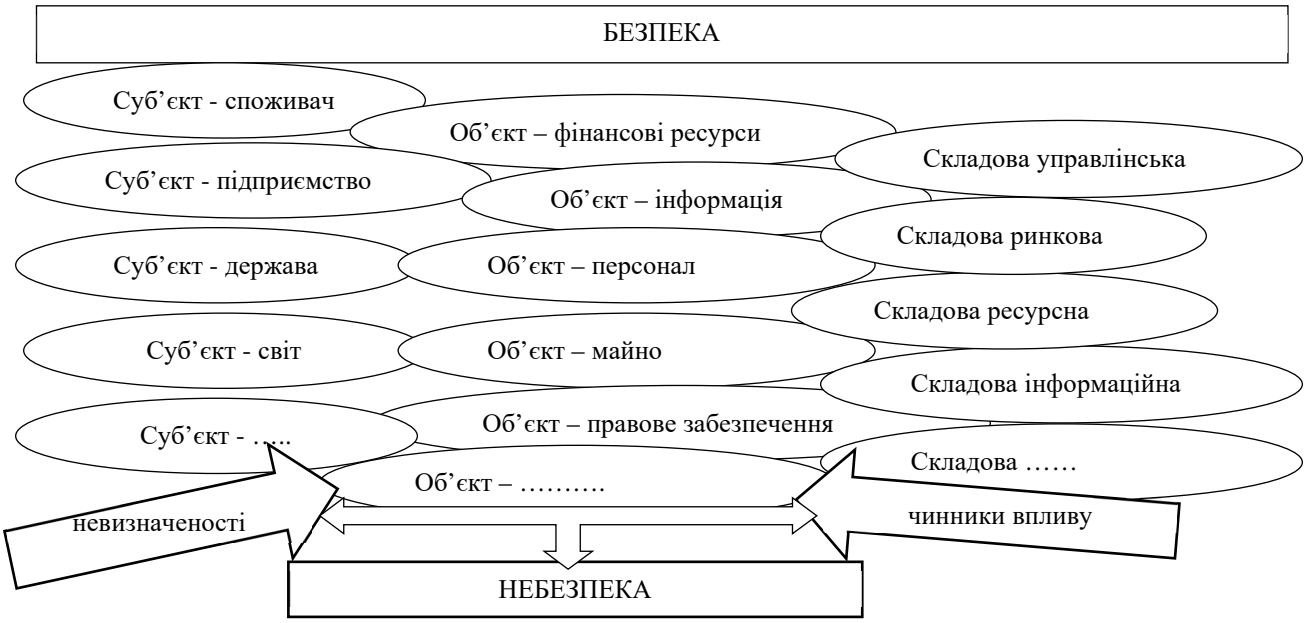


Рис. 1.7. Багатовимірна суб'єкт-об'єктна дія на складові безпеки підприємства *(авторська розробка)*

Якщо інтереси підприємства не збігаються з інтересами суб'єктів зовнішнього середовища, то в діяльності підприємства неминуче виникнуть зміни негативного характеру.

Детальний опис суб'єктів, об'єктів, складових, чинників та невизначеностей надасть базис для побудови надійної системи управління безпекою підприємства, чим більше охоплено складових безпеки, тим ефективніше спрацює система.

Аналіз наукових праць, в яких досліджувалося поняття "економічна безпека підприємства" та результати, що нами отримані, надали можливість графічно інтепретувати розуміння його змістовного наповнення та окремим блоком виділити "виклик–ризик–загрозу", які виникають у разі неможливості віддзеркалити чинники впливу, і, як наслідок, вони переходять в іншу форму. У залежності від реагування на чинники та обрання заходів боротьби з ними, форми їх прояву можуть нести різні за ступенем дії наслідки.

Очевидним недоліком більшості визначення науковцями економічної безпеки, як нами з'ясовано, є неврахування розуміння його сутності на базову рівні сприйняття, інтуїтивному, яке вбачається у відсутності небезпек чи загроз.

Окреслення контексту безпеки для підприємства відбувається за огляду наявності сприятливих або несприятливих умов, які існують як поточні, минулі, можливі у майбутньому, що чинять вплив на функціонування підприємства, розвиток, стан. Ступінь сили впливу чинників переходить, у міру їх наростання, в форми: початкового виклику, який переходить у ризик, що в подальшому трансформується у загрозу. Кожна наступна форма несе за собою більший негативний вплив, тому ідентифікацію чинників варто визначати якомога раніше, щоб упередити від руйнівних впливів та нарощення загроз.

Початковим до розгляду є виклик – сукупність обставин, не обов'язково загрозливого характеру, які потребують реакції на них [31, с.14], тобто є станом невизначеної напруженості, що виникає на підприємстві, реакція вирішення. Його можна визначити як протиріччя між наявним станом системи і потребою у внутрішніх змінах, а також він є теоретичним (інформаційним) проявом

деструктивних чинників. Інколи виклики і реакція на них споглядаються з позитивного боку, наприклад виклик цифровізації, призвів до спростування багатьох бюрократичних питань, полегшенню документообігу через появу цифрового підпису, електронного документообігу, електронних платежів, крім того, з'явилася нова платформа для торгівлі – електронної. Реакція на виклик, що надійшов із-зовні призводить до пришвидшення та спрощення багатьох процесів, але за наявності інформаційно-комунікаційних технологій, набуття цифрових навичок та якісних послуг електронних комунікацій. Цифровізація посилила роль підприємств сфери зв'язку, без послуг, що ними надаються продовжувати працювати у таких умовах, як невизначеність – пандемія, а з лютого 2022 року – воєнного стану було б доволі проблематично. Тому виклик для підприємств як цифровізація та вчасна реакція на нього підготував підприємства працювати в надскладних умовах, бути готовими до невизначеностей та продовжувати функціонувати.

Реагувати на виклики не обов'язково, головне – дослідити наслідки їх дії на підприємство, у разі негативних – відповідати на них.

Наступною категорією просування за шкалою "виклик–ризик–загроза" є ризик. На відміну від виклику, ризик вказує на ймовірність настання події, відхилення результату від запланованих, очікуваних.

Вперше дане поняття в європейському регіоні, а саме в Італії, зустрічається ще у 1248 році, використання його тісно пов'язане із морською торгівлею, ризикам, що виникали на морі під час транспортування вантажів. У книзі Яна Бертінга [75, с.130] слово "ризик" має походження від італійського "risco", яке є похідним від латинського "resecum", що означає "те, що ріже". Звідси стає зрозумілим, до чого торговельна діяльність та транспортування морем, бо малася на увазі можливість зіткнення кораблів зі скелею (те, що ріже) під час транспортування вантажів. Пізніше, 1347 року, в Генуї з'являється перший страховий поліс в морській торгівлі, який містить у собі інформацію про ризики під час перевезення товарів кораблем морськими шляхами з Генуї до Майорки [76].

За оксфордським словником англійської мови ризик (від англ. risk) – це ситуація, пов’язана з небезпекою; ймовірність (можливість) того, що станеться щось неприємне. Ризик – це кількісне або якісне оцінювання небезпеки [28, с. 32], тобто поняття дотичне із небезпекою.

У Постанові КМУ щодо внутрішнього контролю розпорядниками бюджетних коштів, ризик визначений як можливість настання події, що матиме вплив на здатність установи виконувати завдання і функції та досягати визначеної мети (місії), стратегічних та інших цілей діяльності установи [114].

У посібнику, що складений з врахуванням плану заходів з реалізації Стратегії реформування системи управління державними фінансами на 2022 - 2025 рр. (схваленого від 29.12.2021 № 1805-р), наведене наступне визначення поняття “ризик”: “потенційна можливість того, що під час реалізації функцій, процесів та операцій, спрямованих на досягнення встановленої мети (місії), цілей та виконання завдань, можуть виникнути обставини, що призведуть до втрат ресурсу, небезпеки або небажаного результату у майбутньому” [116]. Знову ж таки у визначенні ризику “можливість небезпеки” сприймається як ключовий визначник ризику. Подібної думки, що ризик передує загрозі, є первинною категорією по відношенню до неї, а загроза випливає з ризику і є вторинною, дотримується Горячева К.С. [78].

У посібнику під редакцією Орлова В.М. надано наступне визначення поняттю “ризик” – суб’єктивно-об’єктивна економічна категорія, яка характеризує невизначеність кінцевого результату діяльності внаслідок можливого впливу (дії) на нього низки об’єктивних та/або суб’єктивних чинників, які не враховувалися при його плануванні [119, с.457].

С. Хадон вбачає, що ризик виражає ймовірність настання небажаних подій, вірогідність нанесення шкоди й одночасного розгляду цієї ймовірності та негативних наслідків [74, с.7]. Як ймовірність негативного відхилення результатів конкретних рішень або дій від очікуваних, вбачають ризик Швиданенко Г. О., Кузьомко В. М., Норіцина Н. І. [32, с.15], автори

підкреслюють лише ймовірність часткової втрати ресурсів, доходів, зростання витрат підприємством.

Ризик можна сприймати не лише як ймовірність настання події, що може перейти у загрозу й призвести до небезпеки у результаті неврахованих або неусунутих впливів, а й потенційна можливість розвитку за певних умов та використання їх на користь підприємства. Отже, ризик – не тільки загроза, а потенційна позитивна можливість розвитку підприємства. Ризик – це безпосередньо умова появи у площині безпеки її антиподу – небезпеки, але небезпека за ризику залишається на рівні можливості, є гіпотетичною (може бути прихованою/ передбачуваною). Часто ризик пов'язують із теорією ігор та вірогідністю, тому обчислюється кількісно за вірогідністю ризику.

Тож, спираючись на знання етимології ризику, можемо зробити висновок, що ризики є подіями, які можуть не відбутися (оскільки ризику притаманний ймовірнісний характер), характеризує стан підприємства, як небезпечний, але у разі, якщо ймовірність його настання близько 0%, тоді ми будемо говорити про виклики. Якщо ж, ризик наближатиметься за вірогідністю свого настання до 100%, то перейде у наступну категорію – загрозу, що характеризуватиме стан безпеки як небезпечний. Тобто ймовірність ризику більше нуля, але менше 100, саме у цих межах йдеться про ризик. Якщо ймовірність настання події дорівнює 0, тоді подія не відбудеться, якщо дорівнює одиниці – подія реальна і відбудеться. Відбувається ніби перехід гіпотетичної вірогідності у реальну дію, можемо стверджувати, що ризик перетворюється на загрозу.

Загроза – це небезпека на стадії переходу з можливості в дійсність [55, с.216], вважає Захарченко В. І., Меркулов М. М., Ширяєва Л. В., з переходом із можливого в дійсне, погоджуємося, а небезпеку сприйматимемо, як окрему категорію, яку окреслимо трохи згодом.

Загроза являє собою форму вираження протиріч між інтересами підприємства та зовнішнім середовищем його функціонування, яка відображає реальну або потенційну можливість прояву деструктивної дії різних чинників та умов на їх реалізацію у процесі розвитку і, яка спричиняє прямий або

непрямий економічний збиток, навмисне чи випадкове (ненавмисне) порушення режиму функціонування підприємства [28, с. 27].

У підручнику [72, с.63] авторським колективом загроза діяльності підприємства вбачається у наявному негативному впливі на підприємство і пояснюється наявністю процесів та явищ, які відбуваються у внутрішньому та зовнішньому середовищі підприємства та діями (поведінкою) суб'єктів зовнішнього середовища за певних умов.

За аналізованими визначеннями, на нашу думку, загроза – це вже реальна подія, за якої потенційна небезпека переходить зі стану можливості у реальну площину. Для виникнення загрози є активними обидва компоненти: існують як самі негативні чинники, так і можливості їх впливу на об'єкт економічної безпеки. Конкретна та безпосередня форма небезпеки, що зумовлює об'єктивно та суб'єктивно негативний вплив, які містять у собі деструктивні дії, і є загрозою. Об'єктивно негативні впливи йдуть усупереч інтересам підприємства, виникають самі по собі без участі керівництва та персоналу, суб'єктивні негативні впливи є результатом неправильного та неефективного керування, тобто з'являються через помилки або некомпетентність керівництва, персоналу.

Наступною категорією, яка вартує уваги є небезпека, її джерелами появи виступають умови та чинники, що містять деструктивну основу для її появи, сама ж небезпека є станом, протилежним безпеці.

Дане поняття корелює із безпекою, без нього важко визначати та ідентифікувати площину безпеки, крім того виклик – ризик – загроза є вектором руху від безпеки до небезпеки. Поняття безпека і небезпека є протилежними за своїм значенням, що підтверджується тим фактом, що безпека вбачається по-перше, у можливій відсутності небезпеки, по-друге, реальною захищеністю від небезпек. В обох випадках йдеться про небезпеку, точніше її відсутність, що вказує на потребу її вимірності, щоб ідентифікувати безпеку, можна припустити, що поняття взаємозалежні, є точка, в якій небезпека переходить у стан безпеки.

Небезпека вбачається гіпотетичною на думку Тулуб О., авторка вважає, що ні об'єкт, ні суб'єкт невідомі, нанесення збитків гіпотетичне за певних умов, а саме загроза є наміром і можливістю нанесення збитку одночасно, має конкретний характер направлення, тобто націлена на об'єкт. Проте, гіпотетичність вказує на ймовірнісний характер, що притаманно ризикам, тому з думкою важко погодитися і сприймати небезпеку "суб'єктивним наміром" або "об'єктивною можливістю" нанесення збитку [89, с. 8-9]. На нашу думку, все ж таки небезпека є станом з чітко вираженими змінами у функціонуванні підприємства.

Двояко сприймається визначення, яке надали автори Швиданенко Г. О., Кузьомко В. М., Норіцина Н. І., так, погоджуємося із тим, що небезпека є станом, "… погіршують її стан, надають її розвитку небажаної динаміки або параметрів", однак, не можемо не погодитися із формулюванням "…це об'єктивно існуюча можливість негативного впливу на економічну систему, в результаті чого їй може бути завдано яких-небудь збитків, шкоди….", це вказівка на вірогідність негативного впливу, що асоціюється із ризиками [32, с.16].

Авторами Сосновською О.О. та Житарем М.О. небезпека вважається формою прояву загрози, що призводить до зміни параметрів функціонування підприємства та кінцевих результатів його діяльності. Небезпека продукує появу суб'єктивних або об'єктивних подій у різних сферах діяльності підприємства через загрози, що призводить до позитивного чи негативного результату. Загроза розглядається авторами, як потенційна можливість отримання негативного економічного результату для підприємства, що виникає внаслідок існування небезпеки та виникнення ризиків під впливом дестабілізуючих чинників внутрішнього та зовнішнього середовища [58, с. 129]. На нашу думку, вкрай важливо для підприємства бути спроможним швидко, дієво нейтралізувати потенційні загрози, бо самі від правильності та швидкості прийняття рішень залежатиме економічна безпека та її рівень, стійкість функціонування підприємства в невизначених умовах.

Подібним баченням небезпеки є визначення її, як форми прояву загрози, що призводить до реальних втрат [54, с. 111], тобто виникає від дії загроз, а не вірогідності їх появи (ризику), що дає змогу припустити, що небезпека також є станом, як і безпека, бо відбуваються зміни, спостерігається певна динаміка. У противагу безпеці будуть віддзеркалюватися основні визначники безпеки, зокрема: розвиток – занепад або стагнація.

При реалізації загрози можливий збиток оцінюється за рівнями небезпек:

– незначна небезпека, коли існує здатність суб'єкта небезпеки завдати незначної шкоди тому іншому об'єкту (індивіду, соціальній групі, державі тощо);

– середня небезпека – здатність суб'єкта небезпеки завдати такої шкоди об'єкту, коли стає неможливим його нормальне функціонування, а саме, коли виникають суттєві труднощі у виконанні життєво важливих для нього функцій;

– висока небезпека – здатність суб'єкта небезпеки завдати такої шкоди об'єкту, коли стає практично неможливим виконання життєво важливих для нього що, зрештою, може призвести його до загибелі [55, с.17].

Враховуючи вищевикладене, нами з'ясовано, що безпека є станом, тому цілком логічно диференціювати рівні безпеки (небезпеки), як відбувається при оцінці стану безпеки в результаті техногенних впливів. Водночас, опрацювавши низку джерел, нами з'ясовано, що відбувається плутанина навколо понять, які близькі за зазначенням і формують площину безпеки функціонуючого підприємства. Дану проблему, на нашу думку, вирішить їх відокремлення на ділянках, що відображатимуть стани безпеки (небезпеки), пропонується представити їх графічно з подальшим поясненням (рис. 1.8).

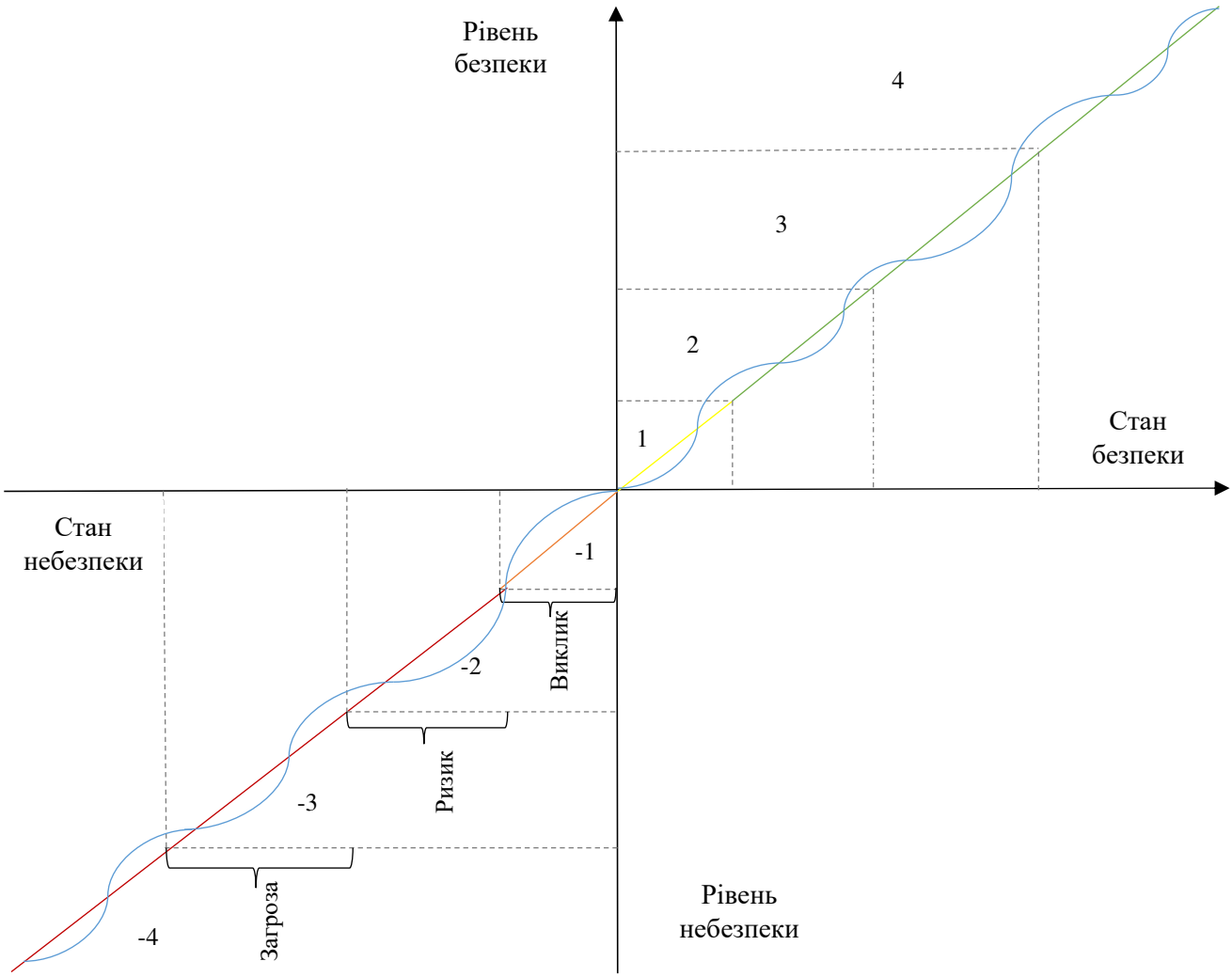


Рис. 1.8. Модель оцінки небезпеки підприємства (графічна інтерпретація) *(авторська розробка)*

Графічне представлення станів безпеки та небезпеки, на нашу думку, демонструє ступінь наростання небезпеки на відрізках дії: виклик, ризик, загроза, останній відрізок є найнебезпечнішим і, навпаки, рух по прямій угору відзначається наростанням станів безпеки – найкращий для підприємства у зоні 4. Кожному із відрізків відповідає стан безпеки або небезпеки:

-1 – незначний стан небезпеки;

-2 – передкризовий стан небезпеки;

-3 – кризовий стан небезпеки;

-4 – критичний стан небезпеки;

1 – відносний (порівняно) стан безпеки;

2 – нормальний (безпечний) стан безпеки;

3 – стабільний стан безпеки;

4 – досконалий стан безпеки.

Дана градація станів безпеки дозволить відслідковувати процес їх зміни з можливістю здійснювати управління відповідно до конкретних ситуацій, впливів, умов, що призводять до перетворень та порушень на підприємстві.

Дослідження ґенези поняття "безпека", аналіз праць науковців щодо визначення понять "безпека підприємства", надав змогу зробити висновок щодо основних ознак безпеки, які полягають у: здатності до розвитку; стійкості, конкурентоспроможності; платоспроможності; прибутковості та рентабельності; врахуванні інтересів стейкхолдерів. Не варто забувати, що безпека підприємства найбільше торкається питань захисту прибутку, як основної цілі господарюючого суб'єкта, що підтверджується тим, що дві із існуючих теорій прибутку пов'язані саме із ризиками:

– за теорією ризику прибутку (Ф.Б. Хоулі), прибуток є винагородою за ризик у бізнесі (далі Н. Карвер, підтримуючи таку думку, продовжив: "прибуток є результатом розумно підібраних ризиків") [105, с. 456];

– за теорією прибутку, що несе невизначеність (Френк Х. Найт), що грунтується на теорії ризиків прибутку, наведено припущення, що існують передбачувані та непередбачувані ризики, останні і є невизначеністю [106].

Тож, безпека тісно пов'язана з ризиками, викликами, умовами, невизначеністю, загрозами, точніше з їх відсутністю, тому варто розібратися з їх сутністю. Пошук площини забезпечення безпеки, спричинив потребу в уточненні та розмежуванні понять, що її формують, з'ясовано, що виклики можуть призвести чи не призвести до змін, які матимуть або позитивні (за певних умов) або негативні зрушення. Виклик не завжди переходить у ризик, який є ймовірністю появи змін і перетворення їх у реальну дію у результаті появи загроз, що порушують безпеку та рухають функціонуюче підприємство до переходу у стан небезпеки. Дія ризику та загрози різнитиметься, так,

розглядаючи ключові ознаки підприємства, можемо припустити, що їх дія, відповідно до ознак, співвідноситися таким чином (ознака безпеки – ризик – загроза):

1) здатність до розвитку – ймовірність призупинення розвитку – гальмування розвитку;

2) конкурентоспроможність – вірогідність втрати конкурентоспроможності – втрата конкурентних переваг; неконкурентоспроможність;

3) стійкість – вірогідність втрати стійкості – порушення стійкості;

4) платоспроможність – вірогідність втрати платоспроможності – погіршення показників платоспроможності – втрата платоспроможності;

5) прибутковість та рентабельність – ймовірність зниження рентабельності та прибутковості – зростання витрат, скорочення темпів приросту прибутку та рентабельності;

6) інтереси – ймовірність невідповідності та порушення інтересів – дегармонізація, порушення інтересів.

Відображення різниці між впливом ризиків та загроз, їх дію у вигляді результатів зміни ознак безпеки з формуванням передумов для небезпеки, представлено на рис. 1.9.

Схематичне представлення наслідків реалізації загроз та дії ризиків потребує більш глибинного вивчення з формуванням нових підходів до їх аналізу, оцінки, спираючись на концептуальні рішення забезпечення безпеки.

Нинішні умови, в яких функціонують підприємства, як вже зазначалося, особливі, в яких не перебувало суспільство, здавалося б, малоймовірні, проте, на жаль, реальні. Умови посилюються цифровізацію сфер діяльності, інформатизації, переходом у новий технологічний вимір.

Рис. 1.9. Концепт цільових безпекових орієнтирів підприємства *(авторська розробка)*

Питання безпеки є нагальним, актуальним і вбачається його вирішення за рахунок врахування напрацювань та досвіду їх розв'язання науковцями-попередниками.

Сукупність невизначеностей, що постали перед людством, суспільством, державою, господарюючими суб'єктами нагадують величезну полум'яну кулю із безліччю викликів, ризиків загроз, що посилюються обставинами

непереборної сили – воєнним станом. Не просто так окремим напрямом діяльності серед операційної, маркетингової, фінансово-економічної; виробничої, інноваційної, інвестиційної, інформаційної, обліково-контрольної, в управлінській діяльності нещодавно виокремлено безпекозабезпечувальну діяльність.

Пояснення появи безпекозабезпечувальної діяльності, як окремої гілки в управлінні, надано у роботі Вахлакової В.В., як: "….експоненціальне зростання кількості загроз функціонуванню різноманітних об'єктів на всіх рівнях соціально-економічної системи, мультиплікатизація їхнього впливу через одночасність реалізації та її серйозні наслідки" [61].

Тобто, безпекозабезпечувальна діяльність є новим видом управлінської діяльності на підприємстві, а її виникнення зумовлено складністю умов функціонування підприємств у нинішніх умовах, усвідомленням важливості для їхньої діяльності безпеки (економічної, технологічної, інформаційної, екологічної та ін.), необхідністю її постійного, системного забезпечення за дієвого управління наявними ресурсами (фінансових, інтелектуальних, матеріальних, та ін.).

Безпекозабезпечувальна діяльність підприємства, як вид управлінської діяльності зосереджується на спостереженні за процесами та явищами, що відбуваються у зовнішньому та внутрішньому середовищі діяльності підприємства, відслідковуванні загроз діяльності та розвитку підприємства. Аналізуються процеси та явища, що відбуваються у зовнішньому та внутрішньому середовищі діяльності підприємства, ідентифікуються загрози діяльності та розвитку підприємства, проводиться аналіз наслідків реалізації загроз. Далі здійснюються заходи щодо: попередження та уникнення загроз діяльності, розвитку підприємства; зменшення негативних наслідків від реалізації загроз шляхом: організаційної діяльності з їх убезпечення; координаційної діяльності та контролю за виконанням завдань з убезпечення. Напрями безпекозабезпечувальної діяльності та їх зміст як виду управлінській діяльності підприємства представлено на рис. 1.10.

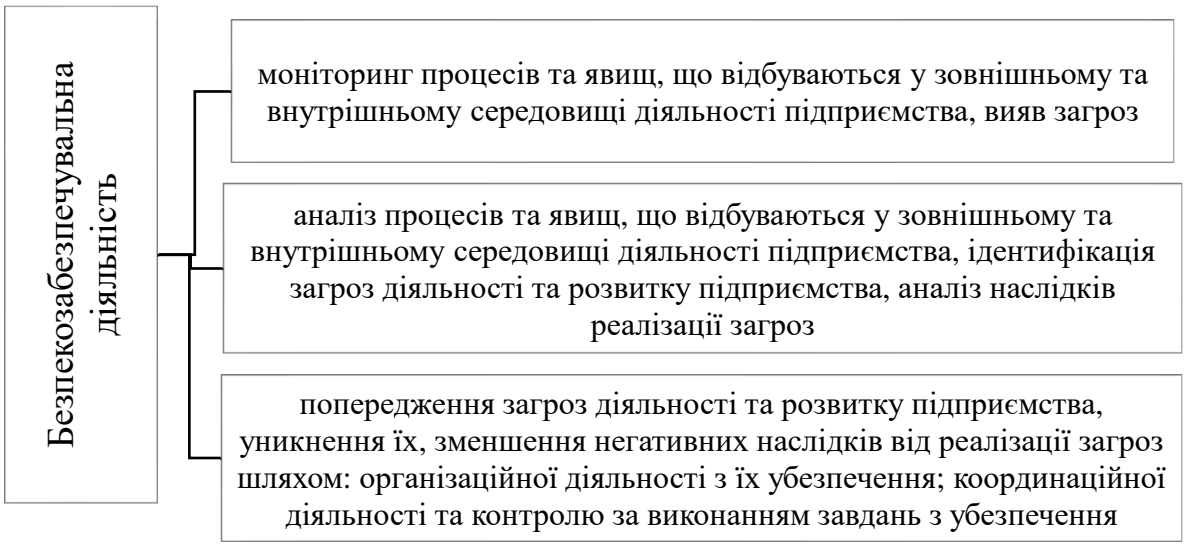


Рис. 1.10. Функціонал безпекозабезпечувальної діяльності в управлінні підприємством

(складено автором за [59; 60; 61])

1.3. Складові безпеки підприємства та множинність чинників впливу на безпеку підприємства

У попередньому пункті роботи нами було визначено, що підприємство є системою, безпека підприємства компонує систему елементів та передбачає їх захист, при чому система формується із взаємозв'язаних, поєднаних, взаємодоповнюючих складових, які є його основою, що слугуватимуть при дослідженні безпеки початковими точками для побудови підходів до її аналізу, оцінки, забезпечення з використанням методологічного базису та концептуальних засад управління безпекою, при чому до кожного елемента вбачитиметься окремий змістовний підхід.

Вивченню складових економічної безпеки підприємства присвячені наукові праці вчених: Ю. Работіна, В. Вороніної, Т. Меліхової, Б. Буркинського та В. Грищенко, С. Ілляшенко, Е. Данілової, Б. Дуб, С. Покропивного, В. Геєця, Швиданенко Г.О., Шевченко І., Васильців Т.Г., Волошин В.І, Бойкевич О.Р.,

Зубко Т.Л. [6; 7; 8; 9; 10; 11; 12; 13; 18; 28; 31; 85; 90; 92], однак невизначені умови, що виникають впродовж останніх трьох років потребують розширення переліку складників з урахуванням посилення ролі електронних послуг, цифровізації економіки та діджиталізації суспільства в період пандемії та воєнного стану в країні. У напрямку розгляду питання – важливості послуг сфери інформаційно-комунікаційних технологій у функціонуванні та безпеці підприємств, проведено низку досліджень вченими: О. Гудзь, Л. Худолій, С. Легоміновою, В. Сотниченком, О. Сосновською, В. Пильновою [14; 15; 16; 17], які слугуватимуть базисом для проведення аналізу та обґрунтування важливості інфокомунікацій як складової економічної безпеки підприємства.

В умовах невизначеності та глобальних проблем людства, таких як: пандемія, що спричинена поширенням коронавірусної хвороби, проблеми зміни клімату, війни, недостатня забезпеченість продовольчими товарами та енергоносіями у деяких країнах світу, відсутність послуг зв'язку, освітніх послуг призводять до актуалізації питань "економічної безпеки". Питання стосуються й базового соціального забезпечення, котрі визначаються рівнем доступу до інфраструктури (в сфері транспорту, зв'язку, освіти, здоров'я, безпеки). Звісно ж, аналогічні питання торкаються й суб'єктів господарювання, особливо гостро питання економічної безпеки підприємств постає в обставинах непереборної сили, до яких відносять і воєнний стан в України. Будь-яке підприємство, бізнес-структура має дбати належним чином про економічну безпеку, щоб виконувати свою функцію – задовольняти потреби споживачів та отримувати прибуток, а для держави виступати як економічна одиниця, яка забезпечує виконання своїх функцій та поповнювати бюджет. Саме вивчення складових економічної безпеки з урахуванням несприятливих умов та змін, що ними спричиняються, можуть стати у нагоді при формуванні механізмів та розробці комплексних заходів щодо усунення загроз та забезпеченні економічної безпеки підприємства, чим і актуалізується питання для дослідження.

Із урахуванням посилення ролі електронної комунікації в нинішніх умовах невизначеності перегляд та можливість розширення переліку складових економічної безпеки підприємства в даних умовах дозволить удосконалювати оцінювання економічної безпеки підприємства та враховувати результати оцінки при розробці заходів, інструментів, механізмів управління економічною безпекою підприємства.

Із плином часу та розвитком економіки та суспільства поняття "економічна безпека підприємства" переходить у новий формат, який включатиме інформатизацію та цифровізацію економічних процесів в складниках, які враховуються при формуванні механізму управління економічною безпекою підприємства. Електронні комунікації при цьому відіграють особливу роль, оскільки забезпечують безперебійне функціонування господарюючих суб'єктів в умовах невизначеності, як спостерігалося в період запровадження локдауну при поширенні коронавірусної хвороби, так і під час воєнного стану [107]. Сфера зв'язку слугує невід'ємним компонентом у діяльності всіх підприємств, крім того, визначається критично важливим сектором, оскільки забезпечує допоміжну функцію у всіх секторах інфраструктури, в тому числі – критично важливих.

Інформаційні технології виокремлено як один із 16 важливих секторів критичної інфраструктури, що підтверджується директивою PPD-21 [4]. За Законом України "Про критичну інфраструктуру" [1] серед критично важливих послуг – інформаційні послуги та електронні комунікації. У переліку секторів (підсекторів), основних послуг критичної інфраструктури країни знаходиться й інформаційний сектор, який містить:

1) підсектор інформаційних технологій, який включає в себе:

– надання хмарних послуг, у тому числі зберігання та обробки даних у центрах обробки даних та/або хмарних сховищах, здійснення хмарних обчислень;

– забезпечення функціонування систем електронного урядування;

– розповсюдження ефірного цифрового наземного мовлення з використанням радіочастотного спектра в трьох та більше областях країни.

2) підсектор електронні комунікації, який включає в себе:

– забезпечення функціонування точок обміну Інтернет-трафіком (IXP);

– адміністрування адресного простору українського сегмента Інтернету, у тому числі надання послуг з підтримки та адміністрування систем доменних імен (DNS) в Інтернеті;

– адміністрування та ведення реєстрів доменних імен верхнього рівня в Інтернеті, у тому числі домену “.UA”.

Сфера зв’язку представляє собою конкурентоздатну, взаємопов’язану сферу, що поєднує та використовує наземні, супутникові та бездротові системи передачі даних, між собою пов’язані провайдери дротової, супутникової та бездротової мережі, наразі вони залежні один від одного в частині передавання та термінації трафіку, компанії часто спільно використовують засоби та технології для забезпечення відповідності та можливості якісного та безперебійного надання електронних комунікаційних послуг підприємствами-постачальниками.

Однозначно, що господарюючі суб’єкти, не залежно від того, яку діяльність вони провадять, намагаються виконувати свої функції та функціонувати, що уможливлюється в умовах невизначеності саме за рахунок електронних послуг, що надаються операторами та провайдерами зв’язку [108].

Слід підкреслити важливість еволюції інформаційно-комунікаційних технологій, які продовжують забезпечувати високий рівень взаємопов’язаних цифрових й електронних операцій в межах безпеки на всіх рівнях: мікробезпеки (підприємства), мезобезпеки (регіонів), макробезпеки (держави). На сьогодні вже йдеться про шосте покоління мобільного зв’язку – 6 G, завдяки його появі суттєво розширяться можливості його використання, а також реалізуються

програми, що націлені на цифровізацію суспільства (порівняння стандартів мобільного зв’язку 4 G, 5 G, 6 G наведено на рис. 1.11)

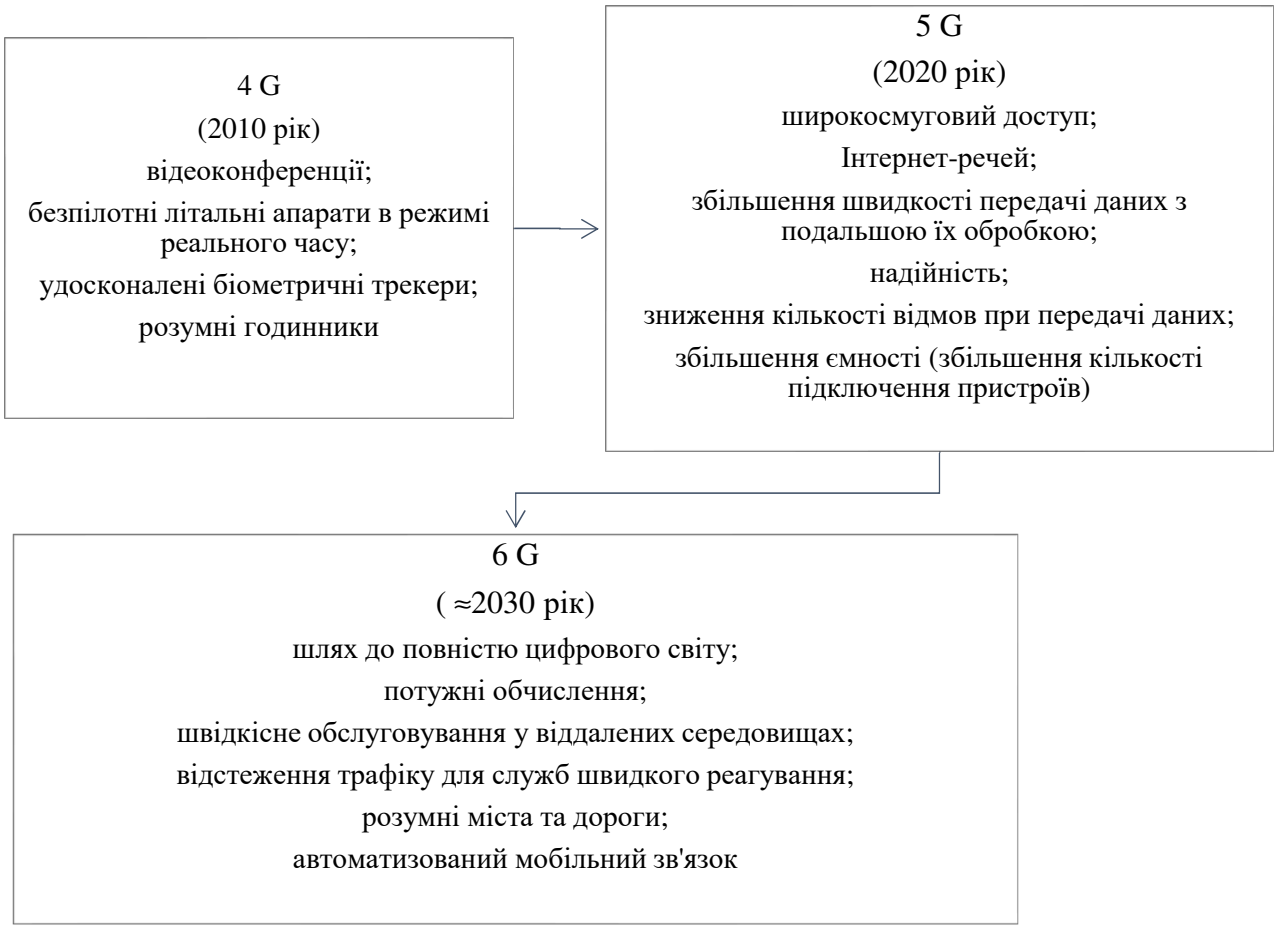


Рис. 1.11. Генеза поколінь стандартів мобільного зв’язку

(складено автором за даними [20])

Зрозуміло, що стандарти 5 G розширюють можливості підприємств, що їх використовують, оскільки підвищується надійність зв’язку, а отже й стабільність передачі даних, зменшується кількість відмов при передачі даних, збільшується кількість підключень гаджетів.

Поява та використання нового стандарту Generation 6 (G 6) дозволить реалізувати цифровізацію у всіх сферах, автоматизувати зв’язок та створити розумні міста.

Нові стандарти наближують суспільство до цифровізації світу, використання їх дозволить підприємствах посилити економічну безпеку у

частині обробки інформації, а отже й інформаційної складової за рахунок саме інноваційних технологій.

Сьогодення потребує перелаштування на віддалений доступ, який став основною вимогою для підприємств незалежно від виду діяльності, який ним провадиться, його розмірів. Здатність підприємства миттєво, безпечно та повною мірою перейти до моделі "робота з будь-якого місця" визначатиме, як господарюючий суб'єкт переживе невизначені умови, які переводять суспільство у режим віддаленої, а підприємства до онлайн роботи.

Саме тому, сучасний цифровий бізнес сьогодні змінюється та адаптується до нових умов і потребує нового підходу щодо віддаленого доступу: деталізованої безпеки; глобальної масштабованості; оптимізованої продуктивності. Змінюються технології забезпечення віддаленого доступу в Інтернет, так технологію VPN замінює Zero Trust Network Access – мережевий доступ з нульовою довірою, який забезпечує надання безпечного доступу до сучасного бізнесу. За надання через хмарну службу SDP усуває обмеження масштабованості VPN й миттєво забезпечує збільшення віддаленого доступу без необхідності додаткового обладнання або програмного забезпечення. SDP також забезпечує підвищену безпеку, оскільки забезпечує детальний контроль доступу на рівні додатків, а також можливості моніторингу.

Отже, прослідковуються зміни у бік діджиталізації та цифровізації світу, тому варто врахувати посилення ролі та значення інфокомунікацій та електронних комунікацій у функціонуванні економічних одиниць будь-якої сфери, тому стає доречним розгляд їх у розрізі економічної безпеки підприємств, зокрема її складових [85].

Особливості формування системи економічної безпеки та її складові розглядала Шевченко І., вважаючи доцільність представлення складових узагальнено або ж у деталізованому вигляді в залежності від умов функціонування підприємства. Загальні складові системи безпеки вбачалися в: управлінні (діяльність підприємства), безпеці ресурсів (людських, матеріальних та всіх наявних), ринковій безпеці (рейдерство, конкуренти), інформаційній

безпеці (конфіденційність) [90, с.180], проте, з науково-технічним прогресом відбувалися зміни у переліку складових.

Серед множини поглядів на структурно-функціональні складові елементів економічної безпеки підприємства, Васильців Т.Г., Волошин В.І, Бойкевич О.Р., Каркавчук В.В. виділяють: фінансову, продуктову, логістичну, інтелектуально-кадрову, силову, ресурсну, техніко-технологічну, інформаційну, політико-правову, екологічну, суспільно-політичну, соціальну, ринкову, інтерфейсну складові, охоплюючи функціональні елементи діяльності підприємства, більшість їх них торкаються вивчення зовнішнього оточення та загроз [92].

Зубко Т.Л. виокремила функціональні складові безпеки виробничо-торговельного підприємства з урахуванням його особливостей [28, с.72]:

– безпека операційної діяльності (ринкова та техніко-технологічна);

– безпека фінансової діяльності;

– безпека інвестиційної діяльності;

– безпека інноваційної діяльності;

– інтелектуально-кадрова безпека.

Інноваційна складова є найвагомішою для високотехнологічних підприємств, так інноваційні ресурси, інноваційні компетенції та інноваційні здібності) суттєво покращують можливості інноваційної діяльності підприємств, підвищують їх конкурентоспроможність [110].

Для більш чіткого розуміння забезпечення безпеки на підприємстві Штамбург Н.В. представлено її складові в сукупності корпоративних ресурсів: капітал, інформація, технології, персонал, техніка, устаткування, права [111], однак представлено завузько, навіть із точки зору відсутності повного переліку ресурсів, задіяних підприємством для виконання своєї операційної діяльності.

Потребу у чіткому визначенні системи забезпечення безпеки вбачає Живко З.Б. [113, с. 154-155] та наголошує на обов’язковості поділу її на складові: науково-методичну, практичну та організаційно-економічну.

Узагальнено основні функціональні складові безпеки підприємства Швиданенко Г.О. [32, с.33-38]:

– фінансова складова: досягнення найефективнішого використання корпоративних ресурсів;

– інформаційна складова: ефективне інформаційно-аналітичне забезпечення господарської діяльності підприємства; захист інформації;

– фізична (силова) складова: забезпечення фізичної безпеки працівників фірми (передовсім керівників) і збереження її майна;

– інтелектуальна та кадрова складові: збереження та розвиток інтелектуального потенціалу підприємства; ефективне управління персоналом;

– політико-правова складова: всебічне правове забезпечення діяльності підприємства, дотримання чинного законодавства

– техніко-технологічна складова: відповідність застосовуваних на підприємстві техніки та технологій сучасним світовим аналогам щодо оптимальних витрат ресурсів;

– ринкова складова: відповідність внутрішніх можливостей розвитку підприємства зовнішнім, які генеруються ринковим середовищем;

– зовнішньоекономічна складова: забезпечення безпеки зовнішньо-економічної діяльності підприємства;

– екологічна складова: дотримання чинних екологічних норм, мінімізація втрат від забруднення довкілля.

Через глобальні проблеми людства концентрується увага навколо екологічних питань безпеки: усунення шкідливого впливу виробництва на суспільство та навколишнє середовище, точаться питання щодо екологічної відповідальності та зменшення шкідливих викидів, раціонального використання ресурсів, корисних копалин. Розробляються проєкти та екологічні ініціативи в напрямку сталого розвитку, вбачаючи у цьому вирішення глобальних проблем людства. Звісно, що підприємства не залишаються осторонь, обговорюється потреба переходу не окремо

підприємств, а й в цілому галузей на альтернативні джерела енергії, здійснюється пошук можливих варіантів модернізації виробничих процесів, свідченням цього є розроблена Європейською комісією дорожня карта плану заходів скорочення викидів парникових газів у 2050 році на 80%, що відповідає рівню викидів вуглецю 1990 року [91].

Безперечно, що екологічна складова, як складова корпоративної соціальної відповідальності, враховуватиметься у забезпеченні безпеки підприємства, що дозволить уникнути репутаційних (питання соціальної відповідальності відображається на репутації компаній у разі втрати довіри стейкхолдерів), фінансових (податкове навантаження зростає через недотримання норм щодо шкідливих викидів, можливі штрафні санкції) ризиків [331]. Працюючи на упередження, навіть якщо законодавчо не регулюються питання відповідальності заподіяння шкоди виробництвом навколишньому середовищу, при побудові системи управління безпекою підприємствам доцільно включати екологічну складову.

Вивченню складових економічної безпеки підприємства присвячені наукові праці вчених: Ю. Работіна, В. Вороніної, Т. Меліхової , Б. Буркинського та В. Грищенко, С. Ілляшенко, Е. Данілової, С. Покропивного, В. Геєця [6; 7; 8; 9; 10; 11; 12; 13; 18].

Базовими складовими економічної безпеки підприємства вважаються, на думку науковців:

– фінансова, яка вбачається у забезпеченні безпечного руху коштів, а також стійкого фінансового стану;

– техніко-технологічна, що окреслює умови безпеки к використання матеріальної та технічної бази;

– виробнича – включає забезпечення виконання функцій операційної діяльності;

– енергетична – передбачає заходи для максимальної економії енергоносіїв;

– політико-правова – врахування всіх норм, правил, законів та положень, що регулюють діяльність сфери, в якій функціонує підприємство;

– ринкова – відповідність умовам ринку, конкурентоспроможність продукції та її якість відповідно до вимог ринку;

– інтелектуальна та кадрова, яка відповідає за безпечні умови роботи персоналу, захист їх прав та правомірне використання їх інтелектуального потенціалу;

– інтерфейсна, яка характеризується надійністю взаємодії з економічними контрагентами (споживачами, конкурентами, постачальниками, кредиторами, посередниками).;

– інформаційна – у системі захисту комерційної таємниці, збереженні цілісності та достовірності даних;

– фізична (силова) представляє собою фізичний захист як приміщень, так і персоналу та інформації, а також матеріальних об’єктів підприємства;

– екологічна – через політику захисту навколишнього середовища.

Вивчаючи питання складових безпеки підприємства (замінивши їх на складники, вважаючи більш прийнятним та правильним до використання, оскільки ближче до українського “склад”), Дуб Б.С. основні функціональні складники представлено наступним чином [11, с. 14]:

– політико-правовий;

– фінансовий (в свою чергу, поділяється на грошово-кредитний, бюджетний, податковий, борговий, банківський, валютний, емісійний, інвестиційний, біржовий/фондовий, страховий, зовнішньоекономічний/ міжнародний);

– інформаційний (захист конфіденційної інформації, комерційної таємниці);

– кадровий (в т.ч. інтелектуальний, соціальний);

– ринковий (захищеність збутової діяльності, забезпечення конкурентоспроможності продукції та успішної позиції на ринку);

– фізичний (силовий/пожежний/майновий);

– виробничий/ операційний (до якого належать ресурсний, техніко-технологічний, екологічний, енергетичний);

– інтерфейсний (безпека взаємодії з контрагентами).

Функціональні складові економічної безпеки підприємства досліджуються Кузьомко В.М., відштовхуючись від чотирьох концептуальних підходів їх стуруктуризації:

– перший підхід виокремлює функціональні складові або ж напрями безпеки;
– другий підхід розглядає об’єкти безпеки;
– третій підіхід розділяє процес забезпечення безпеки на потребу захисту ресурсів та функцій, які потрібно для цього виконувати;
– четвертий підхід полягає у розподілі складових на внутрішньовиробничі та позавиробничі.

Автором запропоновано наступні складові безпеки підприємства: техніко-технологічна, ринкова, зовнішньоекономічна, інтелектуальна і кадрова, інформаційна, фізична (силова), політико-правова, екологічна і фінансова безпека [200, с. 211].

Марченко О.С. виокремлено п’ять груп складових безпеки, а саме за [185, с. 77]:

1) видами господарської діяльності та функціями підприємства: підсистеми виробничої (операційної); логістичної, фінансової; ринкової; техніко-технологічної; інвестиційної, інноваційної; правової; інформаційно-комунікаційної; енергетичної; інтелектуально-кадрової; екологічної; соціальної; інтерфейсної; фізичної (силової) безпеки та кібербезпеки;

2) джерелами загроз: підсистеми внутрішньої (загрози внутрішнього середовища підприємства) та зовнішньої безпеки (загрози зовнішнього середовища підприємства);

3) об’єктами: підсистеми безпеки персоналу, майнової безпеки, безпеки інтелектуальної власності, ноу-хау, безпеки фінансових фондів (цільових та нецільових) та грошових потоків, безпеки бази знань та інформації, клієнтської бази;

4) складовими економічного потенціалу підприємства: підсистеми забезпечення безпеки виробничого, кадрового, техніко-технологічного, управлінського, ринкового та інших видів потенціалу підприємства;

5) періодами життєвого циклу підприємства: підсистеми убезпечення підприємства від криз; безпеки у період стабільного стану підприємства; безпеки розвитку; безпеки у період змін та трансформацій.

Такий підхід є безперечно правильним, але з урахуванням плину часу та невизначених умов, що виникають впродовж останніх трьох років потребує розширення переліку складових, зважаючи на посилення ролі електронних послуг, цифровізації економіки та діджиталізації суспільства в період пандемії та воєнного стану в країні. У напрямку розгляду даного питання – важливості послуг сфери електронних комунікацій у функціонуванні та безпеці підприємств, проведено низку досліджень вченими: О. Гудзь, Л. Худолій, С. Легоміновою, В. Сотниченком, О. Сосновською, В. Пильновою [14; 15; 16; 17]. Зокрема, О. Сосновською [15] підкреслюється динамічний розвиток електронно-комунікаційної сфери серед галузей світової економіки, а також суттєвий вплив на функціонування підприємств, соціально-економічний розвиток регіонів. Тому науковицею пропонується інноваційно-інформаційна складова економічної безпеки, що є цілком доцільно до розгляду в умовах цифровізації суспільства.

Із причин невизначеності умов (особливо з часів поширення Covid-19) безпека у інформаційному та інфокомунікаційному просторі набуває особливої значимості, світовими організаціями проводяться дослідження та наводяться статистичні дані безпечності роботи у глобальній мережі [201; 202]. Світовим банком проводився аналіз у розрізі країн світу щодо безпечності інтернет-серверів, найбільш безпечними вважаються сервери Сполучених Штатів

Америки – 46678110 серверів на 1 млн осіб, потім – Німеччини 8109646 серверів на 1 млн осіб й Великої Британії – 2445275 серверів на 1 млн осіб. Щодо України, то показник відчутно нижчий – 395092 сервери на 1 млн осіб (рис. 1.12).

Зрозуміло, що розвиток техніки та технологій, інфокомунікацій, поширення Інтернет у досліджуваних країнах відбувався швидшими темпами. Крім того, з появою глобальної мережі та інтернет-технологій у досліджуваних країнах (що займають лідируючи позиції захисту серверів) з'являлися послуги, що надавалися за їх використання, тому й питання захисту та безпеки в інфокомунікаційному просторі ставилися одночасно із їх наданням. Саме тому рівень захисту та безпеки у даних країнах в цифровому просторі вище. Україна тяжіє до вирішення питань захисту та безпеки, імплементує нові закони та положення, нормативно-правові акти, світові стандарти, які убезпечують роботу підприємств у інфокомунікаційному просторі.

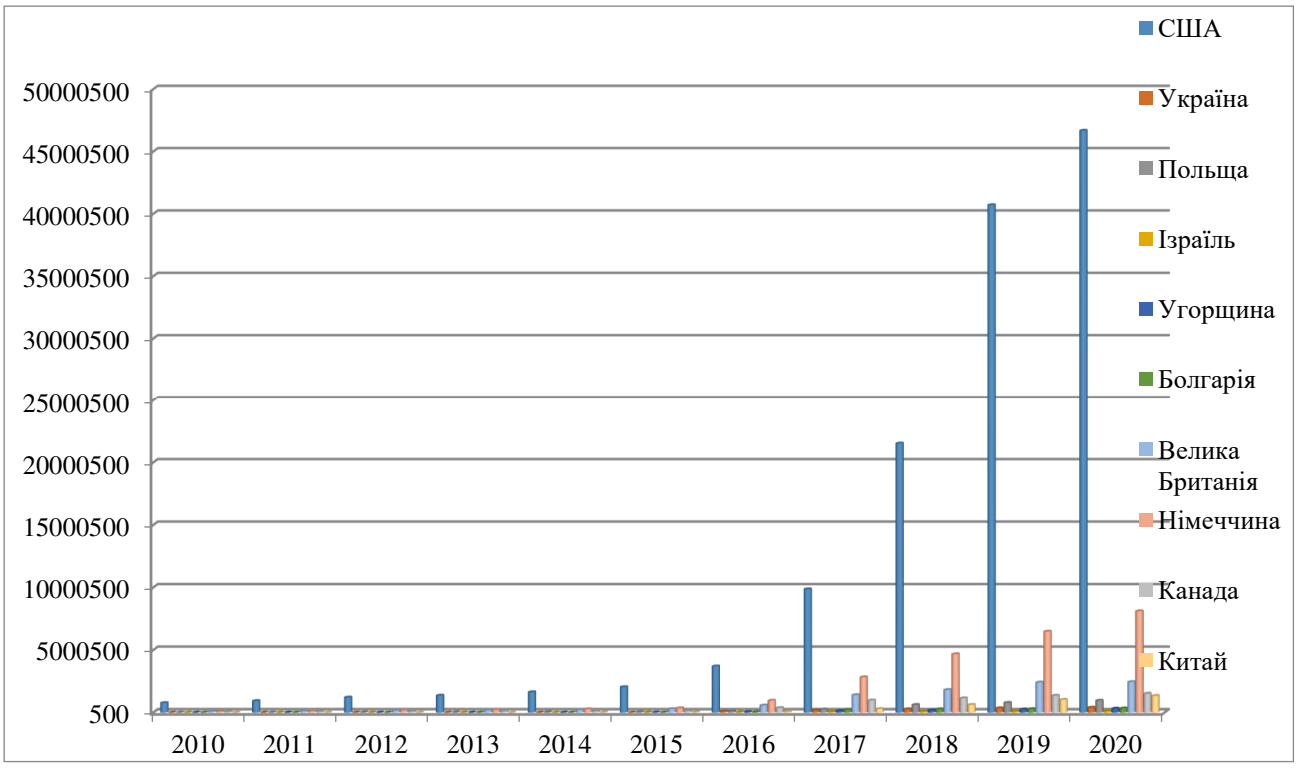


Рис. 1.12. Динаміка показників безпечності інтернет-серверів (на 1 млн осіб) за країнами світу впродовж 2010-2020 рр.

(складено автором за [19])

Стали доступними мережі 4G, імплементуються акти Європейського Союзу, щодо управлінням радіочастотного спектра. Наприкінці 2019 року Європейський Союз офіційно розпочав в Україні нову програму “EU4Digital: підтримка цифрової економіки та суспільства у Східному партнерстві”. Дана програма передбачає розширити переваги Єдиного цифрового ринку Європейського Союзу для України та інших держав Східного партнерства з метою стимулювання економічного росту, створення робочих місць, покращення життя людей та допомоги бізнесу.

Тому в Україні на законодавчому рівні зазнають змін правила, що регулюють діяльність у сфері ЕК. Так, втратив чинність ЗУ “Про телекомунікації” (якому передував ЗУ “Про зв’язок”), замість нього у 2022 році введено в дію Закон України “Про електронні комунікації” [1], зміна якого пояснюється динамічним розвитком сфери та важливістю регулювання підприємств, що функціонують у ЕК сфері у відповідності до нових умов та світових вимог до підприємств зв’язку та послуг, що ними надаються.

Даним законом “електронна комунікація” визначається як: передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій; а “електронна комунікаційна послуга” – як послуга, що полягає в прийманні та/або передачі інформації через електронні комунікаційні мереж і, крім послуг з редакційним контролем змісту інформації, що передається за допомогою електронних комунікаційних мереж і послуг. Сутність даних категорій та їх смислове значення, дозволяє прийти до висновку, що на сьогодні будь-яке підприємство, враховуючи умови невизначеності (що спричиняються загрозами, на які безпосередньо вплинути не може, а може лише адаптуватися), продовжує функціонувати лише за використання електронних комунікації. Саме тому, крім перерахованих вище складових (фінансової, техніко-технологічної, виробничої, енергетичної, ринкової, інтелектуальної, кадрової, інтерфейсної, інформаційної, фізичної (силової), політико-правової, екологічної, інформаційно-інноваційної) доцільно ввести електронно-

комунікаційну (рис. 1.13). У свою чергу включення даної складової до базових дозволить суттєво посилити економічну безпеку підприємств, оскільки дозволить розширити врахування ризиків з метою подальшого вивчення та уникнення переходу їх у загрози економічній безпеці підприємства. Особливо відчутна важливість електронних комунікацій для підприємств в умовах воєнного стану, оскільки деяким підприємствам довелося змінити формат провадження своєї діяльності й своє територіальне місцерозташування. Слід розуміти, що введена складова дозволить покращити процес оцінки економічної безпеки та визначати її рівень.

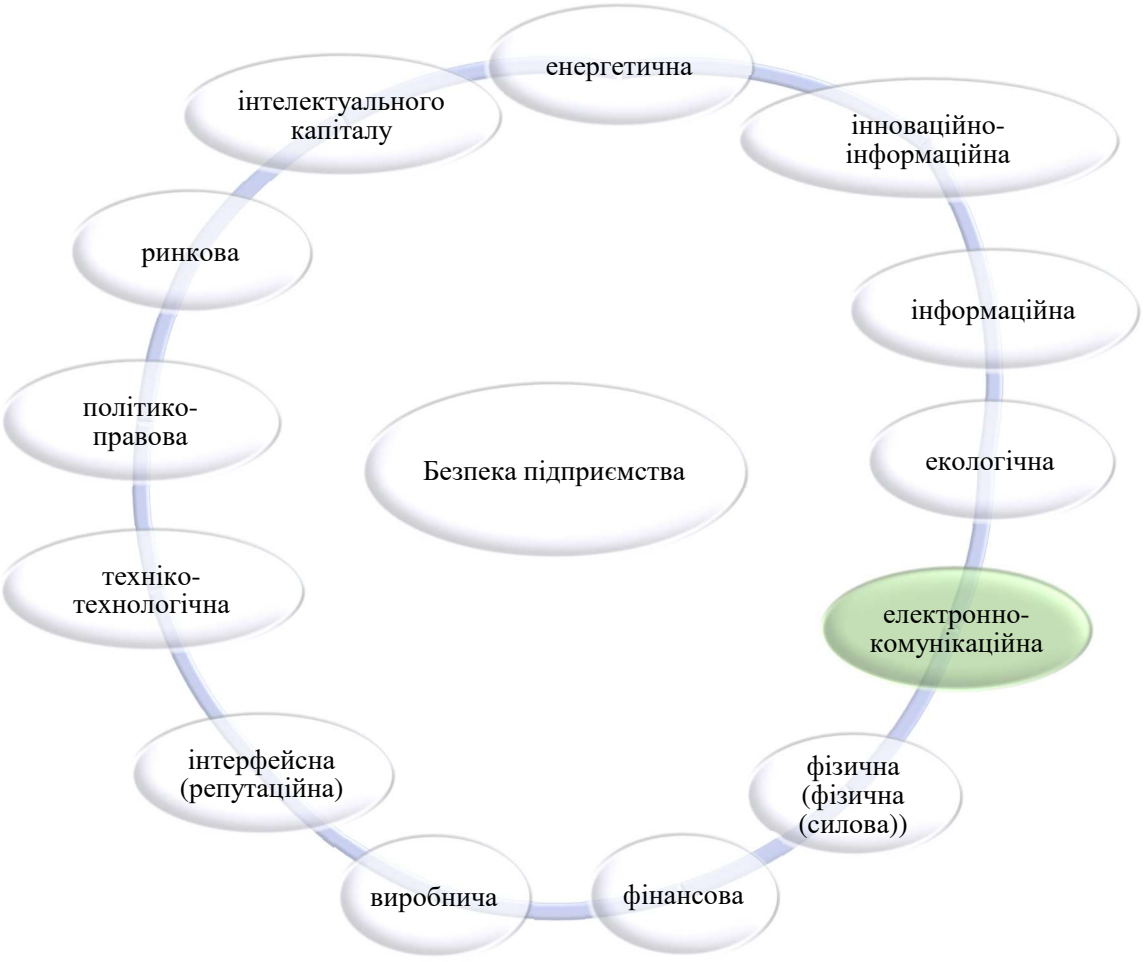


Рис. 1.13. Складові безпеки підприємства з урахуванням посилення ролі електронних послуг (авторське доповнення)

(узагальнено та складено автором на основі [7-13; 15])

Розширення складових (з урахуванням умов невизначеності та потреби здійснювати левову частку роботи віддалено) дозволить якісніше та повною мірою охопити можливі ризики, виклики та загрози, оцінити показники рівнів впливу кожної із складових, визначити вагомість окремої складової економічної безпеки здійснити та провести оцінку економічної безпеки.

Отже, аналіз і оцінювання рівнів складових економічної безпеки є основою для розроблення комплексу заходів протидії загрозам та підвищення рівня економічної безпеки підприємства і, відповідно, розширення його адаптаційних можливостей до змін умов господарської діяльності, створення умов стабільного функціонування і розвитку.

Крім того, доцільність перегляду складових економічної безпеки підприємства з урахуванням мінливості середовища, умов функціонування та невизначеностей має сенс через те, що її рівень визначається у послідовності: оцінювання кожної складової економічної безпеки підприємства, що досліджується; визначення вагомості кожної складової економічної безпеки досліджуваного підприємства.

Отже, визначення рівня безпеки підприємства розпочинається саме з оцінки складових економічної безпеки, тобто не врахувавши або обравши їх неправильно унеможливлюється достовірність та правильність визначення рівня економічної безпеки для досліджуваного підприємства. Саме за рахунок постійного моніторингу змін, що виникають під дією зовнішнього оточення та чинників впливу, вдасться більш досконало проводити аналіз та оцінку складових економічної безпеки, ранжувати їх за ступенем сили дії з подальшою розробкою алгоритму виявлення ризиків, що можуть перейти у виклики та спричинити загрозу економічній безпеці підприємства. Далі розробити комплекс заходів щодо нейтралізації виявлених загроз та адаптувати до несприятливих умов, забезпечити стабільне, безпечне функціонування підприємства та сприяти його розвитку, розкриттю потенційних можливостей. Пропозиція доповнення складової безпеки – електронно-комунікаційною, дозволить в теперішніх невизначених умовах удосконалити оцінювання

економічної безпеки підприємства та враховувати результати оцінки при розробці заходів, інструментів, механізмів управління економічною безпекою підприємства [85].

Висновки до першого розділу

Досліджено поняття “безпека”, яка нині значиться як ключовий орієнтир у формуванні політик та програм розвитку через геополітичні напруження, посилення та взаємозалежність економік на міжнародному рівні, при чому вважається важливим забезпечення безпеки, починаючи із рівня індивіда, підприємства та рухаючись по вертикалі у бік глобальної, оскільки закладається її розуміння з перших рівнів й неможливо її гарантувати на світовому щаблі без забепечення на мікрорівнях. Відзначено, що наразі під загрозою знаходиться національна безпека, що у свою чергу призводить до порушення безпеки на усіх рівнях, що нині чітко прослідковується, тому важлим є вирішення питання безпеки на всіх рівнях із урахуванням масштабів її порушення та впливу на індивідів та суб’єктів господарювання.

Етимологічний аналіз поняття “безпеки” дозволив дійти висновку, що безпека є керованою, оскільки окрім розуміння її як: відсутності небезпек, впевненості, захисту, спокою, містяться згадки про володіння ситуаціїю, що дозволяє зробити припущення, що досягти безпеки можна за рахунок управління. Відзначено, що термінологічний базис розуміння безпеки підприємства нашаровується із часом відповідно до нових умов функціонування, науково-техніного прогресу, проте її суть залишається незмінною, передбачає перебування підприємства у стані захищеності від небезпек.

У результаті критичного аналізу напрацювань щодо питань безпеки підприємства, розгляду її етимології надано визначення безпеки підприємства як стану стійкого функціонування й потенціальної спроможності його розвитку за умови відсутності небезпек (викликів, ризиків, загроз), а у разі їх появи – захищеності, що гарантує досягнення цільових безпекових результатів

діяльності. Безпека підприємства окреслюється сукупністю елементів, серед яких визначають суб'єкти, об'єкти, виклики, ризики, загрози, оточення та його впливи, виявлено, що на безпеку підприємства чинять вплив об'єкто негативні впливи, що йдуть усупереч інтересам підприємства, виникають самі по собі без участі керівництва та персоналу. Також значаться суб'єктивні негативні впливи на безпеку підприємства, що є результатом неправильного та неефективного керування, з'являються через помилки або некомпетентність керівництва, персоналу. Прослідковується чіткий зв'язок безпеки із стейкхолдерами, якими приймається рішення щодо розвитку, функціонування підпримства.

У результаті дослідження понять "небезпека" та "безпека" вдалося з'ясувати, що вони віддзеркалюють один одного, але не передбачають перебування на одному відрізку, вони рухають стан безпеки підприємства у площині. За теорією прибутку та теорією ризику відзначається їх зв'язок із безпекою підприємства, за визначеннями поняття "безпеки підприємства", та розглянутими теоріями фірм виокремлено маркери безпеки, що в сукупності дозволило сформувати площину елементів управління безпекою, що окреслюється ознаками, за якими сформовано концепт цільових безпекових орієнтирів підприємства: прибутковість та рентабельність, конкурентспроможність, платоспроможність, конкурентоспроможність, розвиток та інтереси стейкхолдерів, що постійно перебувають під дією ризиків та загроз, викликів.

Зважаючи на потребу вимірності цільових безпекових орієнтирів, проаналізовано складові, які її формують та відзначено загальноприйняті (фінансова, техніко-технологічна, виробнича, енергетична, ринкова, кадрова, інтерфейсна (репутаційна), інформаційна, фізична (фізична (силова)), політико-правова, екологічна, інвестиційно-інноваційна) та запропоновано додати електронно-комунікаційну складову безпеки у відповідь на посилення ролі електронних комунікаційних послуг в умовах активної цифровізації та зростанню кількості кібератак на підприємства зв'язку.

Основні ідеї та наукові положення, презентовані у даному розділі, викладені у піблікаціях та працях [23; 34; 85; 86; 103; 107; 108; 201; 202; 248; 315]

РОЗДІЛ 2
НАУКОВА ЕВОЛЮЦІЯ ПОГЛЯДІВ ЩОДО УПРАВЛІННЯ БЕЗПЕКОЮ ПІДПРИЄМСТВА

2.1. Ризики та загрози як рушії небезпеки в управлінні підприємством у визначеному та невизначеному середовищі

Останні декілька років світ стикається з новими викликами, які діють ізовні і на які підприємства, що функціонують в умовах невизначеності, не можуть впливати, тому господарюючим суб'єктам потрібно адаптуватися до таких змін та формувати, відповідні до вимог часу та умов, підходи до управління безпекою підприємства, методи оцінки, критерії оцінки безпеки, враховувати нові фактори впливу на безпеку підприємств. Лише за вчасного реагування на зовнішні виклики можна досягти безпеки у функціонуванні, створювати сприятливі умови з огинанням небезпек, що можуть потенційно виникнути.

Система управління безпекою підприємства в невизначених умовах, які наразі на собі відчувають всі господарюючі суб'єкти, організації, держава та суспільство, має трансформуватися з урахуванням загроз, ризиків, що викликані сьогоднішніми умовами. Інакше – система зазнає руйнівних змін, які призведуть до деструктивних змін на мікрорівні, а згодом – макрорівні.

Процес управління є складним і потребує деталізації при побудові системи управління безпекою з урахуванням усіх складових безпеки, об'єктів захисту та суб'єктів безпеки, інструментів, що можливі для застосування, поглибленим вивченням факторів впливу та оточення, методів управління безпекою з розмежуванням викликів, загроз та ризиків, які потенційно можливі, або ж наявні з подальшими методами оцінки для побудови ефективної системи управління ризиками підприємства.

Управління безпекою підприємств являє собою процес оцінки ризиків безпеки, з подальшим планування заходів щодо їх усунення, спрямованих на подолання викликів, що пов'язані з роботою в небезпечному, складному несприятливому середовищі, наразі – в невизначеному. У нинішніх умовах ризик можна визначити як ймовірність зіткнення із загрозою та потенційними наслідками зіткнення із загрозою [93].

Доцільним є створення спільних рамок для визначення ризиків, що загрожують підприємствам в окремих сферах з попередньо проведеним їх ранжуванням, щоб чітко визначитися з найбільш загрозливими, та виокремленням пріоритетних із них з подальшою розробкою плану стримування або ж прийняття, у разі неможливості його усунення. У свою чергу, таке виокремлення дозволить ранжовані ризики відносити до різних категорій та таких, які неможливо усунути, з метою оптимізації та економії часу для упередження їх дії за пріоритетністю.

Нині умови вимагають надшвидкої реакції на критичні інциденти небезпеки на підприємствах та миттєвого управління кризовими ситуаціями. За наявності плану антикризового планування при управлінні безпекою та завчасного його використання вдасться усунути виявлені ризики.

Враховуючи теперішні загрози, підприємства повинні переорієнтовуватися та використовувати підходи до управління ризиками та стійкістю до небезпек, щоб упереджувати дію невизначених умов на функціонуючі підприємства. Так як, дія зовнішніх ризиків надсильна, а вплив на них з боку функціонуючих підприємств може бути мінімальним, виникає потреба у спільній побудові структури визначення та оцінки ризиків не лишень підприємствами, але й урядами, зовнішніми стейкхолдерами, тоді можна розраховувати на довгострокову ефективну та безпечну роботу підприємств та організацій. Варто будувати систему управління ризиками, починаючи із визначення ризиків, з якими може зіткнутися підприємство з виділенням найбільш характерних для певної галузі та категоризації ризиків, спираючись на їх ознаки (товарні ризики, ринкові, і.т.д.). Після чого потрібно обрати

потенційні методи їх зниження, впровадити та тестувати методи їх усунення з подальшим оцінюванням придатності пропонованих методів (прийняття або відхилення), і останнє – контроль ефективності визначених категорійованих ризиків та застосовуваних методів їх зниження щодо доцільності використання з плином часу.

Систематизоване управління ризиками з використанням розроблених рамок визначення ризиків з їх ранжуванням за ступенем дестабілізації показників ефективності роботи підприємства, що функціонує в конкретній сфері, допоможе вчасно прийняти рішення про те, які із заходів є доцільними для забезпечення безпеки досліджуваного підприємства в сучасних умовах [86].

Загальновідомо, що підприємства створюються та функціонують для отримання прибутку через задоволення потреб споживачів, сама мета підприємства стає досяжною лише за умілого управління ним. Саме управління може розглядатися як процес, який має відбуватися безперервно, щоб підприємство динамічно розвивалося. Суб'єкти господарювання можуть його забезпечити у разі: ефективного обміну товаром (послугою) зі споживачем та оточенням на умовах справедливості (справедлива ціна (тариф) за наданий ресурс, товар, послугу) при правильному розподілі ресурсів; гідного відношення до персоналу, як людського ресурсу, що створює продукт, надає послугу; організації своєї діяльності відповідно до умов та оточення, пристосування до мінливих умов функціонування.

При управлінні безпекою підприємства, об'єктом управління виступає керована система, актив, який підлягає захисту, а суб'єктом виступатиме особа, яка керує, приймає рішення щодо об'єкту, на який негативно впливають чинники або діють умови невизначеності через брак знань щодо ймовірності настання певних подій. Звідси й бере початок складність управління безпекою, що охоплює площину небезпек, які виникають в результаті настання певних подій, які можуть бути, як визначеними, так і невизначеними.

У розділі 1, досліджено, що площина безпеки-небезпеки формується ще й ланцюгом "виклик-ризик-загроза", тобто доцільно визначати їх для того, щоб

точно формувати базу вихідних даних для ефективного управління, ухвалення рішень щодо безпеки підприємства та чітко скеровувати завдання щодо об'єкта захисту. Крім того, множинність складових має враховуватися та формуватися власний підхід щодо аналізу та оцінки чинників впливу, тобто джерел, що визначатимуть виклики, ризики, загрози, в залежності від ступеня настання певної події.

Існує теза, що саме власність пов'язана із ризиками, тобто все, чим володіє господарюючий суб'єкт на правах власності є об'єктами впливу ризиків. Саме тому, об'єктами захисту на підприємстві виступатиме персонал, майно, те, що належить йому на правах власності, та використовується для забезпечення його діяльності, на що спрямоване управління безпекою, до прикладу: види діяльності, майно, ресурси, інформація, персонал, комерційна таємниця, інтелектуальна власність, репутація, інтереси підприємства.

Видатний економіст М. Фрідмен вважав, що за чинник ризику має вводитись додаткова плата – компенсація, а вибір рішень в залежності від ризиків представив наступним чином [77, с. 288]:

– невеликий ризик (при прийнятті рішень відомий результат);
– помірний ризик (у разі невеликих доходів і витрат);
– великий ризик (у разі великих доходів і витрат).

Вбачаємо у такому розподілі потребу у поінформованості щодо результату, проте не завжди реально заздалегідь отримати інформацію, оскільки оточення функціонування підприємства мінливе, тому не є цілком визначеним.

Навпаки, нинішні умови, в яких функціонують підприємства, покликані невизначеністю оточення, тому особливо гостро потребують прийняття рішень щодо безпеки. Сама ж безпека буде динамічною через швидкоплинність подій, крім того, інформація змінюється саме з причин невизначеності, досягти повноти отриманих даних важко за браку часу.

Д. Канеманом та А. Тверскі (кінець 1970-х років) запропоновано теорію перспектив, за якою спростовано традиційне припущення раціональної поведінки щодо прийняття рішень в умовах ризиків із спробою наведення доказів на користь психологічного сприйняття проблеми втрат доходів, пояснюючи таку поведнку бажанням радше уникнути втрат, аніж отримати еквівалентні вигоди, оскільки втрата психоемоційно чинить сильніший вплив, аніж отримання виграшу. Суттєвим внеском для розуміння сутності поняття ризику є напрацювання Ф. Найта, яким запропоновано теорію фірм, за якою відзначається взаємозв'язок ризиків і прибутків. Науковець вважає, що саме за ризик при прийнятті рішень, суб'єкт господарювання отримує винагороду [106].

Відзначається роль підприємця, який ініціює появу ризику з початку зародження підприємницької ідеї, при чому ризик є вимірним, а невизначеність – невімірною [23].

У процесі управління, прийнятті рішень велику роль відіграватиме рівень поінформованості щодо стану проблеми безпеки. Вибір рішення може прийматися в умовах визначеності; в умовах ризику; в умовах невизначеності.

Визначеність характеризується достатньою інформованістю стосовно подій, відомий результат дії. Ризик передбачає прийняття рішення із множини варіантів, за попередньо відомою ймовірністю отриманого результату. В невизначених умовах є безліч варіантів щодо прийняття рішень внаслідок дії певних процесів, явищ, чинників з невідомою ймовірністю їх настання.

Під невизначеністю розуміємо неможливість отримання даних щодо об'єкту та вірогідності появи негативного результату через події, що відбуваються, тобто їх відсутність для аналізу та попередніх припущень щодо наслідків

Управління потребує досконалого розгляду питань, що торкаються не тільки самих об'єктів та суб'єктів, джерел-першопричин виникнення негативних подій, а й середовища, умов, в яких функціонують господарюючі суб'єкти.

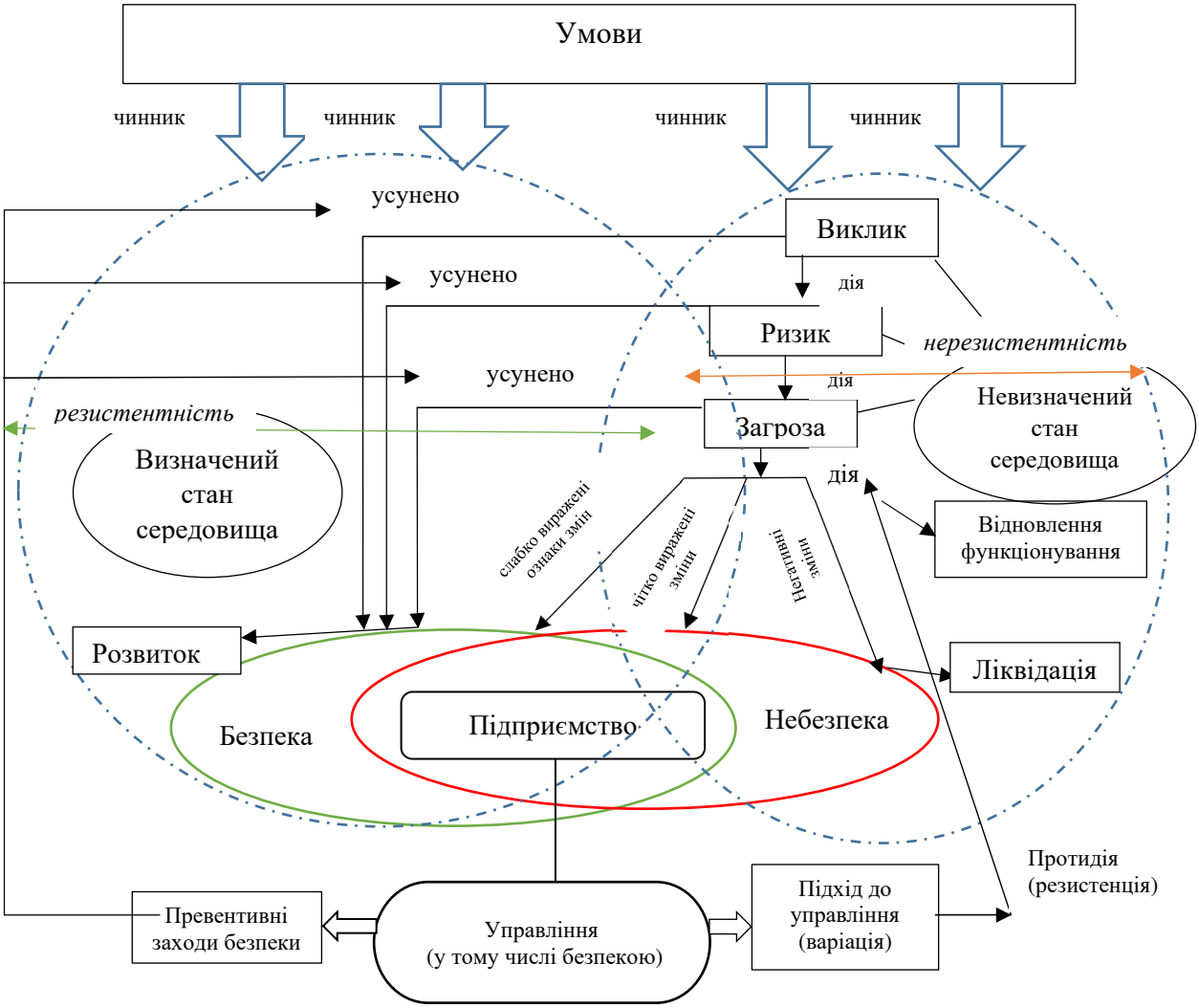


Рис. 2.1. Фрагментація виразності розгалуження ризиків та загроз у безпековій площині за визначеного та невизначеного середовища підприємства *(авторська розробка)*

Під час свого функціонування підприємство знаходиться на межі безпеки й небезпеки через низку умов, що сформувалися навколо нього, чинників, що дію, визначеного та невизначеного стану оточення, інформованості щодо явищ та подій, що відбуваються в середовищі господарювання. Управління підприємством (у тому числі безпекою) у визначеному та невизначеному середовищі підприємства (рис. 2.1) дозволяє скерувати дотичністю їх співіснування.

Визначені умови для підприємства є сприятливими для функціонування підприємства, поінформованість щодо умов функціонування дозволяє швидко

реагувати на зовнішнє мінливе середовище, влив чинників, адаптуватися до змін та перебувати в безпеці. Як нами з'ясовано, на підприємство діють виклики, ризики, загрози, за успішного їх усунення та визначених умов підприємство знаходиться у безпеці.

Важливими категоріями при управлінні ризиками є ризикостійкість підприємства. Стійкість є здатністю до відновлення функціонування підприємства та адаптування до змін, тоді ризикостійкість – спроможність підприємства чинити опір чинникам, явищам, подіям без суттєвих втрат та відхилень від запланованих результатів, так завана "толерантність" до ризику.

Доцільно ввести поняття резистентності, яким описуватиметься протидія ризикам та загрозам, невизначеностям, викликам в оточенні підприємства ("resistência" походить від португальського, означає: здатність витримувати, протидія, стійкість, опір [203]).

Резистентність (стійкість, несприйняття, здатність чинити опір) підприємства знижується у міру невизначеності середовища. У разі динамічності оточення, неспроможності протидіяти викликам, ініціюється процес переходу викликів у зону ризиків. За неспроможності підприємством усувати ризики резистентність знижується, гіпотетичний ризик переходить у реальні загрози, які безпосередньо чинять деструктивний вплив на результати діяльності підприємства. Відбуваються зміни негативного характеру, що наражають підприємство на небезпеку, можуть призвести до його ліквідації, актуалізується питання безпекозабезпечувальної діяльності підприємства. Розглядаються всі можливі заходи безпеки із захисту активів задля протидії негативним змінам та повернення спроможності підприємством провадити свою операційну діяльність, відновлення його функціонування. При чому не важливо, які зміни відбуваються на підприємстві – слабко виражені, чітко виражені або негативні, з боку підприємства протидія має бути зчинена щодо всіх існуючих змін. Досягти результату щодо ефективного спрацювання захисних заходів реально за рахунок ефективного управління безпекою на підприємстві і за визначеного, і за не визначеного середовища. За певних умов,

чинників, начебто слабкі виклики, можуть призвести до появи ризиків та загроз, тому за визначеного та спокійного функціонування, підприємством має бути розроблена низка превентивних заходів для вчасного реагування, управління безпекою.

Підприємства природньо зазнають ризиків, починаючи із зародження підприємницької ідеї, оскільки вже на цьому етапі з'являються виклики, що пов'язані із реакцією на пропонований товар – сприйняття його ринком або відторгнення, господарюючі суб'єкти стикаються із низкою ризиків, які варто розглянути більш детально для того, щоб розуміти їх суть та нейтралізувати перехід у загрози.

Чітке окреслення викликів, ризиків та загроз, розуміння їх природи, класифікація та характеристика дозволять реагувати на них правильно, розробляти як оперативні, так і превентивні заходи захисту, управляти безпекою предметно.

Виклики описуються на конкретний момент дослідження об'єкта безпеки, пов'язані із зовнішнім оточенням, змінами, що покликані політичною, ситуацією, податкової політикою, економікою, нормативно-правовим регулюванням, екологічними налаштуваннями, міжнародною політикою. Посилюються за рахунок оточення, точніше його визначеності або невизначеності. Для них є характерними обриси ризиків, оскільки є передумовою їх появи. Тому більш детально розглянемо ризики, їх види, специфічність для галузей, бо саме ризики за неналежного ставлення до їх вивчення, моніторингу, аналізу та оцінки можуть призвести до переходу їх у загрози для безпеки підприємства.

Безумовно підприємницька діяльність пов'язана із ризиком, про що йшлося у розділі 1 (із існуючих теорій прибутку – дві пов'язані із ризиками) і підтверджується думкою Кляйнвехтера, що при організації виробничого процесу підприємці подвійно ризикують, отримуючи технічний та економічний ризики, автор підкреслює, що за ризики підприємці отримують плату – прибуток [106, с.220].

Таке розуміння взаємозв'язку між ризиком та прибутком, того, що дохід є премією за прийняття ризику є фактом, доволі значущим у безпекозабезпеченні. Будь-яка діяльність, особливо підприємницька, наражається на ризики, які різняться характером походження, часом, впливом зовнішніх та внутрішніх чинників, що впливають на його рівень, та, відповідно, на їх аналіз, оцінку, методику їх дослідження.

За спільними ознаки та критеріями ризики можна згрупувати, що дозволяє систематизувати, класифікувати їх для більш точного вивчення, аналізу, оцінки.

Існує множина класифікацій ризиків в залежності від сфери діяльності підприємства та галузевої приналежності, наприклад ризики на ринку цінних паперів, ризики на ринку нерухомості, ризики на страховому ринку, ризики на транспорті, ризики на ринку ЕК.

Класифікація ризиків дозволяє визначати ризики, відслідковувати природу їх походження, комплексно проводити ідентифікацію з урахуванням загальних та специфічних умов їх появи, обирати механізми та засоби боротьби із ними, а також використовуватися при управління безпекою для підвищення ефективності забезпечення безпеки підприємства.

Узагальнено ризики класифікують за часом їх появи, чинниками виникнення, характером наслідків їх впливу.

Класифікація ризиків на основі ключових чинників макросередовища, використовується при проведенні PESTLE аналізу [80; 83], який складається із врахування: соціальних (S – social), технологічних (T – technological), економічних (E – economic), політичних (P – political), юридичних (L –Legal), екологічних або екологічних (E – ethical or environmental) чинників зовнішнього середовища.

Політичні чинники включають: податки, трудове законодавство, екологічні правила, торговельні обмеження, реформи, тарифи та політичну стабільність.

Економічні чинники: економічний ріст або зниження, процентні ставки, обмінні курси валют, рівень інфляції, ставки заробітної плати, тривалість робочого часу, безробіття (локально й національний), вартість життя, кредити.

Соціологічні чинники: культурні особливості та очікування, стан здоров'я, темпи росту населення, розподіл за віковими групами, кар'єрній можливості, безпеку, глобальне потепління.

Технологічні чинники: зміни щодо продукції, інноваційні аспекти послуг, нові технології, бар'єри для входу у ринок, фінансові рішення (аутсорсинг), ланцюг поставок.

Юридичні чинники: зміни законодавства, які впливають на зайнятість, доступ до матеріалів, квоти, ресурси, експорт та імпорт, система оподаткування, стандарти безпеки.

Етичні або екологічні чинники: пов'язані із етичними нормами та екологічними аспектами (клімат, географічне розташування, ґрунти, забруднення, водні ресурси), переробка, відходи, в більшості випадків мають економічний або соціальний характер.

За часовими інтервалами ризики бувають: короткострокові, дія є миттєвою на цілі; середньострокові (до 1 року), дія не є очевидною відразу, але проявиться впродовж декількох місяців або через рік; довгострокові (до 5 років), вплив на організацію через тривалий час після настання події, від 1 до 5 років.

Наслідки впливу ризиків оцінюються за трьома рівнями: високий ризик, помірний ризик, незначний.

Рівень оцінки ризику, як правило, узагальнюється та представляється у вигляді шкали (рис. 2.2), що дозволяє чітко визначати пріоритетність їх впливу на функціонування підприємства.

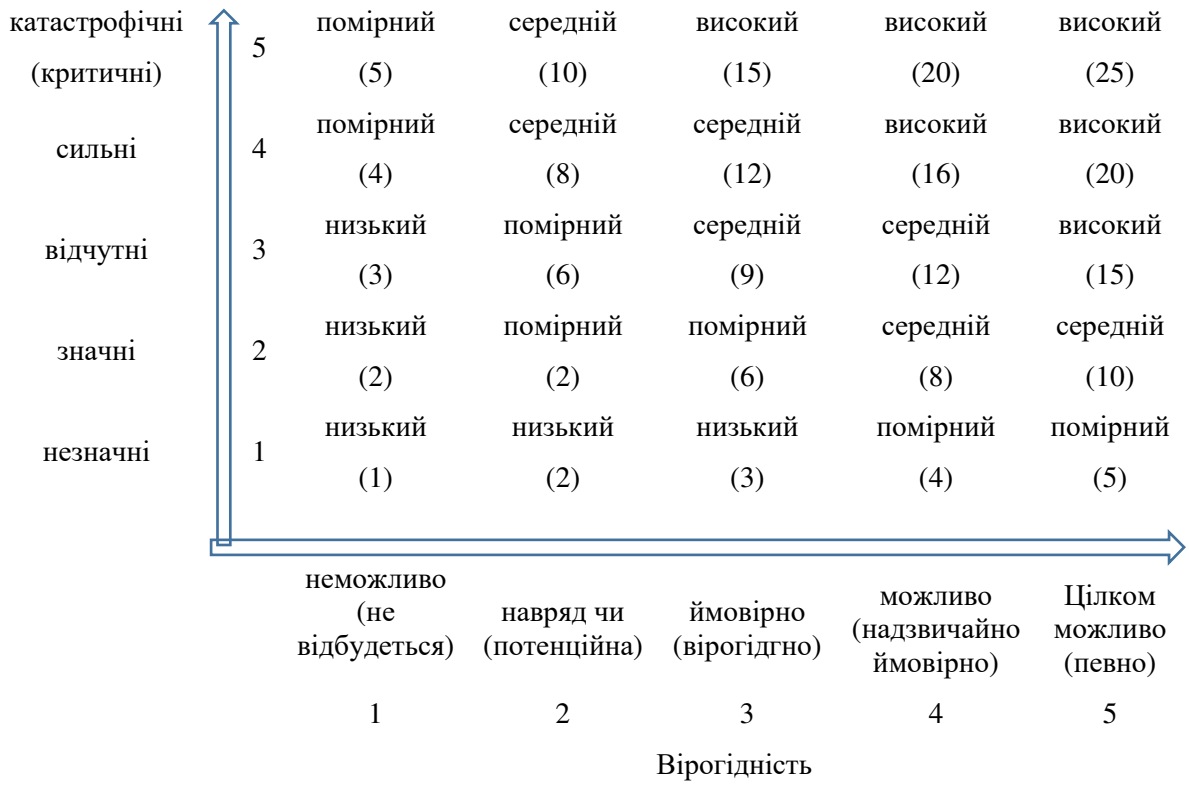


Рис. 2.2. Матриця рівнів оцінки ризиків

(складено автором за [82; 83; 84])

П’ятирівнева шкала будується від найменш ймовірнісного за ступенем дії чинника до найбільш ймовірнісного негативного впливу, а саме: чим вища ймовірність появи, тим більший негативний вплив та сильніший ризик. Шкали формують чарунки матриці оцінки ризиків, яка представлена у формі графічного звіту, починаючи із лівого кута з незнатними ризиками, рухаючись по діагоналі до більш значущих ризиків.

Аналіз допомагає оцінити та врахувати чинники, що діють на організацію для використання сильних сторін й укріплення позицій, а слабкі – для передбачення викликів та ризиків, їх упередження та пом’якшення. Метод управління, який вивчає впливи подій, чинників ззовні, що відображаються на ефективності компанії чи організації та полягає в: оцінці важливості дії ризиків для організації (наприклад, критична, велика, важлива, значна, помірна або незначна) з одночасною оцінкою ймовірності того, що це станеться (наприклад, певність, надзвичайно ймовірно, вірогідно, потенційно, віддалена можливість

або не відбудеться). Класифікацію ризиків та загроз досить детально представила у монографії Зубко Т.Л., якою надано власні доповнення до наявного їх переліку. Ризики класифіковано за наступними ознаками [28, с.35]: рівнем появи (мікрорівень (підприємства), галузевий, міжгалузевий, регіональний, державний, глобальний); причинами виникнення: суб'єктивний вплив; невизначеність майбутнього, недостатність інформації; сферою виникнення (законодавчі; соціально-політичні; природно-екологічні; адміністративно-фінансові; виробничі; демографічні; геополітичні); належністю до країни функціонування суб'єкта господарювання (внутрішні; зовнішні); ступенем системності (системні; несистемні (унікальні)); відповідністю допустимим межам (допустимі; критичні; катастрофічні); зв'язком із підприємницькою діяльністю (підприємницькі; непідприємницькі); ступінь обґрунтованості прийняття (обґрунтовані; частково обґрунтовані; авантюрні); реалізацією (реалізовані; нереалізовані); за частотою виникнення збитку (поодинокі; ризики середньої частоти виникнення; часті ризики); адекватність часу прийняття (опереджувальні; поточні; запізнілі); за ступенем поширеності (масові; унікальні); група, яка реалізує ризик та приймає рішення щодо поведінки у випадку його реалізації (індивідуального рішення;колективного рішення); за ступенем урахування часового чиннику (безстрокові (ризики, які не мають тимчасових обмежень)); термінові, серед яких виділяються довго- і короткострокові; стратегія фірми стосовно прийняття ризиків (від яких відмовляється; які залишає; які передає); час дії чиннику (короткотермінові; постійні; систематичні; періодичні); за характером наслідків (чисті та спекулятивні); масштаб впливу (одноосібні; колективні (багатоосібні)); можливість прогнозування (прогнозовані; частково непрогнозовані); ступінь впливу на діяльність (негативні; нульові; позитивні).

Зважаючи на багатоаспектність класифікаційних ознак ризиків, Коренюком П.І. загально представлено їх види [109]:

– масштаби та розміри ризику – глобальний, локальний;

– аспекти ризику – психологічний, соціальний, економічний, юридичний, політичний, медико-біологічний, комбінований (соціальноекономічний);

– міра об’єктивності/суб'єктивності рішень щодо ризиків – з об’єктивною ймовірністю, з суб'єктивною ймовірністю, об'єктивно-суб’єктивною ймовірністю;

– міра ризиконасиченості рішень за ризиками – мінімальний, середній, оптимальний, максимальний, або допустимий, критичний, катастрофічний;

– типи ризиків – раціональний (обґрунтований), нераціональний (необґрунтований), авантюрний (азартний);

– час прийняття ризикованих рішень – випереджуючий, своєчасний, запізнілий;

– чисельність осіб прийняття рішень щодо ризиків – індивідуальний, груповий;

– ситуація – стохастичний (невизначені умови), конкуруючий (за умов конфлікту).

Гранатуров В.М., Захарченко Л.А., Орлов В.М., Отливанська Г.А., Потапова-Сінько Н.Ю. доволі узагальнено класифікували підприємницькі ризики з урахуванням розгляду у контексті підприємств ІТ сфери:

1) Кримінально-правові ризики

1.1. Кримінальні ризики

1.1.1. Злочинні ризики

1.1.2. Корупційні ризики

1.1.3. Ризики злочинної халатності

1.1.4. Шахрайські ризики

1.2. Адміністративно-правові ризики

1.2.1. Ризики навмисних порушень

1.2.2. Ризики ненавмисних порушень

2) Техніко-технологічні ризики

3) Природно-кліматичні ризики

4) Політико-економічні ризики

4.1.Ризик країни

4.2. Соціальні ризики

4.3. Податковий ризик

4.4. Фінансовий ризик

4.4.1. Інфляційний ризик

4.4.2.Дефляційний ризик

4.4.3.Відсотковий ризик

4.4.4. Валютний ризик

4.4.4.1.Трансляційний ризик

4.4.4.2. Операційний ризик

5) Організаційно-управлінські ризики

5.1. Маркетинговий ризик

5.2. Селективний ризик

5.2.1. Ризик втраченого зиску

5.2.2. Кредитний ризик

5.2.1. Кредитний ризик щодо позичальника

5.2.2. Кредитний ризик щодо способу забезпечення позики

5.3. Організаційний ризик

Більшість із перелічених вище ризиків відносяться до зовнішніх, окрім того дана класифікація доволі узагальнена та потребує деталізації для підприємств, врахування ризиків, що виникають усередині підприємства.

Ризики підприємницької діяльності Захарченко В. І., Меркулов М. М., Ширяєва Л. В. класифікували [55]:

1. За сферами прояву:

1.1. Економічний – ризик, пов’язаний зі змінами економічних чинників у процесі реалізації інвестиційного проекту.

1.2. Політичний – ризик виникнення різноманітних адміністративно-законодавчих обмежень господарської діяльності, які пов’язані зі зміною інвестиційної політики держави.

1.3. Соціальний – ризик страйків, здійснення під впливом працівників незапланованих соціальних програм та інші аналогічні загрози.

1.4. Екологічний – ризик виникнення екологічних катастроф і різних природних лих (землетрусів, пожеж, паводків і т. п.), котрі негативно впливають на діяльність підприємства.

1.5. Інші ризики – ризик рекету, крадіжок майна, обману з боку партнерів по бізнесу тощо.

2. За масштабами впливу – міжнародний, країнний (у масштабах країни), регіональний, галузевий, ризик окремих суб’єктів господарювання.

3. За джерелами виникнення виділяють два основні види ризику:

3.1. Систематичний або ринковий – властивий усім суб’єктам ринку, спричинений процесами, що відбуваються в ринковому середовищі в цілому.

3.2. Несистематичний ризик – цей вид ризику притаманний окремим суб’єктам господарювання, залежить від особливостей їх діяльності.

4. Залежно від можливого результату:

4.1. Чистий ризик – означає можливість отримання негативного або нульового результату (природні, екологічні, політичні, транспортні і частина комерційних ризиків).

4.2. Спекулятивний ризик – виражається в можливості отримання як негативного, так і позитивного результату. До цього виду ризику належать фінансові ризики, які, у свою чергу, можуть бути поділені на ризики, що пов’язані з купівельною спроможністю грошей (інфляційні і дефляційні, валютні, ризики ліквідності) та інвестиційні (ризики втраченого зиску, зниження дохідності, прямих фінансових втрат).

5. За відношенням джерел ризику до підприємства – внутрішній і зовнішній ризики.

6. За ступенем обґрунтованості рішень або дій – виправданий і невиправданий ризики та інші.

Відносно цілей захисту бізнесу цими ж авторами представлені види ризики [55, с. 364]:

– ризики втрати конкурентної позиції підприємства;

– ризики втрати доходів;

– ризики настання відповідальності при невиконанні зобов'язань;

– ризики втрати формального контролю над бізнесом;

– ризики невідповідності господарських операцій вимогам законодавства.

Авторами слушно зауважено, що єдиної класифікації ризиків немає та провести її практично неможливо через складність систематизації ризиків з причини їх різноманіття.

Класифікаційні ознаки загроз економічній безпеці та їх види представлено наступним чином [28, с. 379-381]: джерело виникнення (зовнішні; внутрішні); сфера виникнення загроз (правові, ринкові, політичні, екологічні, соціальні, науково-технічні, технологічні, демографічні); ступінь імовірності (невірогідні, маловірогідні, вірогідні); за функціональними складовими (фінансові, виробничі, інвестиційно-інноваційні, кадрово-інтелектуальні, інформаційні, маркетингові, силові); можливість виявлення та прогнозованість (явні та приховані, прогнозовані, непрогнозовані); тривалість впливу (довготермінові, середньотермінові, короткострокові); систематичність прояву (систематичні, несистематичні); обсяг втрат (несуттєві, істотні, значні, катастрофічні); людська діяльність (об'єктивні, суб'єктивні); ступінь керованості (керовані, некеровані); сфера діяльності підприємства (фінансові, виробничі, кадрові, інформаційні, техніко-технологічні); ієрархічність (стратегічні, поточні, оперативні); форми прояву (кількісні, якісні); масштаб виникнення (точкові, локальні, загальні); напруженість (нормальна, підвищена, надлишкова); природа виникнення (природна (об'єктивна), що спричинена стихійним природним явищем, незалежним від людини; штучна (суб'єктивна), що спричинена діяльністю людини, ненавмисною або навмисною)); за

напрямами структурних дисбалансів в економіці щодо об’єкта (інвестиційно-інноваційної активності; доданої вартості; структури капіталу; секторальної структури бізнесу; ділової активності). Окремо авторкою запропоновано класифікувати види загрози за особисто удосконаленими ознаками: за пригніченням функцій ринку та державного регулювання (порушення безперервності та взаємозв’язків процесів суспільного відтворення; перекручення інформації для споживача про продукцію вітчизняного виробництва; неадекватне ціновстановлення на споживчі товари (послуги); неналежне стимулювання внутрішнього виробництва продукції підвищеного суспільного попиту [233]; зменшення державного контролю за процесами у сферах виробництва, розподілу і споживання; зниження дієздатності організаційно-управлінської системи регулювання внутрішнього ринку і місцевого виробництва; зменшення кількості мотиваційних програм розвитку економіки); за змінами системи споживання (зниження частки продажу і споживання товарів інвестиційного характеру; послаблення інституційних можливостей системи прав споживача; зменшення можливостей і рівня впливу системи організацій з розвитку споживчо-купівельних переваг населення); за девіантними процесами у системі бізнесу (посилення рівня монополізації та концентрації на споживчому ринку; зростання передумов до збільшення тіньової (прихованої) економічної діяльності; деформація конкурентного середовища шляхом лобіювання поставок імпорту, експортно-імпортних операцій; погіршення кон’юнктурних характеристик у більшості сегментів внутрішнього ринку (зайнятості, оплати праці, доходів і витрат); збільшення обсягів імпорту сумнівного та низького рівня якості); за чинниками “пригнічення чинних конкурентних переваг” (послаблення мотивації та можливостей до розроблення та впровадження інновацій; зменшення ефективності створення територіально галузевих замкнутих виробничих циклів; зменшення мотивації переходу зі сфери торговельного посередництва до виробничого бізнесу; погіршення умов діяльності підприємств малого та

середнього бізнесу; нівелювання переваг виробництва якісної та конкурентоспроможної продукції).

Також науковицею запропонована класифікаційна ознака – ступінь впливу й, відповідно до неї, види загроз: виправні; невиправні; з можливістю уникнення; фатальні, проте пропоновані види, вказують на ознаку щодо їх усунення, а не ступінь впливу.

Досить чітко класифікували загрози Дідик А.М., Кузьмін О.Є., Ортинська В.Л., Козаченко Г.В., Погорелов Ю.С., Ілляшенко О.В. за наступними ознаками [72, с. 84]: ймовірністю реалізації (потенційні та реальні); ступенем поширеності (загрози загального характеру, специфічні та індивідуальні); ймовірністю реалізації (неминучі та відтерміновані); ступенем очевидності (явні та приховані); масштабами наслідків реалізації (локальні та загальні). Окремо надано перелік загроз загального характеру для підприємств України: несприятливі умови для бізнесу; тіньова економіка; недоліки у податковій системі; рейдерство; низька ефективність діяльності підприємств; висока енергоємність та матеріаломісткість виробництва; знос основних засобів, низька технологічність та автоматизованість процесів; амортизація (питання перегляду у відповідності до використання основних засобів та технологічності).

Загрози Ляшенко О.М. систематизовано за критеріями стосовно підприємства, із приміткою, що визначати їх потрібно базуючись на чинники реальності, причини виникнення та їх сутності, гостроти причин появи та їх терміновості, потенціалу та наявності коштів у суб’єкта, який спричиняє появу загроз і представляє їх поділ наступним чином: зовнішні та внутрішні; за терміном прояву (короткострокові; середньострокові; довгострокові); деталізовано (за джерелом виникнення, специфікою впливу, сутнісною ознакою, за масштабом впливу, за ступенем прояву, за мірою комплексності) [51, с.223].

Захарченком В.І. надана класифікація загроз у системі безпеки підприємства [53; 55, с. 217]: 1) за відношенням до об’єкту (внутрішнє

рішення); 2) за збитком (матеріальний, моральний); 3) за ймовірністю виникнення (вельми вірогідні, імовірні, малоймовірні); 4) за об'єктом (персонал; матеріальні та фінансові цінності, інформація); 5) за причиною появи (стихійні, навмисні); 6) за характером впливу (активні, пасивні); 7) за величиною збитку (граничний, значний, незначний).

В інструкції, що розроблена Міністерством економіки для проведення внутрішнього контролю на підприємствах, наведені наступні види ризиків (вказуючи на ймовірність) [114]:

- нормативно-правові (відсутність, суперечливість, регламентованість виконання функцій, процесів чи операцій у відповідних нормативно-правових актах)
- операційно-технологічні (недотримання термінів, формату подання документів, розподілу повноважень із виконання функцій, процесів чи операцій);
- програмно-технічні (відсутність прикладного програмного забезпечення, технічних засобів, оновлення або незадовільна робота);
- кадрові (низька професійна підготовка працівників суб’єктів внутрішнього контролю, недотримання посадових інструкцій тощо);
- фінансово-господарські (неналежне ресурсна та матеріальне забезпечення);
- фінансові (ймовірні втрати фінансових ресурсів);
- корупційні (правові, організаційні чинники, заходи контролю, що зумовлюють передумови скоєння корупційних правопорушень суб’єктами внутрішнього контролю);
- репутаційні (ймовірний негативний вплив на репутацію);
- інформаційної безпеки (потенційна можливість впливу на інформаційні системи, що можуть призвести до порушення цілісності, конфіденційності, автентичності, авторських прав чи то доступності інформаційних ресурсів);

Окремо розподіллено ризики на дві категорії – зовнішні та внутрішні, такий поділ, як данина оточенню підприємства (відповідно зовнішньому і внутрішньому) без якого не може існувати підприємство, крім того, така класифікація відслідковується у більшості розглянутих нами робіт, що присвячені ризикам та безпеці.

Внутрішні ризики виникають через події, що ймовірно можуть відбутися та позначитися на результатах діяльності, досягненні мети підприємства, планів, виконанні функцій, на які підприємство має вплив та може контролювати за вжиття певних заходів щодо конкретної ситуації.

Зовнішні ризики пов’язані із подіями, що ймовірно можуть відбутися із-зовні, не пов’язані із роботою підприємства, виконанням ним функцій та завдань, на які підприємство може мати або не мати вплив. Подій із-зовні можуть спричинити суттєвіший негативний вплив на підприємство, ніж внутрішні події, їх важче відслідковувати та прогнозувати, тому має розглядатися множина варіантів протидії їм для забезпечення стійкості підприємства до їх дії.

Безпека тісно пов’язана із захищеністю підприємства або його окремих об’єктів, розгляд ризиків та загроз є обов’язковим, оскільки саме їм чиниться супротив, розглядаються можливості супротиву негативним впливам. Класифікація ризиків та загроз допоможе систематизувати їх та в подальшому використовувати для аналізу, оцінки, розробки відповідних заходів захисту, ідентифікації, моніторингу.

Галузева приналежність підприємства вимагатиме конкретизації ризиків та більш детальної класифікації, оскільки специфіка роботи підприємства впливає на оточення підприємства, формує особливості його функціонування, тому змінюватимуться ризики та загрози, а їх визначення є основою для вирішення питань безпеки.

Послуги різняться від товарів, їм притаманні характеристики незбереженості в часі, невіддільності від джерела отримання (прив’язка до надавача послуг), нематеріальності, невідчутності на дотик, неосяжності,

невидимості (процес передачі часто залишається осторонь отримувача, отримується саме результат). Сфера послуг у загальному ВВП розвинутих країн, у тому числі Європейського Союзу, займає часту 70% і більше, крім того, без послуг важко уявити сьогоденне існування суспільства та функціонування підприємств, серед таких послуг – електронні комунікаційні. Саме підприємства зв'язку є джерелом утримання більшості підприємницьких структур у працездатному стані, дозволяють підприємствам продовжувати роботу навіть у надскладних умовах.

Загальний обсяг ВВП України у 2021 р. становив 1735940 млн грн та 1625230 млн грн у 2022 р., у розрізі сфер на телекомунікації та інформацію припадає 73269 млн грн у 2021 р. та 69501 млн грн у 2022 р., відсоток зменшення за 4 кв. склав – 0,143% (у 4 кв. 2021 р. відбувся приріст на 0,148% по відношенню до 2020 р.). Доходи зростали впродовж аналізованого періоду, у 2022 році відбулося зменшення доходів через вторгнення країни агресора на територію України (рис. 2.3). Однозначно зменшення обсягів доходів вказує на проблеми, які викликані невизначеністю, загрозами обстрілів та відсутністю електроенергії, що призвело до низки проблем з наданням послуг, крім того, частина абонентів була втрачена через їх переміщення в інші країни та потребою більш якісного зв'язку у роумінгу.

Підприємства зв'язку відносяться до об'єктів критичної інфраструктури і потребують захисту з боку держави та інституцій, саме електронні комунікації надають можливість підтримувати працездатність підприємствам у невизначених умовах, що на сьогодні склалися, залишатися на зв'язку абонентам, військовим [204; 205]. Тож підсумовуючи, отримуємо, що ризики та загрози в конкретної ситуаціях потребують класифікації. Складність систематизації ризиків полягає в їх різноманітті, тому побудова єдиної класифікації практично неможлива. У літературі запропоновано багато класифікацій ризиків, пов'язаних з різними цілями та заснованими на різних ознаках, проте, зважаючи на сьогоденну втрату прогностичності та невизначеності умов доцільно розглядати, як ризики, так і загрози, що дозволить конкретизувати управлінські заходи щодо їх упередження та усунення дії.

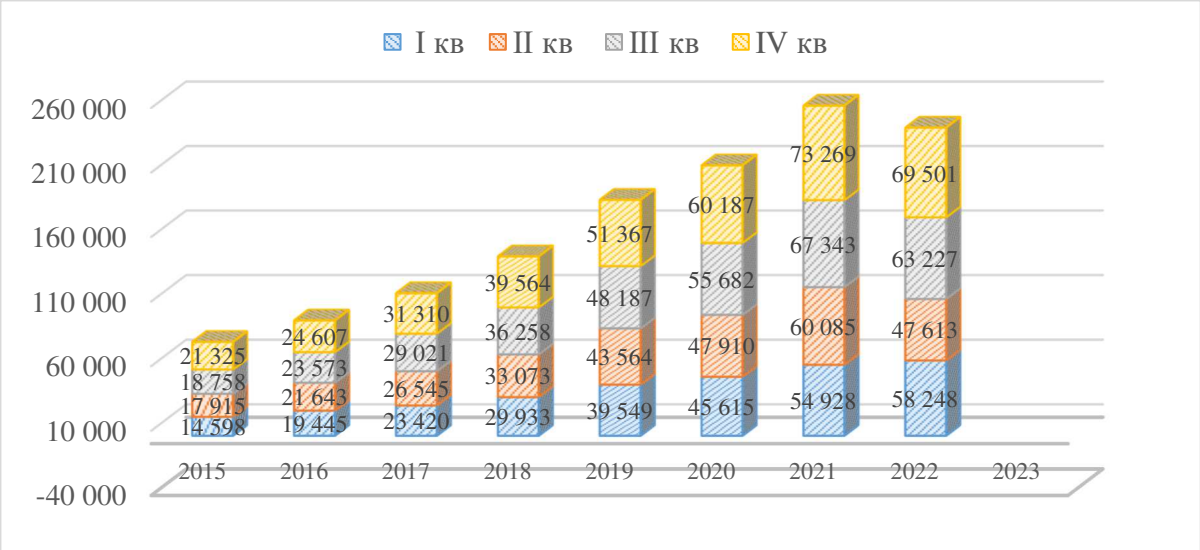


Рис. 2.3. Щоквартальний ВВП за сферою інформація та електронні комунікації впродовж 2015-2022 рр., млн грн

(побудовано автором за[117;118])

Зважаючи на множину ризиків та загроз, що нині існують для функціонуючих підприємств, їх за кваліфікаційними ознаками узагальнено та представлено схематично (рис. 2.4). Більшість із них є описовими, тож при проведенні аналізу та визначенні показників слугують як якісні, тобто характеризують ризики та загрози підприємства, а для аналізу та оцінки краще визначати кількісно ризики та загрози. Із наведеної вище класифікації до таких належать ризики та загрози за ступенем ймовірності (можна оцінити ймовірність настання та реалізованість), за наслідками впливу (межі прийнятності), за масштабом дії (розміри нанесення збитків). Зважаючи на те, що кожне підприємство виконує певні функції, а їх доволі багато, доцільно увагу приділяти ризикам та загрозам, їх оцінці та дослідженню за функціональними складовими. У результаті дослідження наукових праць, у яких висвітлювалися складові безпеки, було виділено основні із них: фінансова, техніко-технологічна, виробнича, енергетична, ринкова, інтелектуальна, кадрова, інтерфейсна, інформаційна, фізична (силова), політико-правова, екологічна, інформаційно-інноваційна та, пропонована нами, електронно-комунікаційна, оскільки цифровізація та підвищення ролі цифрових послуг щодень зростає, тому врахування її при формуванні безпеки набуває сенсу та актуальності.

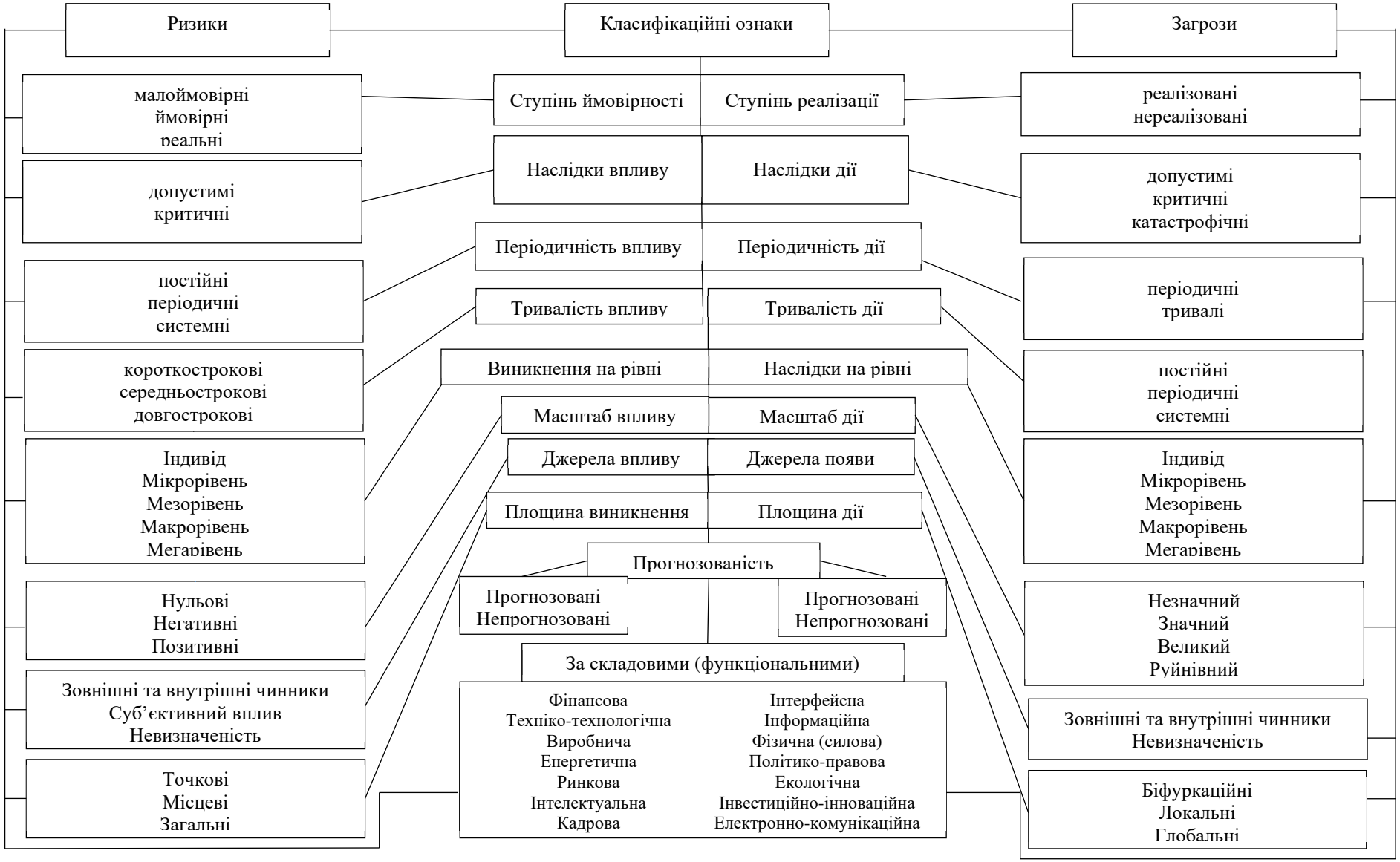


Рис. 2.4. Ризики та загрози безпеці підприємства за кваліфікаційними ознаками

(узагальнено та складено автором за даними [28, с. 379-381])

2.2. Трансформаційні зміни управління безпекою підприємства в умовах невизначеності та втрати прогностичності

Функціонуюче підприємство динамічно розвивається, оскільки відбуваються зміни навколо і всередині підприємства, які виникають внаслідок його діяльності, впливу оточуючого середовища, коливань попиту, зрушень в економіці. Діяльність підприємств не обмежується суто операційною, інвестиційною, фінансовою, тому що невизначеність умов, зростання загроз щодо функціонування підприємств спричинили появу бекозабезпечувальної управлінської гілки.

Погляди на безпеку змінюються через: глобалізацію, цифровізацію, інтернаціоналізацію зв'язків, міжнародну інтеграцію, гармонізацію законодавчих питань для полегшення інтеграції, а останнім часом - глобальні екологічні проблемами людства, пандемію, військові конфліктами на тлі геополітичного напруження. Останні мають невизначений характер, тому спрогнозувати події або гарантувати безпеку підприємств досить важко, проте лише керуючи змінами, прагнучи стабілізувати ситуацію, що загрожує безпеці, можна виправляти негативні прояви тих чи інших подій. Міжнародна діяльність та постачання послуг на міжнародні ринки, потребує досліджень соціокультурних особливостей, міждержавних зв'язків, політичного спрямування та поглядів, щоб убезпечити підприємства від потенційних геополітичних загроз [325; 364].

Саме управління дозволяє скеровувати рух об'єкта в правильному напрямку – стабілізації, утримання конкурентних позицій, забезпечення відновлення у розвитку. Нами визначено, що безпека – стан, до такого стану прагнуть суб'єкти господарювання та економічні одиниці незалежно від сфер діяльності. Наразі питання безпеки актуалізовано, активно досліджується через умови невизначеності, крім того, у повоєнний час потребуватиме

аналізу та напрацювань по її забезпеченню, не просто на найближчу перспективу, а на десятки років.

Узагальнюючи знання щодо управління, можемо ідентифікувати його як:

- цілеспрямовану дію суб'єкта на об'єкт;
- прийняття рішень суб'єкта щодо об'єкта;
- скеровування об'єкта (на основі інформації щодо оточення) у певному напрямку руху суб'єктом.

Верескун М.В., Камишникова Е.В.зазаначають, що в загальній політиці безпеки важливими є базові складові, використання яких найбільше сприяє досягненню безпековому стану, до яких відносять: проактивність та іноваційність (генерація та впровадження інновацій у виробничі та управлінські процеси); ставка на софт-скіллз (багатогранність та ерудованість, особисті якості персоналу); фокусування та концентрація (уникнення одночасної постановки декількох задач, фокус на головному) [112].

На сьогодні всі господарюючі суб'єкти, економічні одиниці є керованими, їх функціонування продовжується саме на основі управління, яке націлене на досягнення ними свого цільового призначення або мети.

Управління – не просто творчий процес, це знання, розуміння його сутності, принципів із поєднанням глибокого аналізу процесів та явищ, що відбуваються в середовищі об'єкта управління.

Відомо, що більшість економістів сприймають управління як сукупність ресурсів: земля, праця, капітал, підприємницькі здібності та інформацію (остання додана із розумінням важливості її в умовах інформатизації суспільства та інформованості щодо продукції та послуг). Менеджери вбачають, що управління – процес, який складається із планування, організації, приведення в дію, контролю щодо досягнення визначених цілей шляхом використання людей та інших ресурсів (Дж. Р. Террі), або ж процес, за якого визначаються, уточнюються, реалізуються цілі та задачі конкретної групи людей (П. Ф. Друкер), подібне й визначення –

мистецтво досягнення цілей через людей із баченням людини, як невід'ємного елемента управління (М.П. Фоллет). Управління розглядається також більш широко, як сукупність заходів (включаючи планування, прийняття рішень, організацію, керівництво, контроль), які направлено на ресурси (людські, фінансові, фізичні, інформаційні) з метою ефективного досягнення організаційних цілей (Р.У. Гріффін).

Поєднуючи бачення економістів та менеджерів щодо управління, розуміємо, що це процес координування та керування певними ресурсами за допомогою людей з метою досягнення цілей.

Екстраполюючи управління на безпеку, управління безпекою буде вбачатися як процес забезпечення функціонування підприємства за людського керування ресурсами підприємства на основі інформації щодо оточення для упередження ризиків, усунення дії загроз та результатів їх реалізації загроз.

Досліджуючи безпекові питання, Орєхова К.В. вбачає поетапне ефективне управління загрозами підприємства запорукою безпеки (починаючи з вибору методу оцінки загроз; розподілу зональності загроз, визначенні рівня загроз, підбору методу управління ними та його використання [с.121, 115]).

Управління ризиками є процесом, який полягає у виявленні, проведенні оцінки та реакції на ризик, як нами з'ясовано, ризики вказують на ймовірність, а загрози безпосередньо на результат реалізації ризику та мають наслідки, тому загрози можуть кількісно визначатися для того, щоб приймати певні рішення щодо них, управляти. Показник загрози залежить від несприятливого впливу реалізації події та ймовірності її настання.

Управління матиме певний напрям руху, який заданий керуючою стороною, рух можна задати на основі інформації щодо ресурсів та середовища, чим краще досліджено оточення та умови функціонування, тим чіткіше буде сформовано безпекові заходи та налагоджений процес управління безпекою підприємства. Однак, розуміння безпеки в нинішніх

умовах змінюється, невизначеність вносить свої корективи, групою науковців на чолі із Черепом О.Г. розглядається управління персоналом в умовах воєнного стану, зазначаючи можливості уряду щодо підвищеного контролю та обмежень свобод громадян, які ускладнюють прийняття рішень за певної обмеженості, сповільнюють процес управління та знижують його ефективність [122]. Також вплив на результати діяльності в умовах воєнного стану сприймається як дія особливих обставин, крім того нестабільність, як економічна, так і політична, зменшує обсяги інвестування, сповільнюючи розвиток підприємства, що ускладнює прийняття стратегічних рішень та планування. Вважається, що залучення інвестиційних ресурсів сприяє модернізації виробничих систем, створенню стабільного економічного поля розвитку суб'єктів господарювання, тобто забезпечує безпечність функціонування [124].

Консалтингова компанія Advanter Group після вторгнення агресора на територію України дослідила ситуацію на ринку функціонуючих підприємств, частка працюючих підприємств в середині березня 2022 року становила 13,5% (із них 5,8 функціонували частково, 5,85 % зменшили обсяги виробництва, 2% – працювали майже без змін). Станом на квітень місяць 2022 року ситуація дещо покращилася – 19,1% підприємств відновили роботу частково, а 8,5 % збільшили обсяги виробництва, а на початок травня зросла кількість підприємств (до 24,1%), що зменшили обсяги виробництва (надання послуг), незмінні обсяги залишились у 12,3 % підприємств [118]. Така динаміка щодо обсягів виробництва та результатів підприємства вказує на таку невизначеність – коливання обсягів через нестабільність економіки, політичної ситуації, коливань попиту з причин зниження купівельної спроможності та зростання безробіття населення через воєнний стан в Україні. Безперечно, втрачається інвестиційна привабливість країни, коли вона того особливо потребує, автоматично зменшуються інвестиції у розвиток підприємств.

Західні підприємства у разі нестабільності оточення вдаються до антикризового управління, широко вживаними є наступні види [125]:

– аматорське антикризове управління (керівник самотужки розробляє план виходу підприємства із кризи);

– кризове консультування (важко оцінити масштаби впливу та наслідки, за рахунок їх масштабованості виникає потреба залучення спеціалістів для розробки комплексу заходів, починаючи від експрес-аналізу стану підприємства, розробку миттєвих заходів щодо урегулювання діяльності підприємства та стабілізації за рахунок антикризових заходів для подальшого розвитку підприємства);

– залучення зовнішнього антикризового управлінця (проблеми глибинні, персонал та керівництво неспроможні самотужки подолати кризу, тому залучають антикризового менеджера, який отримує винагороду у разі виходу із кризи та розвитку підприємства, оплата пропорційна приросту доходу підприємства).

Невизначеність диктує нові вимоги щодо бачення світових проблем, які неможливо розглядати паралельно, оскільки глобалізація призвела до міжнародної інтеграції та взаємної дотичності. Можемо припустити, що формується новий світогляд щодо безпеки, яка має гарантуватися на всіх рівнях та масштабуватися.

Динамічність та невизначеність світу продукувала ідею появи терміну VUCA (акронім – volatility; uncertainly; complexity; ambiguity), який вперше було вжито у 1987 році У. Беннісом та Б. Нанусом (у теорії лідерства), пізніше використаний для опису багатогранності світу після закінчення холодної війни. Зараз широко використовується у корпоративному управлінні, формує підхід, що враховує плинність та змінність умов при прийнятті рішень, коли інформація втрачає свою прогностичну силу.

Умови, в яких нині функціонують усі без виключення підприємства України, є невизначеними, воєнний стан призводить до появи нових

викликів, які важко передбачити. За VUCA існують виклики, які можливо розподілити за 4 типами, а саме [129]:

1. Volatility (волатильність, мінливість, нестабільність, нестійкість) – швидка динаміка, зміни, зростання швидкості, масштабів, інтенсивності, збільшення нестабільності.

2. Uncertainly (невизначеність) – знижується спроможність передбачення подій, раптова та непередбачувана поява нового, незрозумілість причинно-наслідкових зв’язків.

3. Complexity (складність) – збільшується множинність, різноманітність невідомих елементів, систем і рівнів, зростає кількість можливих варіантів дій, що призводить до конфлікту інтересів.

4. Ambiguity (неясність, двозначність, невизначеність) – все навколо стає “розмитим”, рамкові умови та передумови важче зрозуміти, інформацію та описи можна інтерпретувати по-різному, немає об’єктивності в оцінці ситуації.

Процеси, явища, становище підприємства в умовах невизначеності можна проаналізувати за VUCA, склавши матрицю, розподіливши умови на групи: волантильність (V); невизначеність (U); складність (C); неясність (A).

Активаторами VUCA виступають:

– для волантильності – швидкозмінність ринкових агентів та показників (курс валют, нафта, газ), зміна економічних процесів;

– для невизначеності – непередбачуваність явищ, процесів, подій та наслідків їх дії (зміни клімату, науково-технічний прогрес, промислові революції);

– для складності – інтеграційні та глобалізаційні процеси, множинність складових та різноманітність бізнесу;

– для неясності – дезінформація, неправдивість трактувань та смислів, відсутність прецедентів, неоднозначність рішень.

Сьогоднішня складність ситуації потребує проведення аналізу волантильності, невизначеності, складності та неясності умов, їх

розмежування та обрису зовнішнього оточення для управління безпекою підприємства, що дозволить передбачувати та реагувати на швидкоплинність явищ та їх зміну, діяти навіть у тому випадку, коли немає впевненості та чіткого бачення напрямку руху, орієнтуватися у надскладних ситуаціях, забезпечувати (підтримувати) ефективність, незважаючи на непередбачуваність.

У документі "Аналізи ризику. Процеси та застосування" (Американська Асоціації Інженерних товариств) концепція ризику містить оцінку ризику, як наукового аналізу походження та масштабів ризику в окремій ситуації, та управління ризиком, як аналізу ризикової ситуації і розробку рішення щодо мінімізації ризиків.

Окрім невизначеності, на сьогодні важливим питаннями є використання інформаційно-комунікаційних технологій, штучного інтелекту, тому при управлінні варто це враховувати. Оскільки і сам ризик є мостом між визначеністю (коли нібито все зрозуміло, відслідковуються причинно-наслідкові зв'язки) та невизначеністю (коли подія може відбутися непередбачувано спонтанно), врахування невизначеностей є необхідністю, що посилюється в нинішніх умовах функціонуванням підприємств.

Деякі із сфер особливо гостро реагують на зміни, що відбуваються у результаті технологічних змін, відкриттів, розвитку, до такої сфери відносять електронні комунікації. Волантильність характеризується динамічністю, швидкістю змін, більшість із них пов'язано із технологічними змінами до яких частина підприємств пристосовується, а частина виходить на ринок із новими продуктами та послугами, автоматично скорочується життєвий цикл продукту.

Поява смартфонів та смарт-технологій суттєво пришвидшила діджиталізацію, оскільки нові технології спричинили потребу у нових послугах з боку клієнтів – бути постійно на зв'язку, бути мобільним і одночасно виконувати свої функції з будь-якої точки перебування, навіть перебуваючи у постійному русі.

Сфера інфокомунікацій характеризується динамічністю, що стрімко розвивається та представляє нові послуги для клієнтів, які потребують якісних послуг у відповідності до появи нових технологій, наразі 5 G. Розвиток сфери пов'язаний із технологічними змінами: поява технологій потребує нових послуг, заміну засобів передачі інформації на сучасні, які підтримуватимуть нові технології та можливості. Відбулася заміна фіксованого зв'язку на рухомий, і, в противагу використанню впродовж декількох десятиліть стаціонарних телефонів, мобільний зв'язок та технології вимагають постійного оновлення мобільних пристроїв, смартфонів для підтримки нових послуг та технологій зв'язку.

Консалтингова компанія з гнучких інновацій "Me&Company" вбачає, що сучасний світ вже не може існувати без технологій, електронних комунікаційних послуг, представивши бачення серед потреб людини послуги зв'язку та технології їх надання (рис. 2.5)

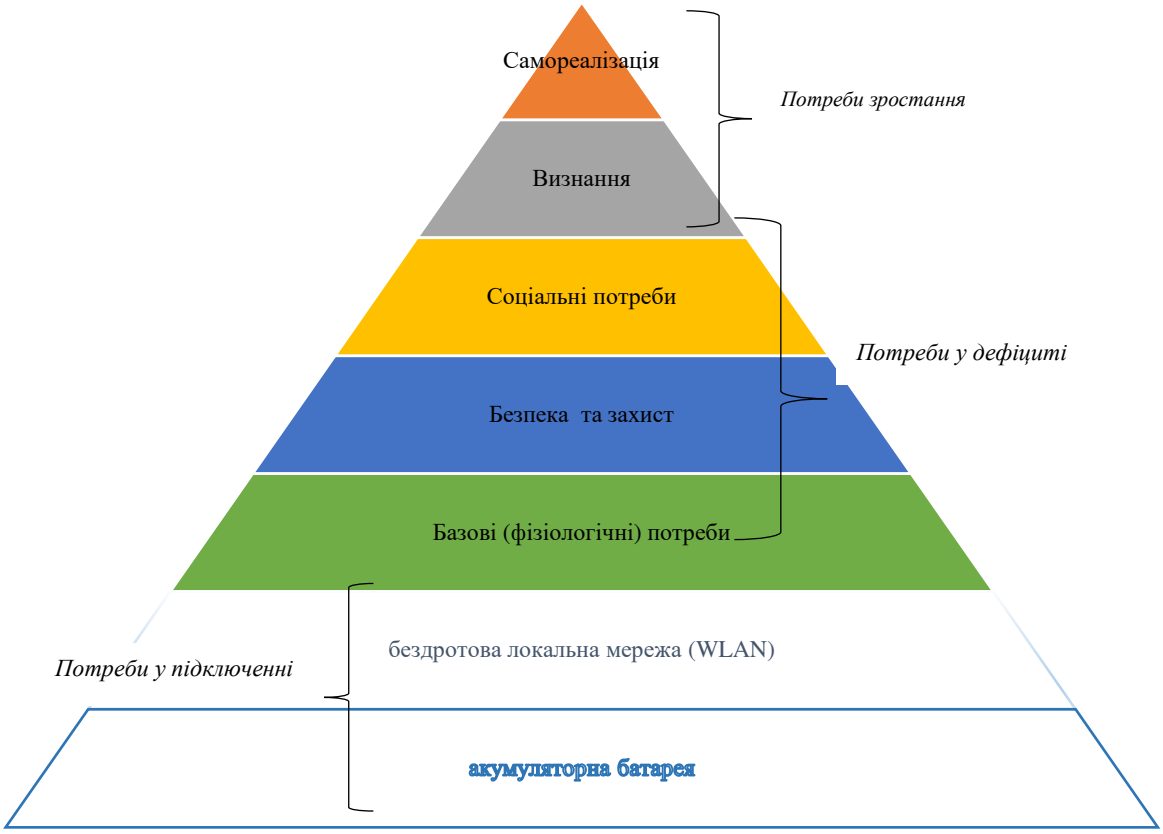


Рис. 2.5. Модернізована піраміда потреб Маслоу безпекового функціонування підприємств електронних комунікацій

(складено та узагальнено автором за даними [124])

Досліджуючи потреби сучасності людства, підприємств у постійному перебуванні на зв'язку, німецька компанія включила щабель "потреби у підключенні" до загальних потреб сучасності для забезпечення свого функціонування, існування та відзначає їх, як волантильність.

Тож при управлінні підприємством невизначеності мають аналізуватися та прийматися до уваги, оскільки вони формують нові виклики та можливості та безпосередньо впливають на функціонування підприємств, появу нових продуктів, послуг, результати діяльності та обсяги виробництва або надання послуг (у бік скорочення або зростання).

Зважаючи на наслідки невизначеностей сьогодення, які можна охарактеризувати за VUCA, на майбутнє компаніям для протидії наслідків невизначеностей, як інструмент варто розглянути – BANI (Brittle, Anxious, Nonlinear, Incomprehensible) [128]:

Крихкий (Brittle) – можливість краху навіть за сьогоднішньої стійкості через бажання максимізації прибутку; криз секторів економіки; збій ланцюгів постачання (відсутність енергетики, припинення торгівлі в одному із регіонів можуть призвести до порушень у інших)

Тривожний (Anxious) – надлишок інформації, тиск фейковими новинами призводять до станів тривоги щодо прийняття рішень, залежності від вибору оточення, навіть, якщо не згодні із ним.

Нелінійний (Nonlinear) – неоднозначність руху через що довгострокові плани нечіткі, рішення не завжди призводять до бажаного результату (екологічні проблеми людства через бачення процесів виробництва, промисловості наприкінці минулого століття без врахування негативних наслідків для екосистем).

Незрозумілий (Incomprehensible) – обернена залежність пошуку істини від широкої поінформованості, не зважаючи на доступність інструментів для їх вирішення в умовах сучасності.

Управління у сучасному світі набуває абсолютно нових траєкторій руху, з урахуванням невизначеностей, майбутніх викликів, стійкості, сталості

розвитку для майбутніх поколінь. Використання матриць VUCA та BANI відкриває нові можливості для підприємств, управління скеровується не лише на сьогодні, а й на майбутнє, що допомагає підприємствам протидіяти викликам сьогодення та боротися із складнощами, наслідками пандемій, екологічних катастроф, війн, економічних криз.

Проєкція процесу управління з безпекою підприємства в умовах невизначеності, передбачає забезпечення керуючої сторони максимально можливим обсягом інформації, чого можна досягти за допомогою VUCA та BANI-аналізу викликів та невизначеностей, вважаємо, що даний науково-методичний підхід, на відміну від існуючих, дозволить отримати максимально можливий обсяг інформації щодо оточення для прийняття рішень, ефективного упраравління безпекою підприємств й дозволить упередити від втраті прогнозованості управління.

Тож, підсумовуючи, робимо висновок, що управління є доволі складним процесом, навколо нього вибудовується система зв'язків між суб'єктами та об'єктами управління, які вступають в управлінські відносини щодо ефективного використання наявних ресурсів, використання потенціалу, супротиву дестабілізуючих чинників з метою отримання максимального прибутку, підвищення конкурентоздатності підприємства. Функціонування підприємства, його розвиток, управління тісно пов'язані із стадіями його життєвого циклу.

Управління безпекою – безперервний процес, в якому мають враховуватися зміни станів підприємства від впливу оточення та стадій життєвого циклу підприємства:

– зародження ідеї появи продукту, його створення

– зростання з одночасним супротивом дії внутрішнього та зовнішнього оточення, упередження від появи загроз

– зрілість, стадія, яка характеризується утриманням позицій, які були зайняті підприємством

– спад, на якому особливо чутливими стають питання безпеки, оскільки підприємство починає втрачати свої позиції, зокрема, частка на ринку скорочується, обсяги продажів спадають, зменшується прибуток, конкурентоспроможність знижується.

Отже, питання безпеки пов'язано із стадіями життєвого циклу підприємства, тому й підходи до управління нею будуть різнитися в залежності від чутливості підприємства до змін під час перебування його на конкретних стадіях (табл. 2.1)

Таблиця 2.1

Зосередження підприємства на питаннях безпеки залежно від стадій життєвого циклу

Стадії життєвого циклу підприємства	Чутливість	Зосередження щодо питань безпеки
Зародження ідеї та створення продукту	Несуттєві коливання, спричинені вподобаннями споживачів та їх побоюваннями щодо пропонованого продукту-новинки	Позиціювання, захист комерційної таємниці
Зростання	Поява внутрішніх і зовнішніх загроз, коливання попиту (зростання)	Розширення виробництва продукції та надання послуг
Зрілість	Втрата позицій, наміри утримати охоплену частку ринку	Маркетинг – створення нових продуктів, використання нових технологій
Спад	Низький рівень економічної безпеки, спад обсягів продажів (надання послуг), зменшення прибутку, зниження конкурентоспроможності	Фінанси підприємства – концентрація уваги навколо збереження ефективних напрямків діяльності

(узагальнено та складено автором)

Спроба пов'язати стани розвитку підприємства та дії загроз була зроблена Мельником С.І. [73, с. 175], який досліджував питання фінансової безпеки, як одне із першочергових до розгляду серед складників економічної безпеки. Науковцем було представлено бачення наростання дії впливу загроз в процесі життєвого циклу підприємства. Так, стадія зародження характеризується появою викликів, розвиток – підпадає під дію ризиків по

усіх складниках безпеки, на стадії часткової стабільності відбувається розвиток загроз (окремі ризики за складниками безпеки посилюють загрози), період спаду знаходиться під впливом зовнішніх і внутрішніх загроз, що врешті-решт, призводить до руйнування системи безпеки на стадії ліквідації, або ж, до оновлення у разі протидії загроз або адаптації до них.

Із появою загроз відбуваються зміни у діяльності підприємства (під час яких відбувається процес переходу їх у конкретну фазу) характеризується наступними трансформаціями:

– слабко виражені ознаки змін умов, процесів та явищ, дій суб'єктів внутрішнього та зовнішнього середовища функціонування підприємства, з'являються першопричини зрушень у негативну сторону (фаза актуалізації загрози діяльності підприємства);

– чітко виражені умови, процеси, явища, що посилюють дію загроз за рахунок впливу дій суб'єктів зовнішнього та внутрішнього оточення (фаза активізації загрози діяльності підприємства);

– зміни негативного характеру на підприємстві під впливом процесів, явищ, у середовищі підприємства, а також дій з боку суб'єктів (фаза загрози реалізації діяльності підприємства).

Підприємство є складною системою, починаючи із появи ідеї та створення, відбувається його знайомство із безліччю викликів, на які миттєво варто звертати увагу, щоби не допустити появи ризиків і переходу їх у загрози. Вчасний та регулярний контроль за діяльністю підприємства, приділення уваги проблемним питанням, дослідження передумов зміни в оточенні, внутрішньому та зовнішньому середовищі, убезпечить підприємство від руйнівної дії в результаті реалізації загроз.

Розвиток загрози діяльності підприємства розглядається науковцями з точки зору виникнення за наявності відповідних умов в індиферентних стосовно підприємства процесів та явищ у внутрішньому та зовнішньому середовищі діяльності підприємства або індиферентній поведінці суб'єктів

зовнішнього середовища адресної спроможності спричинити зміни в діяльності підприємства [74, с.75].

Тобто можемо стверджувати, що паралельно розвитку та життєвим циклам підприємства, існують та розвиваються загрози, які мають свою лінію руху та ескалації, як нами з'ясовано, наростають загрози за вектором: викликів – ризик – загроза, що переводить підприємство у стан небезпеки.

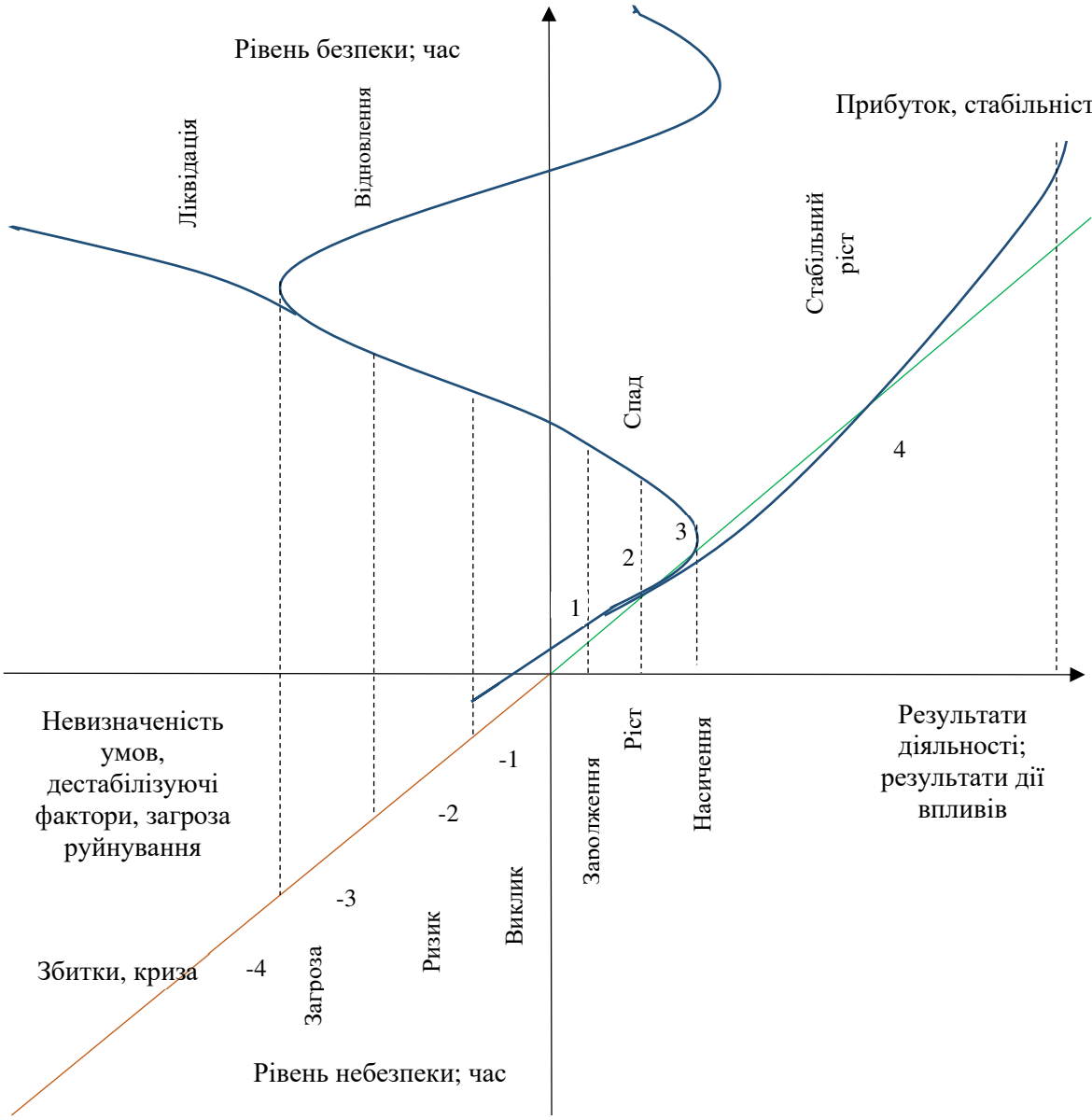


Рис. 2.6. Імплементація у графіку життєвого циклу підприємства дії впливів та відображення їх на результатах діяльності

(авторська розробка)

Беручи до уваги напрацювання щодо управління у контексті безпеки, управління безпекою підприємства буде залежати від чинників впливу та їх комбінації, від індиферентності умов (процеси та явища не впливатимуть на діяльність підприємства), загроз, змін та невизначеностей, складових безпеки (ресурсів), суб'єктів та об'єктів безпеки, від стадій життєвого циклу підприємства та технологічних змін, прогресу. При чому управління безпекою підприємства має бути націлене на протидію зовнішнім ризикам, загрозам та виробленню імунітету до зовнішніх чинників, загроз.

2.3. Еволюція поглядів щодо управління безпекою підприємства обумовленою змінами підходів до виробництва

Підприємствам притаманний активний пошук нового, невіданого, досі непізнаного, того, що надасть можливість досягати нових звершень та удосконалень. Відповідно реагують суб'єкти ринку, зокрема підприємства, які намагаються активно й динамічно розвиватися, реагувати на зміни в сфері його оточення задля вирівнювання як виробничих, так і фінансово-економічних показників. Тому, сучасне підприємство прагне забезпечити собі певну унікальність, яка формуватиме його особливий імідж та слугуватиме гарантією функціонування в довгостроковій перспективі, не зважаючи на жорстку конкуренцію. На сьогодні утвердження підприємства у такому статусі можливо досягти за рахунок абсолютно нового, прогресивного та інноваційного підходу формування засад його створення. Беручи до уваги четверту технологічну революцію та шостий технологічний уклад, який формує нову хвилю розвитку економіки в світовому вимірі важливу роль відграватимуть саме інноваційні, високотехнологічні підприємства, які відповідатимуть тенденціям розвитку у напрямку нового технологічного укладу, до яких відносяться підприємства-постачальники електронних комунікаційних мереж та послуг.

Теоретичним положенням інноваційного розвитку підприємства присвячені роботи зарубіжних науковців: Кристена К., Пітерса Т. Є. Менсфілда, Р. Нельсона, К. Фрімена, серед вітчизняних науковців: Николюк О.М., Антюшкіна В.В. Дослідженням інноваційної активності підприємств займалися М. Кондратьєв, Й. Шумпетер., Бірюков О.В., Р.Солоу.

Низка розробок присвячена аспектам формування інноваційного потенціалу підприємств, над якими працювали науковці: Вербицька В.І., Чугрій Н.А., Куцик В.І., Пішеніна Т.І. Функціонуванню інноваційних підприємств в сучасних умовах, присвячено наукові праці вітчизняних вчених: Гудзь О.Є., Шевченко О.М., Біловодської О.А., але зміна технологічного укладу та євроінтеграційні процеси, які відбуваються сьогодні, актуалізують необхідність визначення ролі та місця інноваційного підприємств саме з урахуванням таких змін.

Технологічні зміни посилюють роль і значення інноваційних підприємств, до яких можна віднести підприємства сфери електронних комунікацій. На сьогодні інтеграційні процеси порушують питання реформування, а технологічні зміни – активізують інноваційні процеси.

Науково-технічна політика проводиться з урахуванням цих змін і процесів, вже здійснено кроки в належному її формуванні про що свідчить низка прийнятих законопроєктів, що стосуються інновацій, інноваційної діяльності, інноваційного підприємства.

За Законом України “Про інноваційну діяльність”, “інновації” – новостворені (застосовані) і (або) вдосконалені конкурентоздатні технології, продукція або послуги, а також організаційно-технічні рішення виробничого, адміністративного, комерційного або іншого характеру, що істотно поліпшують структуру та якість виробництва і (або) соціальної сфери.

Під терміном “інноваційне підприємство” (інноваційний центр, технопарк, технополіс, інноваційний бізнес-інкубатор тощо) розуміється підприємство (об’єднання підприємств), що розробляє, виробляє і реалізує

інноваційні продукти і (або) продукцію чи послуги, обсяг яких у грошовому вимірі перевищує 70 відсотків його загального обсягу продукції і (або) послуг [131].

Максимальне сприяння має відбуватися з боку інституцій щодо створення таких інноваційних підприємств, які у ланцюжку результат інтелектуальної праці – інноваційний продукт повністю використовуватимуть вітчизні чинники виробництва, а не запозичуватимуть чужі ідеї, розробки і засоби для його створення. В подальшому пріоритетність таких інноваційних підприємств стане запорукою стабільного розвитку нашої країни й утвердження її як країни-лідера, в протилежному випадку – потрапимо до країн, що виробляють продукцію за рахунок країн-донорів, за їх науковими відкриттями та інноваційними розробками. Якщо підприємствами взагалі не розроблятиметься, вироблятиметься, реалізовуватиметься інноваційна продукція, а лише споживатиметься продукція, створена закордонними підприємствами, то в такому випадку країну можна буде охарактеризувати як “паразит-споживач інноваційного продукту’ або крана-аутсайдер за науковими відкриттями та інноваційними розробками. Слід зауважити, що новий технологічний уклад та його співпадання з низхідною довгостроковою хвилею економічного розвитку свідчать про нагальність переорієнтації у виробництві. Тобто, створення нових умов для функціонування інноваційного підприємства є необхідністю й спричиняється всеохоплюючим характером змін у світі, пов’язаний з тим, що добігає кінця третя науково-технічна революція. Професором Клаусом Швабом зазначено, що передбачаються значні перетворення, які фундаментально змінять життя, працю, спілкування, відбудуться кардинальні зміни у всіх галузях, руйнуватимуться усталені норми і зв’язки, при чому не пропонуються процедури їх оновлення.

Розглянувши економічні цикли розвитку економіки та рівень розвитку технологій на кожному конкретному етапі, можна прослідкувати вплив останніх на економічне зростання. Праці Шумпетера стали підґрунтям для

формування теоретичних положень щодо тісного зв'язку між підприємництвом та технологічним розвитком, а також активним впровадженнями інновацій із зростанням. На його думку, саме підприємство відігравало важливу роль у виникненні інноваційних продуктів та їх використанні.

Дослідження результатів науково-технологічної революції, технологічних укладів та співставлення їх з періодизацією економічних циклів (для більшої наочності представлено на рис. 2.7), дало змогу зробити висновок, що економіка знаходиться в низхідній фазі циклу свого розвитку.

Роки / Подія	1780	1805		1855	1880	1905	1930	1955	1980	2005	2030
Науково-технічна революція	I (до кінця XIX ст): індустріалізація суспільства, перехід від ручної праці до машинного виробництва						II (до середини XX ст): зміна технологій виробництва, використання електрики, поява ДВЗ		III (з середини XX ст до тепер) Автоматизація виробництва, інформаційні технології		IV (сього дення) біологічні технології, дистр уптивні техно логії)
Технологічний уклад	I (1780-1830): текстильні машини, енергія води		II (1830-1880): паровий двигун, вугілля		III (1880-1930): машинобудування, електрична енергетика		IV (1930-1970): ДВЗ, енергетика вуглеводнів		IV (1970-2010): атомна енергетика, електронні комунікації		VI (теперішній): нано-, біо-, ядерокліти нні технології
Цикли Кондратьєва	I (1780/1790-1844/1851)			1841/1851 - 1890/1896		1890/ 1896-1939-1945	1939/1945-….				
Цикли Кондратьєва за В. Єфремовим	1785-1845			1846-1900			1901-1950		1950-1990	1991-2020	2021
Цикли Кондратьєва за І. Ліпсиц, А.Нещадін	1785-1835			1830-1890			1880-1940		1930-1990	1985-2035	

Рис. 2.7. Взаємозв'язок між науковими відкриттями, розробками та економічними циклами

(складено автором на основі [133; 134; 135; 206])

Вчені прогнозують, що наступна довгострокова хвиля Кондратьєва розпочнеться у 2020 році [5], а п’ята хвиля закінчиться у 2035 році, а нова розпочинається за 10 років до закінчення попередньої хвилі, тобто в 2025 році. Вже зараз відбуваються відкриття та впровадження біологічних технологій, з’являються нанотехнології, біо-, ядеро- клітинні технологій.

Технічний прогрес, важливість інноваційного розвитку та науки (як невід’ємної складової) посилює роль та значимість підприємств-постачальників електронних комунікцаійних послуг в сучасних умовах.

Як нами вже зазначалося, управління тісно пов’язане із умовами функціонування, сьогодні вони характеризуються невизначеністю, тому варто використовувати матрицю VUCA, щоб їх описати. Підприємства постачальники електронних комунікаційних мерж та послуг характеризуються інноваційністю, оскільки зміна технологічних укладів та індустрія вимагають появи нових послуг під інноваційні розробки та рішення. Сучасний підхід до управління теж трансформується під ці зміни, адаптується до умов невизначеності, враховуючи загальну картину змін внутрішніх та зовнішніх, стабільних та деструктивних.

Варто розглянути еволюцію зміни у поглядах щодо управління підприємствами на кожному етапі технологічних змін, які суттєво пришвидшуються: за останні 40 років індустрію 3.0 змінила 4.0.

Проаналізувавши промислові революції, робимо висновок про стрімкий розвиток технологій, починаючи із 1990-х років, наразі в галузі науки і техніки, активно досліджуються та розробляються квантові технології. Вважається, що вони вплинуть на всі без виключення галузі, сприятимуть розвитку нових бізнес-моделей, появі квантових обчислень та квантового зв’язку, такі компанії як “Amazon”, “Intel”, “Google” вже у процесі розгортання квантових технологій.

Динамічність вказує на пришвидшення інноваційних розробок та появу суперкомп’ютерів, у майбутньому креативну, цифрову економіку замінить квантова економіка (рис. 2.9), що грунтуватимется на квантових технологіях

та появі нових бізнес-процесів із квантовими обчисленнями, квантовими комунікаціями, квантових матеріалів.

<table>
<tr><td>Постквантова</td><td>-2020</td><td>Стрімкий розвиток технологій, нестабільність цифрового світу</td><td>Кіберспроможність *</td><td>Квантова економіка</td><td>з урахуванням екосистеми, керованої квантовими технологіями; безпека великих даних, квантових обчислень та квантових комунікацій</td></tr>
<tr><td rowspan="2">4.0.</td><td>2030</td><td rowspan="2">Нестабільність, коливання, невизначеність, множинність, мережевість, зміна цін, ефективність – корпоративна культура, цінність управління (як маржинальність)</td><td></td><td rowspan="2">Креативна, цифрова економіка</td><td></td></tr>
<tr><td>2020</td><td rowspan="3">життя – життя</td><td rowspan="3">з урахуванням невизначеностей VUCA; BANI, стейкхолдер-орієнтованість (на споживача, інвесторів, персонал); динамічне ситуативне управління</td></tr>
<tr><td rowspan="3">3.0</td><td>2010</td><td rowspan="3">Розгалуженість, несуттєві коливання та зміни, падіння цін, орієнтування на клієнта</td><td>Економіка знань</td></tr>
<tr><td>2000</td><td rowspan="2">Індустріальна епоха</td></tr>
<tr><td>1990</td><td>життя – робота</td><td>з урахуванням концепцій сталого розвитку (безпеки наступних поколінь)</td></tr>
<tr><td>2.0</td><td>1980</td><td>робота – життя</td><td rowspan="3">орієнтоване на отримання прибутку</td></tr>
<tr><td>1.0</td><td>1955</td><td rowspan="2">Поступовий розвиток, стабільність, орієнтованість на виробника та постачальника</td><td rowspan="2">робота – робота</td></tr>
<tr><td>Індустрія</td><td>1850</td></tr>
<tr><td>Індустрія</td><td>Роки</td><td>Характеристика</td><td>Мотивація</td><td>Економіка</td><td>Спрямованість управління безпекою</td></tr>
</table>

* авторська пропозиція

Рис. 2.8. Еволюція поглядів на управління безпекою підприємства зі змінами підходів до виробництва (промислових революцій*)*

(авторська розробка)

Рис. 2.9. Ключові складові квантової економіки

(узагальнено та складено автором за [392; 393])

Можемо припустити, що в постквантову епоху з'являться ризики та загрози критичній інфраструктурі, які масштабно впливатимуть на нашу спроможність контролю за квантовою поширеністю та її впливом за допомогою інформаційних технологій. Вважаємо за потрібне ввести поняття "кіберспроможності", як надспроможності (за рахунок наявних кіберможливостей підприємства) здійснювати контроль за бізнес-процесами у кіберпросторі за допомогою інформаційних технологій.

Підприємства мають бути інноваційними й відзначатися креативністю, гнучкістю, стійкістю, адаптивністю до стрімкого розвитку технологій.

Важливим елементом у формуванні інноваційного підприємства є нормативно-правове забезпечення. У Великобританії та Німеччині створили такі умови, що у структурі економіки пріоритетним є сприяння інноваційним підприємствам. Майже 50% програм країн ЄС передбачають політику у сфері

наукових розробок та технологій, свідченням цьому є низка рамкових програм, які являються основним інструментам фінансування науково-дослідних робіт (до прикладу – “Горизонт 2020: рамкова програма ЄС з досліджень та інновацій”).

“Горизонт 2020” – найбільша в історії Європейського Союзу програма, спрямована на фінансування досліджень та інновацій, із загальним бюджетом близько 80 млрд. євро, розрахованим на сім років (з 2014 по 2020 рр.). Вона прийшла на зміну 7-й Рамковій програмі ЄС з досліджень і технологічного розвитку (7РП), що діяла з 2007 по 2013 роки. У програму включено інструмент для підтримки малих і середніх підприємств, який Спрямований на всі типи інноваційних ініціатив для малих та середніх підприємств, які демонструють прагнення до розвитку, зростання і виходу на міжнародний рівень. В рамках таких проєктів надається поетапне фінансування повного інноваційного циклу, а також додаткові послуги з навчання та супроводу. Умови участі: мінімум одне комерційне мале або середнє підприємство, зареєстроване в країні-члені ЄС або країні, асоційованій з програмою “Горизонт 2020” [137; 138]. Програма передбачає єдиний набір спрощених правил і зводить до мінімуму багаторівневі паперові процедури оформлення документів.

Програма розроблена таким чином, щоб забезпечити простоту участі організацій у ній, першочергово для вищих навчальних закладів, підприємств не залежно від їх розміру та територіальної приналежності. Розробники програми підійшли до питань активізації інноваційних підприємств та інноваційної діяльності з правильного боку, а саме – фінансування, розуміючи, що нові продукти забезпечать високу конкурентоспроможність підприємств, високий попит на інноваційний продукт, створення нових робочих місць, збільшення податкових платежів і, як наслідок покращення рівня життя населення та отримання прибутків інноваційними підприємствам [330].

Отже, нормативно-правове забезпечення є важливою складовою у стимулюванні появи інноваційних підприємств та інноваційних розробок, що важливо для вирівнювання науково-технічних розробок країни до рівня науково-технічного прогресу [214].

Інноваційний процес підприємства включає: фінансування наукових досліджень, створення місць зустрічі для обміну досвідом між експертами та розробниками та науковцями, державну підтримку створення та ефективного функціонування елементів інноваційної інфраструктури у закладах вищої освіти, наукових установах та інших суб'єктах інноваційної діяльності [215].

Створення високотехнологічних підприємства передбачає стимулювання підприємств до наукових досліджень та науково-технічних розробок із залученням експертів, а також науковців, які проводять наукові дослідження в межах окресленої тематики. Крім того, активну участь має приймати держава, забезпечуючи підтримку суб'єктів інноваційного процесу через створення технологічних платформ як комунікаційного механізму для державного та приватного замовника інновацій; забезпечити спрощення звітності та зменшення розміру оподаткування на доходи фізичних осіб та оплату праці новоствореного малого інноваційного підприємства [363].

Як зазначалося в роботі раніше, важливим елементом у функціонуванні інноваційного підприємства в умовах нового технологічного укладу є нормативно-правове забезпечення. Вже зроблено вагомий крок у цьому напрямі – прийняття Кабінетом Міністрів України Розпорядження "Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030" від 10 липня 2019 року № 526-р [134; 138], в якому зазначається: "для сталого розвитку держави необхідно забезпечити сприятливі умови для утворення та функціонування інноваційно активних підприємств, розвитку національної інноваційної екосистеми, залучення вітчизняних та іноземних інвесторів".

Механізм взаємодії між суб'єктами інноваційного процесу з інноваційним підприємством має відбуватися таким чином, що держава

створює необхідні умови та інститути, що будуть займатися пошуком науковців та інвесторів у певні галузі, котрі зацікавлені в отриманні інноваційного продукту, якого потребує світ з урахуванням зміни технологічного укладу (рис. 2.10).

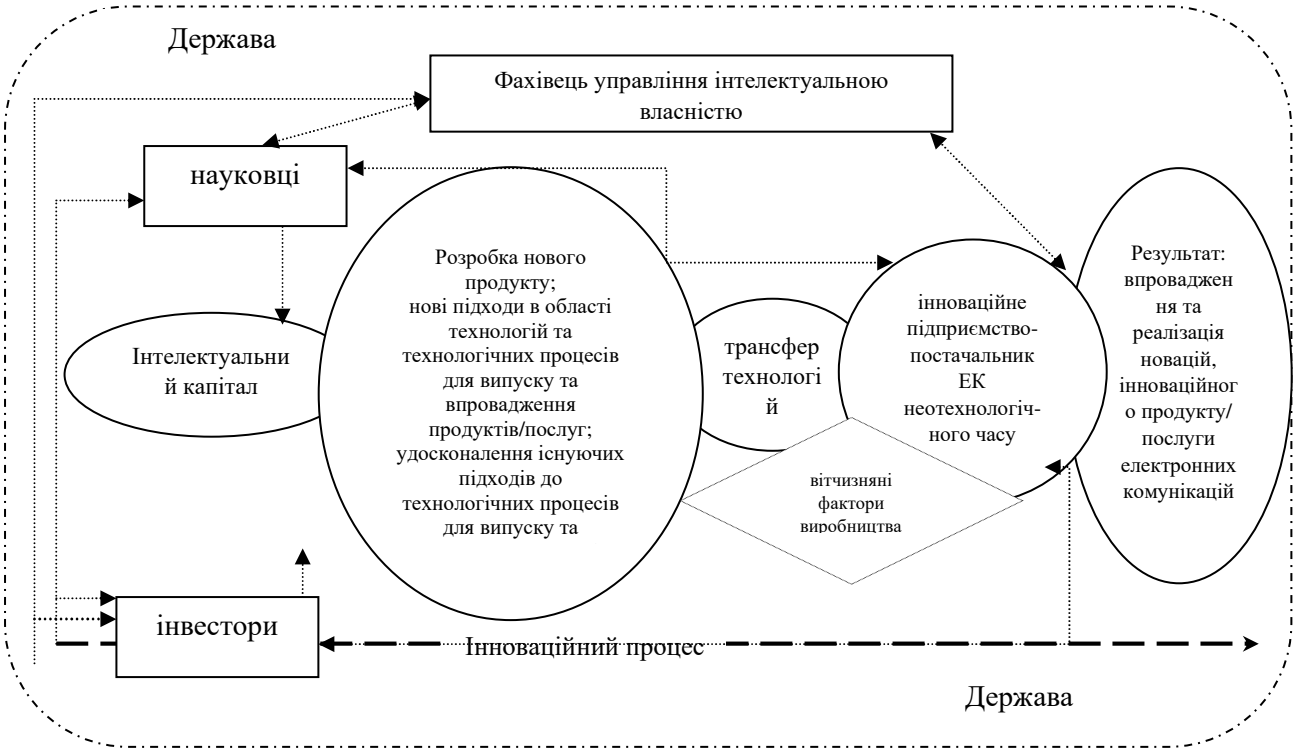


Рис. 2.10. Механізм взаємодії суб'єктів інноваційного процесу з підприємством-постачальником сфери електронних комунікацій

(складено автором на основі [139; 140; 133; 134; 135; 213])

Поєднання інтелектуального капіталу та інвестицій сприятиме більш швидкому продукуванню ідей та розробці нового продукту, або нового підходу до технології його випуску.

Паралельно має працювати фахівець з управління інтелектуальною власністю, котрий виконає формальну передачу прав на використання інноваційного продукту та можливість здійснення виробничих, а також комерційних операцій щодо інноваційного продукту.

Отже, інноваційне підприємство, у тому числі є підприємство-постачальник електронних комунікцаійних послуг, отримавши трансфер

технологій зможе виробляти та реалізовувати на ринку інноваційний продукт, якого вимагає сьогодення в умовах технологічних змін.

Усталений та тісний зворотній зв'язок між всіма суб'єктами інноваційного процесу забезпечить ефективну взаємодію елементів національної інноваційної системи з метою пришвидшення темпів економічного зростання та сприяння нових технологічних рішень, розробок в період нового технологічного укладу. В свою чергу, перехід до нового технологічного укладу відбуватиметься плавно, без значних втрат для економіки та затяжних криз, оскільки до нього готуватимуться завчасно всі учасники інноваційного процесу

Підсумовуючи, можна зробити висновок, що ключову роль у період нового технологічного укладу відіграватиме саме інноваційне підприємство, з яким тісно й активно співпрацюватимуть учасники інноваційного процесу для того, щоб забезпечити стабільне його функціонування й гарантоване отримання ним результату – розробки, впровадження та реалізації новацій, інноваційного продукту(послуги), технологічних процесів. Інноваційне підприємство, створене відповідно до умов нових технологічних процесів, допоможе вивести країну із категорії країн-споживачів інноваційних продуктів і перевести у категорію країн, що стабільно розвиваються, країн-лідерів, які є "донорами" інноваційних розробок та продуктів для світу.

Підприємства-постачальники електронних комунікаційних послуг в умовах високої діджиталізованості суспільства та посилення її в умовах невизначеності – воєнним станом, й переходом переважної більшості підприємств у безпечний он-лайн режим роботи, потребує захисту та, відповідно, управління безпекою підприємств. Потрібно враховувати й вимоги сучасності щодо технологій, послуг, яких потребують споживачі у відповідь на появу інноваційних розробок, додатків, щоб задовольнити потребу в їх користуванні [216; 217].

Площина безпеки підприємства змінюватиметься під дією новітніх відкриттів, розробок, інноваційних продуктів, прогресу та розвитку

суспільства. Підприємства є невід'ємною ланкою у функціонуванні економічної системи, тому неминучим є перегляд підходів, концепцій щодо безпеки підприємства, моделей управління нею, заходів захисту. Питання вже актуалізовано новими викликами технологічних змін, а також невизначеністю функціонування підприємств в умовах геополітичного напруження, тому наразі потребує глибинного вивчення та вирішення в найближчій перспективі.

Висновки до другого розділу

Сформована площина управління безпекою, включаючи цільові безпекові орієнтири та складові, перебуває під дією ризиків, загрози, невизначеностей, викликів, які є переумовами переходу підприємства із площини безпечного стану у небезпечний. Систематизовано поняття, що діють на безпеку, що сприяє їх чіткому розумінню й вчасному прийняттю рішення щодо доцільності заходів забезпечення безпеки досліджуваного підприємства в сучасних умовах.

У результаті етимилогічного аналізу понять "ризик" та "загроза" вдалося з'ясувати, що ризик є ймовірністю настання події, тому прийняття рішень відбувається гіпотетично, із можливістю множини варіантів прийняття рішень на основі передбачень розвитку подій. Загроза вказує на дію, яка відбувається, тобто підприємство відчуває коливання стану безпеки під дією деструктивних змін, тобто поняття не є тотожними, несуть різне смислове навантаження на безпеку підприємства та корелють із цільовими результатами безпеки. Від умов та середовища функціонування підприємства залежить ступінь їх впливу на стійкість підприємства: у визначеному середовищі ризики та загрози усуваються, як правило швидко через поінформованість щодо підприємсва, у разі невизначеності (низької поінформованості щодо середовища існуванні підприємтсва) – усуваються повільно, час на відновлення збільшується, висока вірогідність ліквідпції підприємства, що знову ж таки підтверджує стани перебування підприємства,

як безпечні та небезпечні. З'ясовано, що виклики, в залежності від ситуації та умов, можуть сприяти розвитку підприємства, а можуть стримувати його, одночасно виступають стимуляторами та дестимуляторами.

За результатами дослідження фрагментовано виразність ризиків та загроз безпекової площини у визначеному та невизначеному середовищі, як рушіїв небезпеки.

Відзначено, що підприємство, як складна система постійно пребуває в динамічному середовищі під дією впливів змін оточення, з'ясовано, що на кожній із стадій життєвого циклу підприємство зосереджується на різних питаннях щодо захисту: на стадії зародження – захист позиціювання та комерційної таємниці; на стадії зростання – розширення виробництва продукції та надання послуг; на стадії зрілості – на маркетингу, а саме представленні нових продуктів, використанні нових технологій; на стадії спаду – на фінансових аспектах, концентрується на збереженні ефективних напрямів діяльності.

З'ясовано, що еволюція підходів до виробництва змінює управління підприємством, так індустрія 1.0. та 2.0 передбачала орієнтованість на виробника та постачальника, безпека підприємства вбачалася узахисті прибутку, що втратило актуальність в епоху індустрії 3.0. та 4.0, коли розвиток технологій призвів до порушення стабільного отримання прибутків виробником без орієнтованості на вподобання споживача, четверта технологічна революція докорінно змінила направленість безпеки, котра зорієнтована на клієнтів, стейкхолдерів (захисті їх інтересів), врахуванні екологічної складової (сталий розвиток), що свідчить про динамічність та ситуативність управління.

Відмічено, що прослідковуються імпульси зародження постквантової епохи, відзначено потребу врахування зростання кіберзагроз через нестабільність цифрово світу.

Основні ідеї та наукові положення, презентовані у даному розділі,

викладені у публікаціях та працях [23; 204; 205; 206; 212; 213; 214; 215; 216; 233; 325; 331; 364]

РОЗДІЛ 3
МЕТОДОЛОГІЧНІ ЗАСАДИ УПРАВЛІННЯ БЕЗПЕКОЮ ПІДПРИЄМСТВА

3.1. Науково-онтологічний базис методології управління безпекою підприємства

Методологія є способом отримання наукових знань про процеси й явища, визначає шлях до отримання мети наукового дослідження, сприяє накопиченню інформативного матеріалу про об’єкт дослідження з метою аналізу та систематизації отриманих знань для збагачення існуючих понять та суджень новими власними умозаключеннями, на основі результатів опрацювання наукової інформації та фактів.

Методологічне забезпечення дослідження включатиме онтологічний базис, тобто понятійно-категоріальний апарат навколо об’єкта дослідження, та гносеологічній – пошук та виокремлення зв’язків у структурі категорій з описом та аналізом існуючих методів оцінки та управління безпекою підприємства.

Оскільки процес управління безпекою підприємства доволі складний, методологія накопичується з урахуванням нових поглядів, знань, умов, розвитку суспільства та трансформаційних змін. Управління, на нашу думку, є комплементарним поняттям, в якому варто поєднувати складові елементи, функціональні цеглини, оточення, загрози та невизначеності, тобто враховувати вміст площини безпеки для того, щоб здійснювати ефективний захист підприємства від небезпек.

Методична основа, що оновлюватиметься у відповідності до сучасних умов, дозволить боротися із проблемами, з якими стикаються постачальники

електронних комунікаційних послуг та дотримуватися правил забезпечення безпеки їх функціонування.

Нетрадиційно розглядає методологію управління економічною безпекою підприємства науковця Ляшенко О.М., якою пропонується використовувати методологічний полігон, який є взаємним перетином концепцій, теорій, підходів, принципів, методів та інструментів [49, с.137].

Важко не погодитися з тим, що методологія управління буде багатоаспектною, враховуватиме як базу теоретичні основи управління безпекою, тобто категоріальний апарат (сутність понять "безпека" та "управління", й далі накопичуватиме практичні аспекти) – інструментарій, підходи, концепт, методи, оцінку, моделювання, при чому мають забезпечуватися функції управління, як напрями діяльності суб'єктів (керуючої системи), якими конкретизуватимуться завдання та контролюватиметься їх виконання через отриманий результат.

Через високу поінформованість, доступ до глобальної мережі серед науковців посилюється когнітивність упередження. Вважається, що когнітивне упередження – це підсвідома помилка в мисленні, яка призводить до неправильної інтерпретації інформації з навколишнього світу та впливає на раціональність і точність рішень та суджень [142].

Проаналізувавши бачення когнітивності упередження у дослідженнях про безпеку [145-147] та при оцінці ризиків [147], прослідковується, що у першу чергу виникає упередження підтвердження, що знаходить відображення у бажанні інтерпретувати інформацію таким чином, що підтверджує попередні переконання чи припущення, ігноруючи інформацію, яка протилежна цим переконанням чи припущенням, що може призвести до нездатності розглядати альтернативні точки зору або підходи до безпеки.

Наступне упередження доступності, що проявляється у схильності занадто покладатися на легкодоступну або свіжу інформацію при прийнятті рішень, замість того, щоб розглядати всю релевантну інформацію. Це може

призвести до надмірного акцентування уваги на гучних загрозах безпеці, ігноруючи при цьому менш помітні, але все ще значущі ризики.

Часто у дослідженнях покладаються на інформацію, що отримана спершу, проте це зупиняє, ніби “якорить” при прийнятті рішень, ускладнює зміну подальших суджень, що призводить до надмірного акценту на початкових оцінках безпеки без урахування нових або мінливих загроз.

Далі стикаються з упередженістю через надмірну самовпевненість, коли переоцінені власні здібності або знання з одночасним недооціненням ймовірність негативних наслідків, що ймовірно спричинить нездатність підприємством належним чином підготуватися до потенційних загроз безпеці або до прийняття невиправданих ризиків.

Доволі часто прослідковується ефект масовості, коли переймаються переконання, поведінка, рішення, бачення за принципом переважної більшості дослідників та практиків.

Також прослідковується схильність піддаватися впливу за способом представлення інформації або обрамлення інформації, а не змісту самої інформації, так званому фреймінгу. Фреймінг може призвести до упередженості певних типів безпекових ризиків або рішень, виходячи з того, як вони представлені або надаються.

І, на останок, упередженість ретроспективного аналізу, що полягає у схильності переоцінювати свою здатність передбачати минулі події, вважаючи, що результати були більш передбачуваними, ніж вони були насправді. В свою чергу це потенційно призведе до нездатності враховувати події та наслідки з минулих інцидентів безпеки або до надмірної самовпевненості в майбутніх оцінках безпеки.

Вищеперелічених упередженостей варто уникати задля цінності проведення дослідження, достовірності, науковості, усвідомленості, новизни результатів як цілі дослідження управління безпекою підприємства. Саме тому варто переосмислювати усталені бачення щодо управління безпекою,

уникати “якорів” та когнітивних упереджень, формуючи нові перспективні погляди на проблематику під призмою невизначеності сьогоденних умов.

Розпочати варто із питання динамічності та статичності, бо безпека є станом, тому розуміння місцезнаходження його в динаміці чи статиці є першечерговим. Питання статичності станів в економічному сенсі досліджувалося Ф. Хоулі, який вважав, що економіці не притаманний статичний стан через зміни, які відбуваються на постійній основі [105, с.66]:

1) збільшення кількості населення;
2) зростання потреб суспільства;
3) удосконалення методів виробництва;
4) зміни підходів до виробництва (залишаються на ринку та функціонують ефективні підприємства);
5) збільшення капіталу.

Зазначене вище свідчить про зміни, які відбуваються у світі, а не лише на окремих територіях, що підтверджує динамічність та вказує на потребу адаптації до нових умов функціонування.

Паралельно із перетвореннями, змінами, глобалізаційними процесами, зміною технологічних укладів та технологій відбуваються рецесійні явища, що пов’язані із економічними кризами, циклічністю економіки, геополітичним напруженням, військовим станом в Україні. Підприємства відчувають коливання та втрату рівноваги у функціонуванні, особливо інноваційні, високотехнологічні, які потребують постійного оновлення та відповідності вимогам сучасності, часу. До таких підприємств належать підприємства-постачальники електронних комунікаційних мереж а послуг, які перманентно вирівнюються до технологічних змін та оновлень стандартів зв’язку. Це зумовлює пошук нових методичних підходів до управління безпекою підприємств, адаптації до динамічного та невизначеного середовища.

Наявність небезпек, реалізація загроз – звичне явище в сьогоденних умовах функціонування підприємств сфери електронних комунікацій.

Дворічна тривалість війни спонукає підприємства адаптуватися до змін, що викликані не лише внутрішніми чинниками впливу, а й волантильністю. Проактивність загроз посилюює кризові явища тому підприємствам варто накопичувати знання та поінформованість, підвищувати ситуативну обізнаність щодо безпекових заходів, імплементувати імперативи безпеки до управління та комплексно вирішувати. При підборі підходів, аналізі й оцінці, визначенні критеріїв та індикаторів, проведенні діагностики, формуванні механізмів або моделей управління безпекою слід уникати когнітивних упереджень, які можуть викривляти результати та впливати на концепт безпеки.

Напрацьований теоретичний базис, що розглядався у перших розділах використовуватиметься, як підґрунтя до обрання підходів та методів щодо управління безпекою підприємства. Адже аспекти дослідження управління безпекою базуватимуться саме на теорії та підкріплюватимуться можливістю практичного застосування. Теоретичний блок (безпека підприємства) містить категорії, визначники-маркери безпеки, елементи, чинники, суб'єкти та об'єкти дії, практичний блок – мету та завдання, критерії та індикатори, моніторинг ризиків та загроз, діагностику рівнів безпеки, механізм забезпечення (управління безпекою підприємства).

Узагальнено базис управління безпекою підприємства складатиметься із теоретичного та практичного блоків (рис. 3.1)

Оскільки базис управління безпекою підприємства має вибудовуватися першочергово з теоретичних напрацювань, слід підсумувати результати досліджень та узагальнити понятійний апарат формування площини безпеки.

Зважаючи, на погляди науковців, полеміку навколо поняття "безпеки" та їх обґрунтованість, вдалося виокремити вагомі погляди на безпеку, яка вбачається як: безпека в стійкості, безпека в платоспроможності, безпека в прибутковості, безпека у розвитку, безпека в конкурентоспроможності, безпека у гармонізації інтересів, що розглядатимуться як результати, які варто забезпечити у процесі управління.

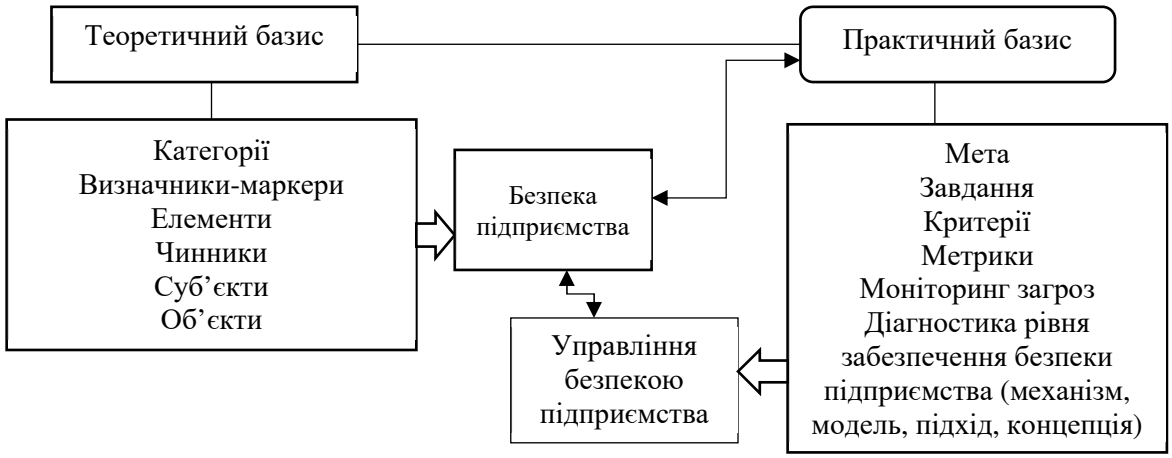


Рис. 3.1. Теоретико-практичний базис управління безпекою підприємства *(авторська розробка)*

Процес управління класично розглядається як вхід ресурсів та результат на виході, в управлінні безпекою підприємства, зважаючи на теоретичні напрацювання категоріального апарату "безпеки", погляди на безпеку та сенси, які вкладаються в розуміння поняття, дозволили сформувати онтологічний базис управління безпекою підприємства, що використовуватиметься в методології управління безпекою підприємства (рис. 3.2). Безпосередньо складові безпеки містять у собі ресурси, якими управляють. Ризики та загрози окреслюватимуться навколо стану безпеки й формуватимуть небезпеки підприємства, так само й чинники, умови невизначеності.

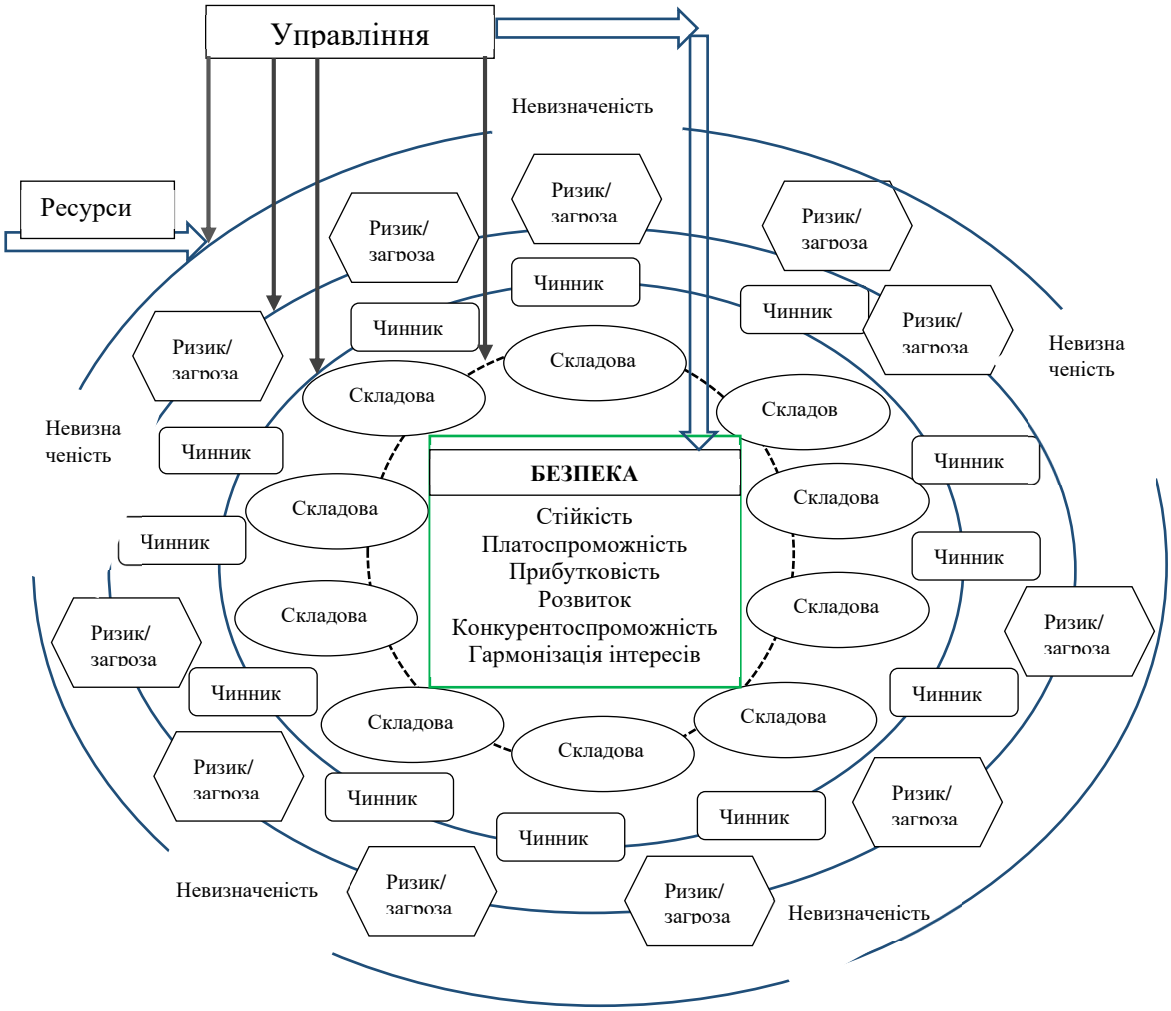


Рис. 3.2. Науково-онтологічний базис методології управління безпекою підприємства

(авторська розробка)

Інформованість щодо викликів, ризиків, загроз; розподіл явищ і процесів за напрямками: волантильність, невизначеність, складність, неясність; переосмислення дій та заходів безпеки в критичних ситуаціях; критичне та раціональне осмислення питання потреб інвестування в мінімізацію ризиків та загроз слугує базисом управління безпекою підприємства.

Управління безпекою підприємства націлене на спроможність чинити опір внутрішнім та зовнішнім загрозам, тим самим зберігати стійкість;

утримувати якісні параметри, забезпечуючи конкурентоспроможність; розвиток та зростання.

За результатаими дослідження нами запропоновано роглядати безпеку підприємства як стан, та з’ясовано, що усталено стійких станів у економіці не існує, тому господарюючі суб’єкти під впливом оточення, чинників не можуть зберігати перманентну безпеку, змінюють безпекову площину (стан безпеки), за ідентифікованими репелер та біфуркаційними точками. За теорією нестабільності (дисипативних структур), стан нерівноваги систем спричинює як порядок, так і безлад, що тісно пов’язані між собою. Нерівноважні системи створюють умови для виникнення унікальних подій і формування історії Всесвіту. Час стає невід’ємною константою еволюції, оскільки в нелінійних системах у будь-який момент може з'явитися новий тип розв'язання проблеми, який не зводиться до попереднього. Синергетичний підхід демонструє, як і чому хаос може виступати чинником творення, конструктивним механізмом еволюції, та як з хаосу можуть самостійно розвиватися нові форми організації. Таке бачення перетворює виклики, ризики, загрози підприємства у потенційні можливості – перебування у якісно новому стані безпеки за вдало та вчасно обраного підходу до управління [148].

Теорія дисипативних структур згадується у праці Й. Шіозави, яким висунуто припущення, що економіка має розглядатися не як рівноважна, а як дисипативна структура. Дане міркування вирізняється від традиційного сприйняттям економіки та економічних процесів у науковому світі.

За допомогою концепцій нерівноважної термодинаміки досліджено фінансові спекуляції та проаналізовано подібності та особливості дисипативної структури фінансової системи та нерівноважної термодинамічної системи для виявлення економічних та фінансових проблем [150].

Комплексність поєднання викликів, загроз, невизначеностей, що виникли в результаті дій країни-агресора проти України, як ніколи

актуалізують завдання щодо забезпечення безпеки господарюючих суб'єктів, розв'язання яких потребує вивчення наукової методології безпекових питань управління підприємством з урахуванням надскладних умов функціонування підприємств ПЕКМП.

Базисом для розуміння сутності поняття "безпека" слугували підходи: захисний, гармонізаційний, ресурсний, тому цілепокладання буде закладено як вектор руху до стану безпеки. Безпека нами вбачається через досягнення цілей підприємства, які відображатимуться як результат у: стійкості, розвитку, платоспроможності, прибутковості та рентабельності, конкурентоздатності досягненні цілей, захисті інтересів підприємства, стейкхолдерів та споживачів підприємства. Отже безпека є результатом копмозиції вхідних наявних ресурсів підприємства, якими виступають у нашому випадку складові, таким чином, що в результаті управління ними отримується стан за якого підприємство досягне свого цільового призначення. На нашу думку, саме цілепокладання той осередок, за якого буде досягнуто бажаного безпечного стану через результати:

по-перше, інтереси стейкхолдерів – гармонізація;

по-друге, підприємство фінансово незалежне та витривале за невизначених умов, здатне упереджувати ризики, протидіяти загрозам– стійкість, платоспроможність;

по-третє, ефективне та результативне – прибутковість, рентабельність;

по-четверте, перспективне, адаптивне, гнучке, сучасне, інноваційне – динамічно розвивається.

Проблематику інтересів стейкхолдерів глибоко досліджено Ляшенко О.М., інтереси представлено як параметр у принциповій схемі управління економічною безпекою підприємства. У монографії неординарно пірамідальну площину, яка складається із взаємоузгодження економічних інтересів стейкхолдерів зовнішнього та внутрішнього середовища й рівня взаємоузгодженості економічних інтересів внутрішнього середовища [51 с. 275].

В управлінні підприємством стейкхолдери відіграють особливу роль, прийняття рішень залежить від їх ставлення до ситуації, умов та бачення вирішення проблем. Стейкхолдери, як інвестори, зацікавлені у прибутковості, розвитку підприємства, оскільки не бажають втратити свої вкладення, намагаючись прийняти сторону підприємства у дискусійних питаннях з метою гармонізації взаємовідносин.

Графічна представлення бачення співставності результатів діяльності підприємства, як інтересу підприємства та інтересів стейкхолдерів через рівень їх задоволення, представлено на рис. 3.3.

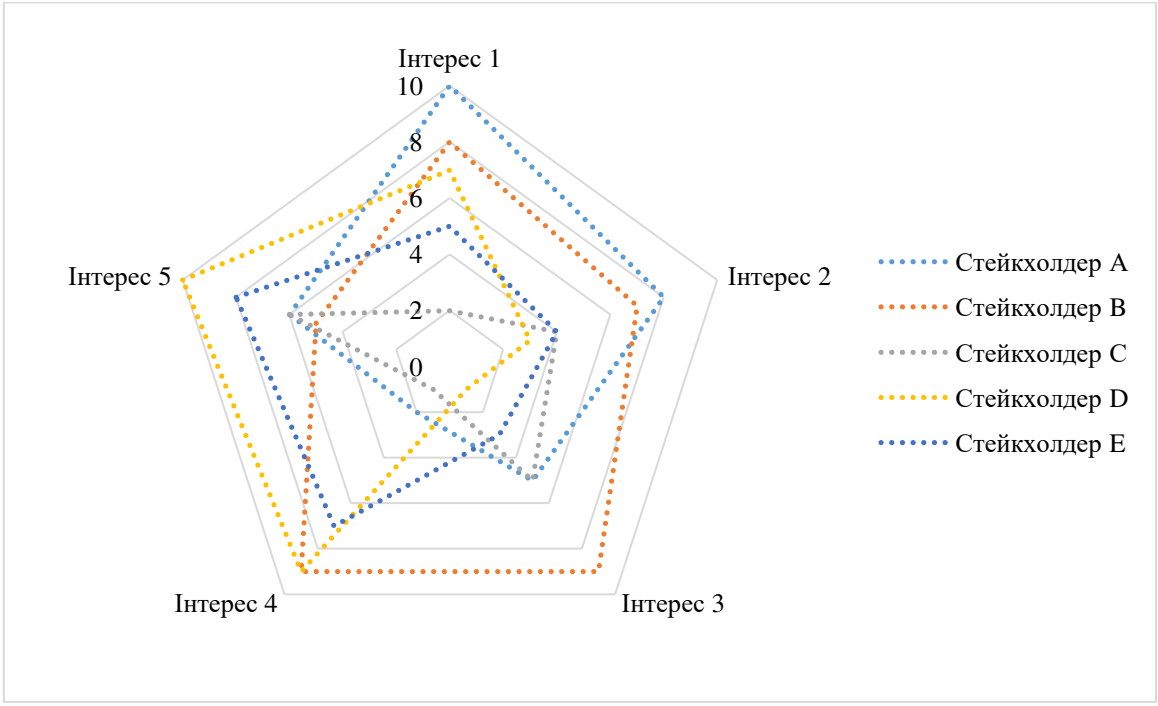


Рис. 3.3. Гармонізація інтересів стейкхолдерів і підприємства

(складено автором)

У теорії управління організацією традиційно виокремлюють внутрішні зацікавлені групи – власники підприємства, менеджери, персонал та зовнішні – конкуренти, інвестори, постачальники. Кількість та стейкхолдери різняться в залежності від розміру підприємства, специфіки, галузевої приналежності та описуються окремо для кожного підприємства.

Підприємства наразі стикаються з викликами невизначеності, які набувають різних форм прояву їх дії, інколи позитивних, коли спрацьовує ворунка можливостей, а зазавичай негативних – збитках, деструктивних змінах, уповільненні розвитку або ж, у найгіршому випадку – ліквідації підприємства.

За таких умов підприємства мають бути гнучкими, стійкими, витривалими, адаптуватися до мінливого та загрозливого середовища, управління переходить у ніби захисний режим перетворюється у превентивне, антисипативне, адаптивне, антикризове.

Перевентивне управління (походить від англ. “preventive management”) пов’язане із передбаченням появи ризиків або вчасної їх нейтралізації, тобто є підходом, спрямованим на запобігання ризиків до їх появи за рахунок заходів попередження негативних наслідків дії ідентифікованих ризиків.

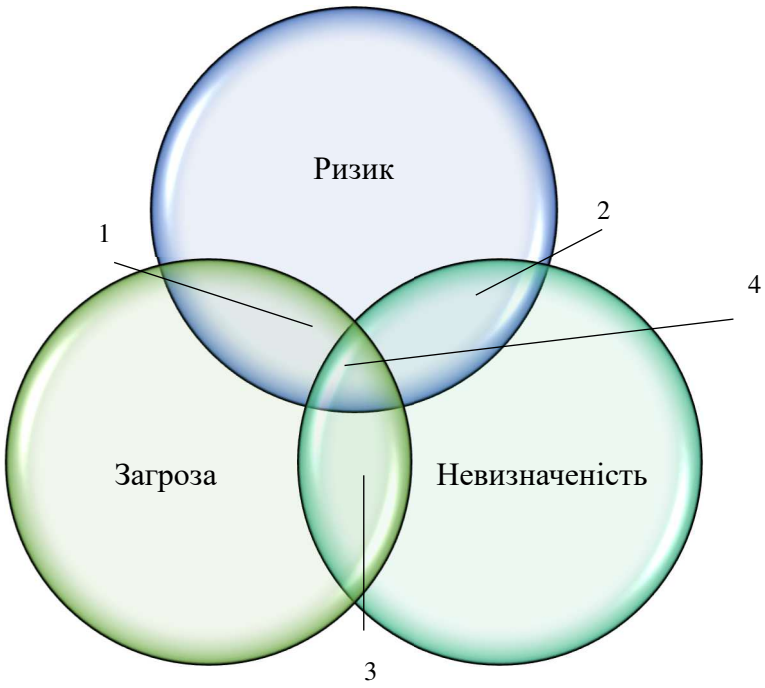
Антисипативне управління заточене на виявлення загроз, точніше передбачає завчасне розпізнавання загроз підприємства з пропозиціями завчаснх дій щодо їх локалізації [179]. В економічній енциклопедії за редакцією Мочерного С.В., “антисипація” трактується як передбачення можливого розвитку подій, або ж передчасне настання певного явища [180, що відображає суть антисипативного підходу.

Адаптивне управління – гнучкий, здатний пристосуватися до мінливих (нових) умов у екзогенному та ендогенному середовищі підхід, завдяки застосуванню нових інструментів, методів управління [181179 с. 123].

Превентивне, антисипативне, адаптивне управління – відповідь на турбулентність умов функціонування підприємств, динамічність розвитку технологій, засобів передачі інформації, стандартів зв’язку, тому найчастіше застосовується в антикризовому управлінні, при потребі уникнення ризиків та усунення наслідків дії загроз.

Мінливість та непередбачуваність середовища окреслює наступний елемент в площині безпеки – невизначеності, виклики, загрози. Сукупно вони посилюють дію один одного, утворюють силу, спричинену синергетизмом їх

поєднання, що матиме потужніший вплив на безпеку підприємства та переводитиме його у відповідний стан. Синергетизм турбулентності середовища перетину “ризик-загроза-невизначеність” представлено на рис. 3.4.



1, 2, 3, 4 – перетин “ризиків-загроз-невизначеностей”

Рис. 3.4. Синергетизм турбулентності середовища на перетині “ризиків–загроз–невизначеностей”

(авторська розробка)

Станів безпеки, нами було розглянуто у розіділі 1 роботи та запропоновано окреслити їх за відрізками руху у площині: (-1) – незначний стан небезпеки; (-2) – передкризовий стан небезпеки; (-3) – кризовий стан небезпеки; (- 4) – критичний стан небезпеки. У відповідності до перелічених станів ідентифікуються наступні варіанти поєднання ризику з невизначеністю або із загрозою та загрози із невизначеністю:

перетин 1 (ризик і загроза);

перетин 2 (ризик і невизначеність);

перетин 3 (загроза та невизначеність);

перетин 4 (загроза, ризик, невизначеність).

За теорією нестабільності чим менша сума впливів на об’єкт або процес у момент біфуркації складноорганізованої системи, тим більший кінцевий синергетичний ефект. Синергетичне міркування щодо управління спрямовує до оцінки та прийняття рішення через прямолінійне порівняння висхідного та наступніх станів (реальна оцінка ситуації із імовірним розвитком подій за прийнятого управлінського рішення).

Для ефективного застосування синергетичного підходу необхідно: а) виділити та схарактеризувати (у поняттях формальної логіки) складну систему або процес, що потребує синергетичного впливу; б) дослідити стратегію розвитку системи, описати можливі рівні її вільності, тобто рівноможливі напрями і шляхи її розвитку; в) здійснити факторний аналіз можливих шляхів самоорганізації системи або процесу; г) визначити мету або бажаний результат (у яких конкретно аспектах необхідно змінити стан певної системи); д) розробити номенклатуру (перелік) слабких впливів, що сприятимуть самоорганізації хаотичної системи, а також тактику їх застосування; е) правильно визначити критичний момент біфуркації досліджуваної системи [178].

Так як сила дії змінюється в залежності комбінацій ризиків, загроз, невизначеності, вважаємо за необхідне відмітити дотичність ризиків, загроз, невизначеностей та окреслити точки їх перетину, як дестабілізуючі. Перехід підприємства у новий стан безпеки у результаті управління безпековою площиною підприємства, ідентифікованою за репелер та біфуркаційними точками наведено на рис. 3.5.

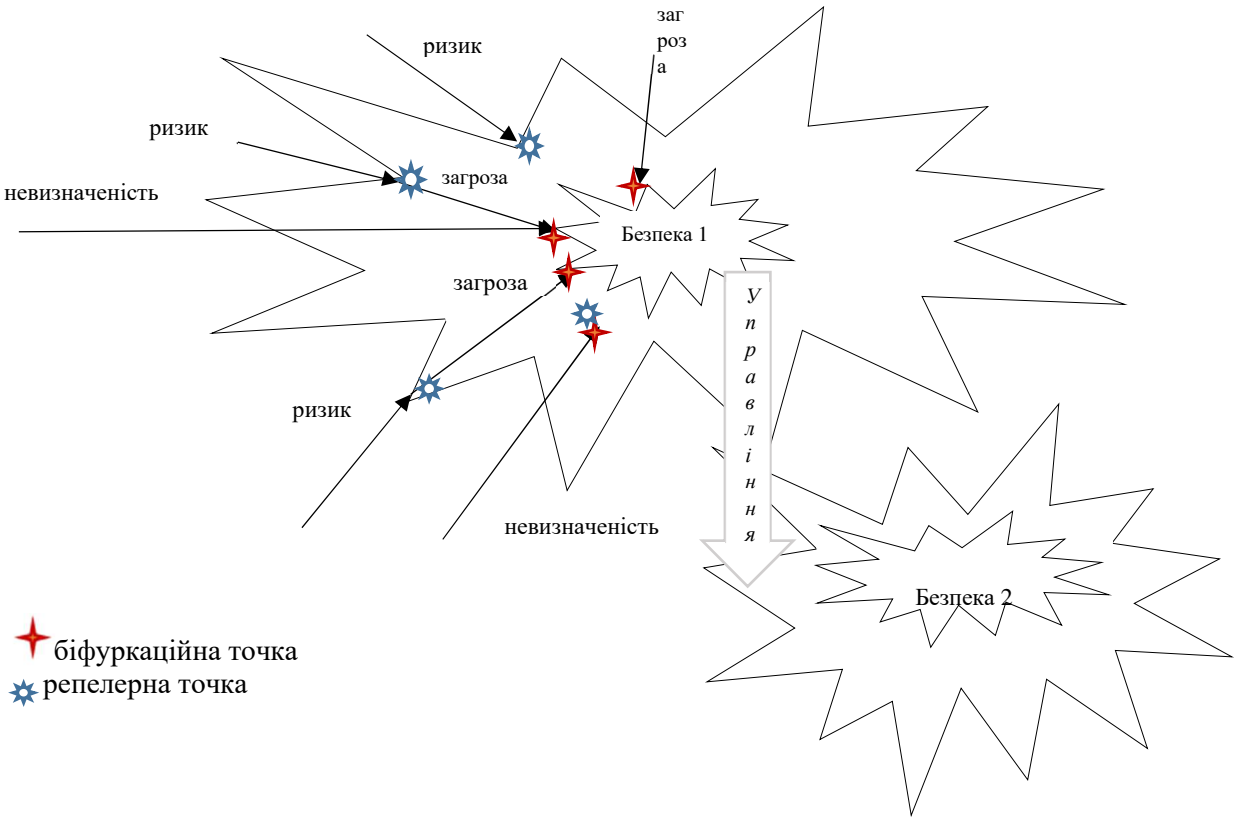


Рис. 3.5. Перехід підприємства у новий стан безпеки у результаті управління безпековою площиною підприємства, ідентифікованою за репелер та біфуркаційними точками

(авторська розробка)

Місцерозташування біфуркаційної точки – перетин ризиків та загроз; ризиків, загроз та невизначеностей, а також окремої дії загроз. Під відокремленою дією ризиків або невизначеностей утворюється репелерна точка. Ідентифікація даних точок важлива для визначення швидкості настання несприятливих подій або наслідків для підприємства. Швидкість реагування на зміни, які відбуваються після переходу у точки впливає на масштаб змін та стратегію і тактику управління підприємством.

Нами приділено увагу ризикам, загрозам, невизначеностям саме через воєнний стан, в якому перебуває впродовж майже двох років наша держава, тому включено даний блок в методологію управління.

Назви для дестабілізуючих точок запропоновані після низки опрацьованих джерел, в яких згадувався адаптивне, антикризе, антисипативне, адаптивне управління, проте, найбільш вдалими виявилися напрацювання в області математики, а саме: нестійкості та нелінійності як джерела невизначеності економічних процесів, в якій досліджуються поведінки систем [183, с.49]. Відзначаються стани: стаціонарності, стійкості, нестійкості і визанчають точки збурень та спокою.

Стійка точка – це точка, в межах якої жоден рух не виходить за межі допустимих відхилень, називається атрактором. Нестійка точка навпаки з'являється, коли рух не досягає області стійкості в межах заданих вищезгаданих допустимих значень та має назву репелер. Точці біфуркації характерна нестійкість стану системи, в якій поводження системи стає неоднозначним.

Саме ці точки фігуруватимуть у методологічному базисі управління безпекою підприємства для ідентифікації зміни процесів та системи, фіксуватимуть траєкторії руху змінних параметрів.

Наступним в управлінні безпекою підприємства пропонується блок – складові безпеки, який буде найбільш громістким при проведенні аналізу. Результати діяльності залежать саме від складових, які співставні з ресурсами, тому впливають на стійкість, здатність до розвитку, платоспроможність, конкурентоспроможність, інтереси стейкхолдерів, прибутковість та рентабельність [314; 332].

Під час управління підприємством комплементуються показники безпеки та можуть відностися до окремих.

Композиція складових та показників оцінки безпеки в процесі управління безпекою представлена на рис. 3.6.

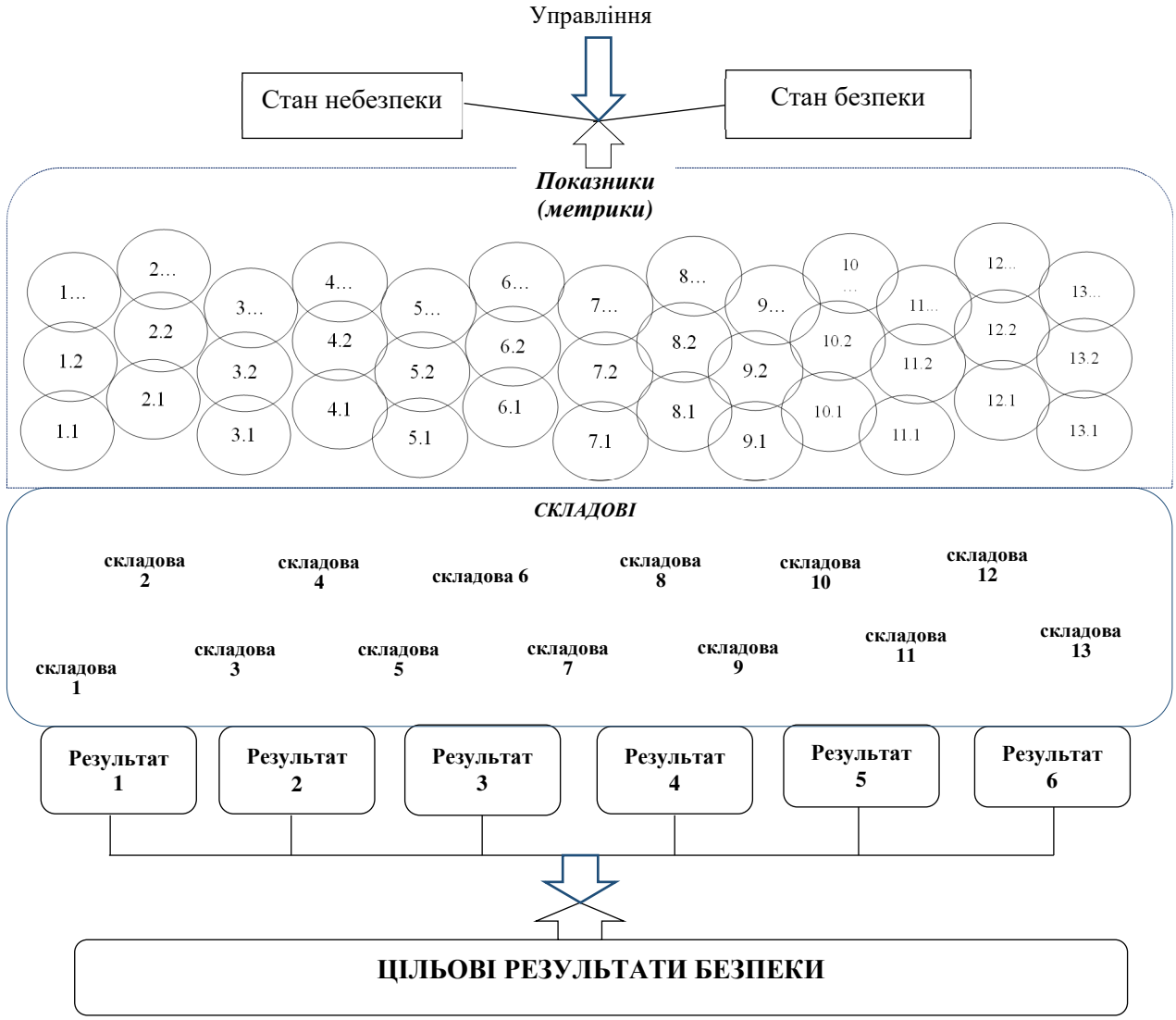


Рис. 3.6. Композиція складових та показників оцінки безпеки в процесі управління

(авторська розробка)

Цільові результати є орієнтиром для стану безпеки підприємства, в залежності від комбінацій складових та їх значень приймаються рішення щодо збалансованості показників в межах прийнятності для забезпечення результатів безпеки (здатність до розвитку, стійкість, платоспроможність, прибутковість та рентабельність, конкурентоспроможність та гармонізаціія інтересів).

До кожного результату обиратиметься складова, яка включає в себе підскладові (метрики), що вираховуватимуться, оцінюватимуться й аналізуватися для виміру безпеки через їх критеріальні значення [325]. Відповідно за показниками, встановленими для них межами, визначатиметься стан безпеки через відрізки безпеки, що описуватимуть стан безпеки з метою подальших рішень щодо управління безпекою підприємства.

Зважаючи на складові, які нами було виокремлено (інтелектуальна та кадрова; ринкова; політико-правова; техніко-технологічна; інтерфейсна; виробнича; фінансова; фізична (силова); електронно-комунікаційна; екологічна; інформаційна; інноваційно-інвестиційна; енергетична), їх варто об’єднати за принципом приналежності до цільових результатів безпеки, що сприятиме чіткому підбору показників, прийнятних для аналізу й оцінки.

Обрані складові окреслюються навколо результатів, що задовольнятимуть вимоги до безпечності функціонування підприємства, як цілі. Виробнича складова характеризує виробничі можливості підприємства, у сфері послуг, зокрема спроможність якісного надання електронних комунікаційних послуг. Так як результатами управління є забезпечення конкурентоспроможності та задоволеності інтересів стейкхолдерів, варто приділити увагу їх потребам, а також потребам ринку, оточення, для яких якісний зв’язок та розгалуженість мережі для підключень відусюди відіграватиме провідну роль.

Вважається, що саме виробнича функція є однією із основних та вагома в операційній діяльності підприємства. Сукупність наявних ресурсів та технологій виробництва характеризує виробничі потужності підприємства, а саме – можливості щодо максимального виробництва товарів або послуг, виконання робіт.

Виробнича безпека забезпечується діями персоналу щодо захисту процесу виробництва за експлуатації виробничих потужностей, засобів, технологій, результатом використання яких є роботи, продукція, послуги [184, с. 111].

Об’єктом захисту виробничої безпеки виступає продукція, роботи або послуги, що відповідають якісним та вартісно-ціновим характеристикам.

На нашу думку, техніко-технологічна складова включає виробничу, енергетичну, силову (фізичний захист, охорона праці), а також може доповнюватися інноваційною та екологічною.

Розглядаючи окремо технічну складову, пов’язуємо її із захистом процесу виробництва та надання посуги шляхом безперебійного забезпечення енергетичними ресурсами, устаткуванням, приладами, обладнанням, будівлями, спорудами, машинами, технікою для інформаційного обігу документацією та зв’язку.

Технологічна складова має забезпечувати відповідність технологій виробництва та надання послуг підприємства етелонним світовим практикам за умові зниження витрат та оптимаціції процесів при використанні цих технологій, характеризує технологічний процес. Звісно, що організація технологічної безпеки сприятиме відслідкуванню прийнятних, економічно вигідних, високопродуктивних, інноваційних технологій, що убезпечитть підприємство від росту витрат, високої енергоємності, зниження продуктивності та якості через моральне старіння основних засобів.

Досліджуючи функціональні складові безпеки інтегральної промислової структури, Чорна О.Ю техніко-технологічну складову визначає як ступінь відповідності застосовуваних на інтегрованій промисловій структурі технологій найліпшим світовим аналогам за оптимізації витрат ресурсів [188, с. 188].

Прогресивні технології, новітні розробки та засоби сприятимуть підвищенню не лише прибутковості (за рахунок високопродуктивності, енергозбереження), а й конкурентоспроможності через зниження ціни, підвищення якості продукції та надання послуг [329].

Енергозбереження – виклик сьогодення, крім того, сталий розвиток суспільства та “зелена” економіка стали поштовхом до переходу на ощадливі

енергоносії еко-виробництво, безвідходне виробництво (“zero-waste”), переглят технологічний процесів та використання технологій.

Таким чином, можемо зробити висновок, що в сьогочасних тенденціях екологічного виробництва та надання послуг, екологічна безпека пов’язана із технологічними процесами підприємства, а також інноваційно-інвестиційними процесами й енергетичною складовою.

На думку Матвійчук Н.М., Коленди Н.В, Сирочук С.В., енергетична безпека є станом технічно надійного, стабільного, якісного, достатнього та екологічно прийнятного забезпечення підприємства всіма видами енергії за економічно вигідною ціною, а також ефективне використання енергетичних ресурсів в процесі господарської діяльності [187, с. 18].

Актуальним на сьогодні є визначення, надане Надтокою Т. та Амельницькою О.: “Енергетична безпека – ступінь захищеності його енергопостачання від загроз в умовах нормального функціонування з урахуванням перспективи розвитку, а також ступінь енергозабезпечення мінімально необхідних потреб в енергії в надзвичайній ситуації” [186, с. 18].

Вважають, що інноваційний розвиток підприємства тісно пов'язаний з економічною безпекою Перерва П.Г та Романчук Т.В., стверджуючи, що чим більше прогресивних технологій, тим вищі показники економічної безпеки [192, с.57].

Інновації – інструмент підвищення рівня техніко-технологічної безпеки та конкурентоспроможності та стійкого розвитку підприємства, інноваційна безпека виступає рушієм для якісної трансформації підприємства, а також поліпшення матеріально-технічної бази й результатів діяльності.

Фізична (силова) складова вбачається у безпеці капіталу, майна, комерційних інтересів, персоналу (силові та моральні впливи). Варто зазанчити, загрози здоров’ їх здоров'ю, фізичному та психологічному, негативно впливають на імідж, репутації компанії, порушують стабільність.

Зайченко К.С. вважає, що негативні дії на підприємстві спрямовані в бік персоналу призведуть до зниження вартості його активів, втрати економічної незалежності [194].

Варто наступною складовою розглянути інтелектуально капіталу, яка є станом захищеності інтелектуального капіталу та інтелектуального потенціалу для забезпечення нормального функціонування та розвитку підприємства на всіх рівнях менеджменту, а також удосконанлення кадрового потенціалу, формування належних, безпечних, ергономічних умов праці [197; 192, 198]. Слід додати, що підприємство має дбати про захист кодифікованих та некодифікованих знань, розглядати інтелектуальний капітал на рівні із фінансовим.

Фінансова складова є вагомою для безпеки підприємства, впливає на прибутковість, розвиток, платоспроможність, стійкість, інтереси, конкурентоспроможність, адже фінансові ресурси та забезпеченість ними слугують базисом виробничої діяльності, а отже операційної без якої не можливо отримати послугу, виготовити продукцію.

Кравчик Ю.В, Каткова Т.І., вважають, що більшість загроз виникають через низьку ліквідність та платоспроможність, порушення фінансової стійкості й структури активів і капіталу [195, с. 86], що підтверджує вплив даної складової на безпеку підприємства.

Інформаційна складова відповідає за інформаційну інфраструктуру підприємства, протидію поширенню неправдивої інформації, негативному інформаційно-психологічному впливу. Об’єкт – інформація підприємства підлягає захисту під час документообігу від несанкціонованого доступу, руйнування, модифікації, розкриття при її переміщенні.

Інформація в Законі України “Про інформацію” визначена як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Підприємство у господарському процесі використовує економічну, ділову, стратегічну та оперативну,

зовнішню та внутрішню інформацію. Інформація може бути відкритого та обмеженого доступу, закритою, конфіденційною тощо [341].

Інтерфейсна складова безпеки виконує функцію запобігання, подолання загроз підприємству з боку контрагентів та персоналу, пов'язана із виробничою безпекою (надійність взаємовідносин з постачальниками); ринковою (надійність комунікації із клієнтами; фінансовою безпекою (надійність оточення на предмет фінансових питань); кадровою (надійність відносин із персоналом); інформаційної (репутація) [185; 226; 227; 228, с.167].

Переходячи до наступної складової, можемо виокремити приналежну до зовнішнього оточення підприємства, проте не менш важливу, політико-правову складову, що підтверджують напрацювання, зокрема Тертичної Л.І., Безпалко О.В. та Рибак Н.О, якими запропонована концепція управління політико-правовою безпекою підприємства, а сама складова розглядається як дотримання чинного законодавства, правового забезпечення діяльності, захист від надмірного податкового тиску, правової захищеності підприємства та його персоналу [188, с.118].

Ринкова складова безпеки, подібно виробничій, характеризує рівень відповідності нормативним значенням, тільки не виробничим параметрам, а ринковим. Ринкова складова економічної безпеки вказує на ступінь відповідності можливостей розвитку всередині підприємства зовнішнім ринковим трендам, які вимагаються середовищем, а також на надійність, захищеність позицій підприємства на ринку. Кузьомко В.М. вважає, що прибутковість досягається через моніторинг кон'юнктури ринку, оцінку ринкових сил у галузі, окремому сегменті, врахуванні потреб клієнта, надаючи складовій другу пріоритетність з-поміж інших [200, с. 212].

Приналежність до результату безпеки складових відображає складова ємність цільових результатів управління безпекою підприємства, яку нами складено за результатом опису складових, їх суті (рис. 3.7)

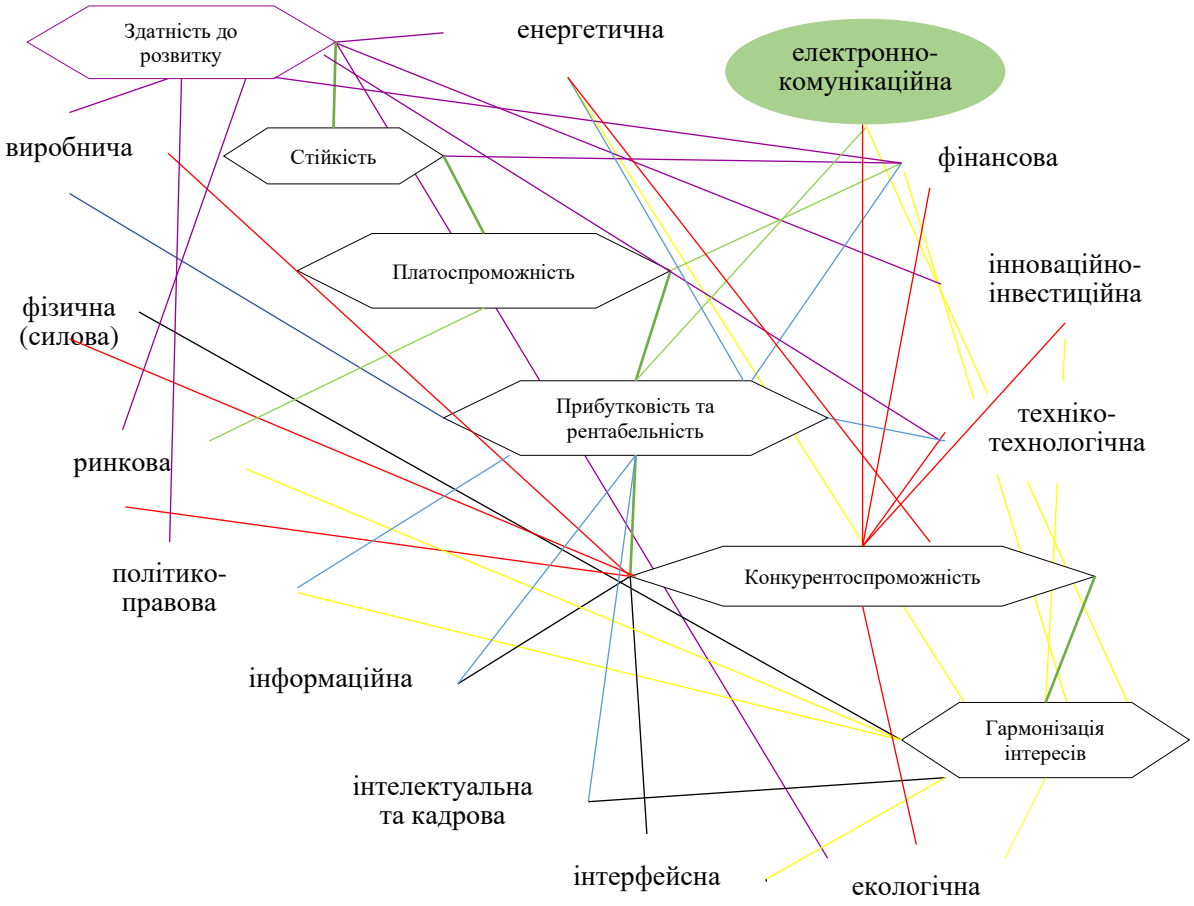


Рис. 3.7. Мережева складова ємність цільових результатів управління безпекою

(авторська розробка)

Електронно-комунікаційна складова запропонована нами як відповідь на виклики діджиталізації суспільства, цифровізації економіки, зростання значення та ролі послуг ЕК для підприємств, населення в період пандемії та воєнного стану (доцільність введення складової була доведена нами у розділі 1 роботи). Тому варто посилити увагу до інформаційного ресурсу та його захисту не тільки від інформаційних атак, але й кібератак, які паралізують роботу підприємств ПЕКМП, й автоматично всіх клієнтів – підприємства, державні структури, населення.

Характеристики складових дозволять нам визначитися із вагою складових по відношенню до результатів, встановити приналежність до результатів, яких треба досягти для гарантування безпеки.

3.2. Концепт траєкторії площин станів безпеки підприємства

Попри актуальність розгляду питань щодо управління, постійний інтерес до нього з боку дослідників, соціально-економічний прогрес вимагає нових поглядів та підходів до управління. Причиною є множинність векторів руху, відмінність у темпах розвитку та швидкість адаптації підприємств до умов невизначеності, що спрямовує дослідження у бік розгляду управління як динамічного процесу.

Економічна динамічність та перехід від індустрії 4.0 до 5.0, зважаючи на характер та швидкість технологічних змін, скорочення тривалості часу переходу від одного технологічного періоду до іншого, вказує на те, що на сьогодні економіка трансформується, їй типова інверсійність. Наразі ми говоримо про глобальні перехідні процеси, але аж ніяк не про статичність, за якої кожен окремий чинник виробництва забезпечував (покривав) те, на що його було витрачено, тобто на що було спрямовано виробництво.

Сфера послуг електронних комунікацій характеризується інноваційністю, розвиток її відбувається паралельно із технологічними змінами та соціально-економічним прогресом. Соціально-економічний прогрес стрімко перейшов у новітню епоху інформатизації, коли знання та освіта відграють ключову роль у формуванні особистості та світогляду. Потреби в обізнаності, поінформованості, перебування на зв’язку формують новий щабель потреб, як нами вже було відзначено, в електронних комунікаційних послугах (модернізована піраміда потреба).

Науковцями пропонується широкий спектр наукових підходів до оцінювання, управління економічною безпекою підприємства, в основу яких, на нашу думку, покладено загальні підходи до управління підприємством, такі як: функціональний підхід; процесний підхід; системний підхід; ситуаційний підхід.

Функціональний підхід тісно пов’язаний із формуванням основ менеджменту як науки у відповідь на промисловий розвиток та збільшення

обсягів виробництва, появи корпорацій, акціонерних товариств, а саме із адміністративним менеджментом.

Із становленням менеджменту як окремого наукового напрямку, класично виокремилося три області:

– науковий (Ф.У. Тейлор, Г. Ґант, Ф. Гілбер), напрям акцентував увагу на отриманні результатів через наукового обгрунтовану організацію виробництва);

– адміністративний (А. Файоль, М. П. Фоллет), за яким загалом розглядалася організація та приділялася увага функціям управління: планування, організація, командний ланцюжок, координація та контроль);

– концепція бюрократичних організацій (М. Вебер), за якою визначалися посадові обов'язки, відповідальність працівників, велася звітність, розділяися окремо власність та управління, що мало вибудовуватися на принципах раціональності.

Засновник класичної адміністративної школи управління А. Файоль розглядає управління як процес, що складається із взаємопов'язаних функцій, що слугувало базисом теорії управління організацією вцілому.

У праці Безгіної К.С., Гришиної І.В. [171, с.4], А.Файоль вважається засновником процесного підходу, проте суперечить теорії, за якою управлінець розглядає функції як незалежні одну від іншої, а сучасний процесно-орієнтований підхід розглядає функції підприємства у взаємозв'язку.

Функціональний підхід полягає у взаємозв'язку всіх функцій управління, таких як: планування, організація, мотивація та контроль, через які задовольняються потреби. Підхід орієнтовананий на результат – задоволення потреб, а також об'єкти управління, сприяє та надає підприємству можливості покращити організаційну структуру, принципи роботи.

Проте вважається, що управління з використанням функціонального підходу не орієнтує підсистеми підприємства на досягнення кінцевого результату загалом усією організацією [159, с.174].

Черноівановою Г.С., на основі попередніх опитувань, проаналізовано відсоток згадувань серед науковців інших функцій, окрім класичних функцій управління за А.Файолем, так, близько 38,5 % вчених використовують функцію координації та 27% – функцію регулювання [160].

З часом функціональний підхід втратив популярність через зниження ефективності використання, тому зазвичай, обраючи його науковці поєднують підхід із іншими, найчастіше із структурним. Проте, на думку, Хринюк О.С., Солосіч О.С., даний підхід може успішно використовуватися як складова частина системного підходу при формуванні елементів системи забезпечення економічної безпеки [172, с.89].

З огляду на інноваційність підприємств Ареф'євою О.В. запропоновано використовувати компетентістно-функціональний підхід до управління, яким фіксується цілеспрямованість у підтримці пріоритетів та універсальність використання знань через компетенції функцій управління, орієнтованість на які зумовлює потребу в застосуванні адекватних інструментів аналізу (метод експертних оцінок), що дозволяє здійснювати оцінку якісних характеристик об'єкта [158, с.10]. Функціональний підхід до забезпечення конкурентоспроможності підприємств призначений для дослідження ефективності виконання функцій, що мають місце в процесі господарювання у зв'язку з чим оптимальним інструментом аналізу є функціонально-вартісний підхід. Маючи на меті підвищити ефективність функціонування підприємства, формулюються завдання орієнтовані на скорочення витрат, стимулювання збуту продукції, оптимізації тривалості операційного та фінансового циклів.

Після втрати ефективності управління за використання функціонального підходу на заміну йому прийшов процесний підхід, набувши поширення на початку 80-х років XX століття. Сутність підходу

полягає у розгляді кожної управлінської функції як процесу, який є загальною сумою усіх функцій. Підхід зазнавав змін у результаті індустріалізації, а саме:

– на доіндустріальному – опис процесів виробництва задля виробництва високоякісної продукції;

– на індустріальному – управління підприємством, організацією задля ефективності системи управління;

– на постіндустріальному підхід – мережа, що включає бізнес-процеси, пов’язані із цілями та місією підприємства, організації.

У нинішніх умовах за даного підходу управління діяльністю організації здійснюється через мережа бізнес-процесів, пов'язаних із цілями та місією функціонуючого суб’єкта господарювання.

Процес – це пов’язаний набір повторюваних дій (функцій), які перетворюють вхідний матеріал і (або) інформацію в кінцевий продукт (послугу) відповідно до попередньо встановлених правил [151] .

Для підприємств бізнес-процес є невід’ємною складовою його функціонування, тому трактувань поняття доволі багато, серед них привертає увагу визначення надане Виноградовою О.В., якою бізнес процес розглядається як циклічна сукупність взаємопов’язаних завдань (дій), що мають певні входи (необхідні ресурси) і виходи (результат), що є цінністю для споживача (внутрішнього або зовнішнього) [153].

Діяльність організації у процесному підході сприймається як сукупність (мережа) бізнес-процесів, що дотичні (пов’язані) із цілями, та місією підприємства.

Управління свого часу М. Портер розглядав як ланцюг з бізнес-процесів, який містив:

– основні бізнес-процеси (операційний менеджмент: ідентифікація потреб споживача; розробка дизайн-проєкту продукту, виробництво товару(послуги); продаж товару (послуги), доставка, обслуговування, сервіс гарантійного обслуговування);

– бізнес-процеси підтримки (ресурсний менеджмент: управління людськими ресурсами; управління фінансовими ресурсами; управління матеріальними ресурсами);

– бізнес-процеси керування (стратегічний менеджмент: управління інформаційними ресурсами).

Варто зазначити, що процесний підхід зосереджується на якості, витісняючи зосередження підприємства виключно на результатах діяльності – прибутках. Підвищення якості продукції залежить від споживчого бачення продукту або послуги, що спонукає підприємство дбати про якісні харакетеристики послуг та вдосконалювати організацію управління під якісну орієнтованість.

З метою розробки механізму управління економічною безпекою підприємства розглядається процесно-функціональний підхід, що враховує ієрархію та відповідальності, взаємоузгодження процесів та взаємодій, які виникають усередині функцій. Хринюк О.С. та Солоніч О.С. вважають: “процесно-функціональний підхід зберігає процесну спрямованість та сукупність організаційних механізмів регулювання та контролю (особливості розподілу відповідальності, регламенти, стандарти, система документування, оптимізаційна орієнтованість), водночас підсилюючись характерними функціональному підходу просторово-функціональними особливостями управління, чіткістю посадової ієрархії та ієрархії відповідальності, взаємоузгодження процесів та взаємодій, які виникають усередині окремих функцій” [172, с. 90].

В умовах кризових ситуацій вартує уваги процесно-орієнтований підхід, що поєднує антикризовий менеджмент із процесним управлінням з метою формування та підтримки у життєздатному стані системи цілей та критерії досягнення.

Процесно-орієнтований підхід до антикризового управління підприємством можливий за рахунок: інтеграції стратегії антикризового менеджменту із процесним управління, а також формування і підтримки в

дієздатному стані єдиної системи цілей, показників і критеріїв їх досягнення [163, с. 329].

Інструмент підвищення ефективності підприємства у процесному підході до управління підприємствами вбачає Стец І.І. Вчений вважає, що підхід зорієнтований не на функціональну структуру підприємства, а на бізнес-процеси, кінцевими результатами виконання яких є створення товарів або послуг, цінних для зовнішніх чи внутрішніх (у межах підприємства) споживачів [165, с. 165].

Під час формування механізму управління економічною безпекою підприємства варто включати питання антикризового управління, зокрема Приходько В.П., вважає за доцільне розділити управління безпекою на попереджувальне управління (планування, стратегії розвитку, аналіз, прогнозування, зміну для своєчасної реакції на події) та антикризове управління (швидке скорочення втрат за рахунок негайного реагування на події) [155].

Сак Т.В., за умов посилення ризиків, пропонує управління економічною безпекою здійснювати з урахуванням взаємозв'язку внутрішнього середовища підприємства із зовнішнім та адаптації до їхніх змін для досягнення мети підприємства та захисту його від впливу загроз, ризиків і досягнення безпечного функціонування шляхом стратегічного управління (через оцінку середовища, рівнів впливу загроз та розробку заходів забезпечення належного рівня захисту за рахунок стратегій) [156].

Системний підхід – один із провідних напрямів методології спеціального наукового пізнання. Системний підхід сприяє формуванню відповідного адекватного формулювання суті досліджуваних проблем у конкретних науках і виборі ефективних шляхів їх вирішення [154, с. 147]. Бліхар В. вважає: "Системний підхід дозволяє комплексно оцінити будь-яку цілеспрямовану діяльність та діяльність системи управління на рівні конкретних характеристик" [154, с.157].

Кустовська О.В. вважає найкращим у формулюванні суті проблем дослідження та пошуку варіантів вирішення проблем та визначає його, як один із основних напрямків методології наукового пізнання та соціальної практики, мета і завдання якого полягають у дослідженнях певних об'єктів як складних систем [142, с.5].

Ситуаційний (кейсовий) підхід, є радше способом мислення подібно до системного. Підхід започатковано у бізнес-школі (Гарвард), в основу якого покладено ситуційне вирішення проблеми та прийняття оптимального рішення, спираючись на наявні чинники в середовищі існування підприємства.

У противагу процесному та системному підходу, які використовують найчастіше для планування в умовно спокійному середовищі функціонування (визначеному), ситуаційний підхід використовується у нестабільному середовищі та важко прогнозованих ситуаціях.

Підхід зберігає концепцію процесу управління, яка застосовується до всіх організацій, проте ситуаційний підхід визнає, що, хоча загальний процес однаковий, специфічні прийоми, які повинен використовувати керівник для ефективного досягнення цілей організації, можуть значно варіювати [168].

Ситуаційний підхід ефективним, на думку Полянської А., у випадку потреби перетворень, а саме: рівень розвитку "незмінного функціонування підприємства" переходить на рівень "звичайних змін" або рівень "помірних перетворень" й вимагає адекватної реакції підприємства на зміни зовнішнього середовища [167, с. 136].

Авторами у контексті безпеки доволі часто згадується стратегічний підхід до антикризового управління, зв'язок з безпекою прослідковується у попередженні ризиків та загроз. Стратегія повинна передбачити наявність інструментів раннього попередження про ризики і загрози, вимагає адекватного реагування з боку підприємств, яке повинно здійснюватися в рамках антисипативного антикризового менеджменту [161, с. 39].

В антикризовому управлінні Польова О.Л. надає вирішальне значення стратегії управління, в якій головна увага приділяється проблемам виходу з кризи, безпосередньо пов'язаних з усуненням причин, що сприяють виникненню кризи [162].

Наростання невизначеності середовища, турбулентностей посилило вагу управління підприємства в надскладних умов, зростає інтерес до напрацювань науковців: Василик Н.М., Гринчишин Я.М., Кузьмін О.Є., Мельник О.Г., Адамів М.Є., Швець Ф.Д., У.Ешлі, Дж.Моррісон, якими досліджується антсипативний підхід до управління підприємством [156; 161, с. 139; 174; 176; 177; 178; 179]. Антисипативне управління підприємством – це одна зі складових антикризово го управління, що спрямована на раннє виявлення та реагування на фінансову кризу та сигналізує керівникам підприємства про загрози і ризики та додаткові можливості щодо підвищення рівня ефективності та результативності фінансово-господарської діяльності [168, с. 98].

Вчені У. Ешлі, Дж.Моррісон вважають, що антисипативне управління направлене на визначення нових можливостей, уникнення потенційних небезпек, а також трансформацію загроз у можливості [179].

У відповідь на проблеми обмеженості ресурсів (при чому не тільки природних, а й виробничих, фінансових, інформаційних, ресурсу часу) Кузьмін О.Є., Мельник О.Г., Адамів М.Є. запропонували процесно-структурований підхід до управління, який поєднує в собі процесний, системний, ситуаційний, динамічний та функціональний підходи і ґрунтується на концепції, відповідно до якої менеджмент розглядається як процес, що є послідовністю певних завершених етапів, кожен з яких має свою структуру, що в сукупності забезпечують здійснення управлінського впливу керуючої системи на керовану з метою досягнення цілей організації у певних умовах функціонування [176, с.72].

За результатами досліджень підходів до управління, робимо висновок про використання традиційних підходів, на які нашаровуються додаткові

підходи через зміни умов функціонування, посилення вимог до товарів та послуг, їх якісних характеристик з боку оточення та середовища, що призводить до трансформації традиційних підходів до умов сучасності.

Пархоменко Н.О. вважає, що всі сфери та галузі важливі, й водночас різні та виділяє найбільш поширені підходи: функціональний, прибутковий та інвестиційний, системний, індикаторний, економіко-математичний, ресурсний при управлінні економічною безпекою будівельного підприємства [143].

Підходи до управління підприємством ґрунтовно досліджено Чернодубовою Є.В., Мартиновим А.А., авторами наголошується на тому, що вони не є синонімічними, а є взаємно доповненими, виокремлюючи наступні [157152, с.861]:

– системний підхід (будь-яка система розглядається як сукупність взаємопов’язаних елементів);

– логічний підхід (використання логіки та законів мислення як інструменту дослідження);

– відтворювально-еволюційний підхід (спрямований на постійне поновлення виробництва товару з найменшими витратами у відповідності до ринкових потреб);

– інноваційний підхід (активізація інноваційності шляхом виробництва нових продуктів, використання інноваційних технологій та підходів виробництва);

– комплексний підхід (врахування технічних, економічних, соціальних та інших аспектів менеджменту);

– глобальний підхід (орієнтація на всі можливі рівні перебування об’єкта дослідження, а не концентруватися на рівень знаходження його під час аналізу);

– інтеграційний підхід (встановлення взаємозв'язків між усіма складовими елементами та суб'єктами управління, не залежно від рівня їх перебування);

– віртуальний підхід (застосування Інтернет-мережі, електронно-комунікаційних мереж та послуг для побудови віртуальної оргструктури);

– стандартизаційний підхід (встановлення норм та правил, нормативів в управлінні);

– маркетинговий підхід (орієнтація суб'єкта управління на клієнта, користувача);

– ексклюзивний підхід (придбання керуючою стороною права користування інноваційними розробками, перевагою інноваційного продукту на власний розсуд);

– функціональний підхід (функції розглядаються як потреба у їх виконанні);

– процесний підхід (передбачає управління через загальнопов'язані функції в процесі виробництва);

– ситуаційний (варіантний) підхід (застосування різних методів управління визначається конкретною ситуацією);

– нормативний підхід (фіксуються нормативи в управлінні);

– структурний підхід (відзначається вага, рівень впливу чинників, інструментацій, пошук оптимальної пропорції структури факторів виробництва (ресурсів);

– оптимізаційний (кількісний) підхід (передбачає вимірювання, оцінювання за використання статистичних, економіко-математичних методів);

– директивний (адміністративний) підхід (регламентуються правила, обов'язки, управлінські аспекти в нормативних документах). Слід зауважити, що стандартизаційний, нормативний, директивний підходи перегукуються у реалізації управління шляхом урегулювання правил, норм та розпоряджень,

тому їх варто об’єднати та розглядати, на нашу думку, як єдиний нормативно-директивний підхід.

Останні наукові праці, що присвячені дослідженню підходів до управління безпекою підприємства, належать: Ляшенко О.М., Дуб Б.С., Сосновській О.О., Даніловій Є.І. Аналіз методологічних підходів у доробках даних вчених, свідчить про їх адаптованість до зміни умов та сучасності, тому перелічені напрацювання слугуватимуть базисом для подальших напрацювань та пошуку методологічних підходів до управління підприємствами ПЕКМП.

Ляшенко О.М., досліджуючи концептуальні засади управління безпекою, припускає, що доцільним в управлінні економічною безпекою є комплексне використання наукових підходів: системного, процесного, ситуаційного, для їх системного безперервного удосконалення [51, с.146], при чому наголошується, що окремий метод може виступати й інструментом. Також авторкою припущено, що теорія управління має доповнюватися теорією конфліктно-керованих процесів, яка вбачається у дослідженні керованих систем в умовах невизначеностей та конфліктів (математична теорія оптимальних процесів у даних умовах).

Проте, в подальшому для дослідження обрано морфологічний аналіз, що базується на принципах класифікацій, головна ідея яких полягає у постійному пошуку найбільшого числа, чи навіть усіх можливих варіантів рішення поставлених завдань шляхом комбінування основних структурних елементів досліджуваної системи або суттєвих ознак таких елементів [51, с.168-169]. Оскільки матеріал систематизується, а досліджувана система може розділятися на частини й розглядатися з різних точок зору, можна припустити, що морфологічний аналіз базується на системному підході. У роботі Ляшенко О.В. пропонує до розгляду методологічний полігон управління економічною безпекою підприємства, який зображено у вигляді шестикутника, що утворений кутами: концепції, теорії, підходи, принципи, методи, інструменти [51, с. 38].

Узагальнючи підходи до управління підприємством, можемо виокремити наступні (рис. 3.8), звісно, що найчастіше вирокристовуються функціональний, процесний, системний, ситуаційний з комбінуванням залежно від специфіки підприємства, умов його функціонцування та цілей управління.

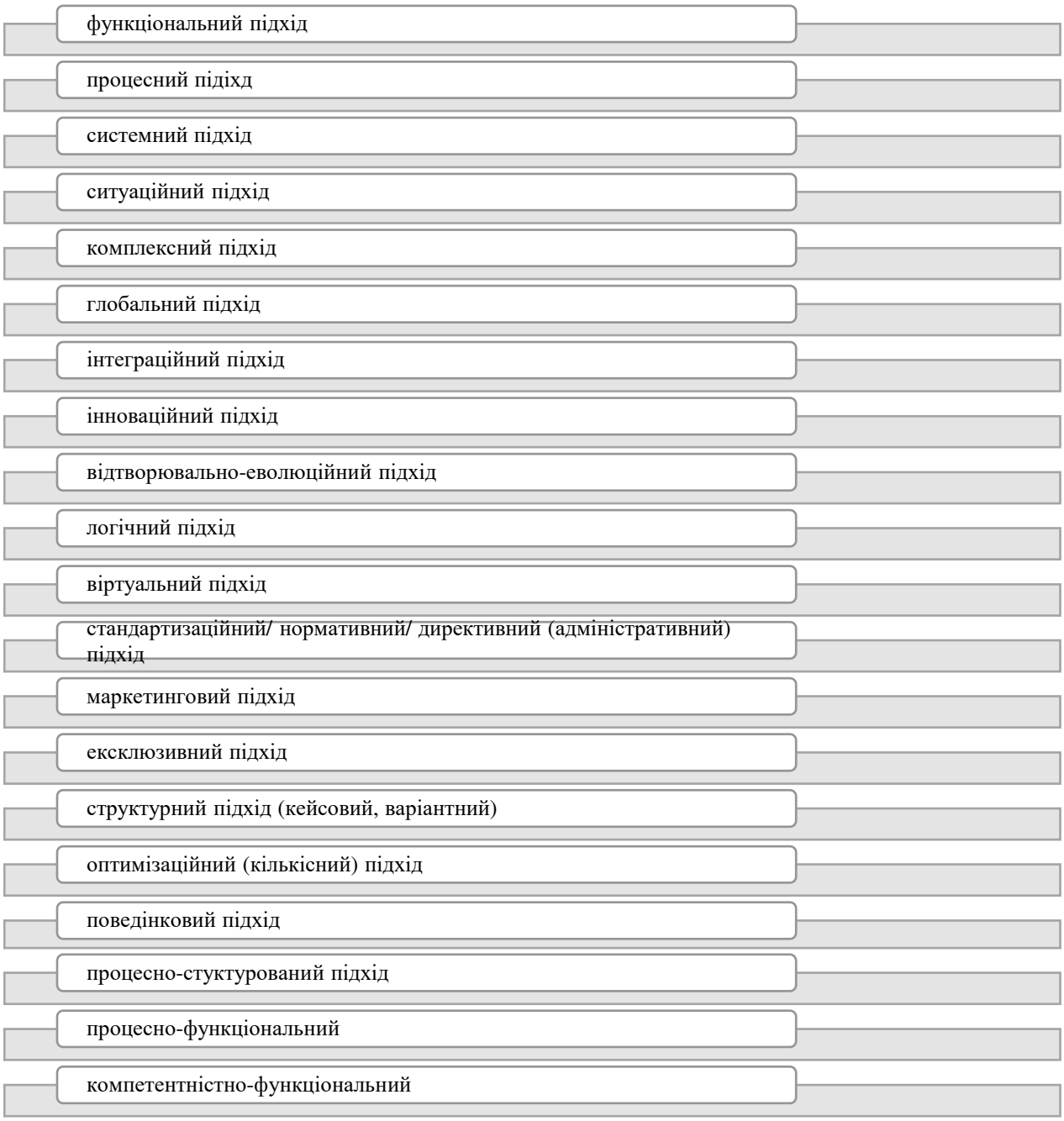


Рис. 3.8. Підходи до управління підприємством

(авторська розробка)

Погоджуємося також із думкою, що економічна безпека є функцією управління, якщо за суттю безпека розглядається як забезпечення результативності підприємства.

До морфологічного опису системи економічної безпеки підприємства вдається Данілова Е.І., включивши на відповідних рівнях [18, с.72]:

– елементи системи економічної безпеки: ресурси, які забезпечують економічний захист діяльності структурних підрозділів підприємства (структури, кадри, фінанси, інформаційне забезпечення (накази, розпорядження, приписи, посадові інструкції, форми звітності, форми аналітичних звітів, програмне забезпечення, методики), технічні засоби (засоби контролю тощо);

– цільові об'єкти захисту: структурні підрозділи підприємства; підприємство як цілісний майновий комплекс та ринковий суб'єкт;

– структуру цілей системи економічної безпеки: на рівні структурних підрозділів: безпека бізнес-процесів; безпека персоналу; безпека матеріальних ресурсів; безпека інформації; безпека відносин; на рівні підприємства: безпека цілісності майнового комплексу безпека іміджу, ринкова безпека.

Опрацювавши доробки науковців з питань економічної безпеки підприємства, Дуб Б.С. виокремлено чотири підходи до управління, грунтуючись на розумінні сутності безпеки, із зазначенням, що за тлумаченням їх варто звести до трьох: структурного, функціонального та діяльнісного. Проте, двом підходам надано авторкою однакову назву, хоча комплекс взаємопов'язаних заходів різноманітного характеру, які мають здійснюватися з метою захисту інтересів підприємства від зовнішніх та внутрішніх загроз [11, с.7] аж ніяк не діяльнісний, бо за своєю суттю відповідає захисному.

Методологічні підходи до визначення економічної безпеки підприємства розглянуто Сосновською О.О., основними виділено: стійкісний підхід, гармонізаційний підхід, захисний, конкурентний, ресурсно-

функціональний [15, с. 92]. Узагальнюючи положення та підходи до управління безпекою підприємства, науковицею запропоновано алгоритм взаємозв'язку між структурними елементами системи економічної безпеки підприємств, що побудовано на об'єктно-суб'єктному підході, який дозволяє систематизувати процес забезпечення економічної безпеки підприємства та виявити його мету, суб'єктів реалізації, об'єкти впливу та методичну основу досягнення кінцевого результату [41, с.137]. Також на основі ризик-орієнтованого підходу проведено аналіз та оцінку ризиків для підприємств зв'язку.

Мойсеєнко І.П. вважає, що адекватна система економічної безпеки містить управлінські, правові, економічні, організаційні, мотиваційні способи гармонізації інтересів підприємства із інтересами зовнішнього оточення для забезпечення належного рівня безпеки підприємства із врахуванням його особливостей та діяльності [141, с. 107]. Із урахуванням сучасних умов функціонування господарюючих суб'єктів, застосування ситуаційно-адаптивного підходу дозволяє реагувати на конкерну ситуацію, що склалася в певний момент часу.

Безпека підприємства полягає у здатності своєчасно реагувати на варіативність зовнішнього середовища, адаптації до змін в умовах функціонування.

Ресурсно-функціональний, фінансовий, індикаторний, програмно-цільовий та підхід на основі економічних ризиків виокремлює у монографії Данілова Е.І., яка вважає, що метод обирається на розсуд суб'єкта дослідження, тобто безпосередньо дослідником [18, с.104].

Методологія безпеки вбачається у послідовному поетапному виявленні та визначенні вимог безпеки в доменах [163, с. 212]: підготовка до визначення вимог безпеки; аналіз вразливостей безпеки; моделювання загроз; визначення вимог до безпеки; оцінка ризиків; категоризація та визначення пріоритетів щодо управління безпекою.

Результатом дослідження підходів є трансформація традиційних методологічних підходів управління підприємствами до невизначеності середовища функціонування підприємства (рис. 3.9), які можуть обиратися та використовуватися підприємствами для управління безпекою в залежності від безпекового об'єкта, на який безпосередньо скеровано управління, а також умов функціонування. Важливим висхідним елементом в управлінні є об'єкт, щодо якого приймається рішення,так на думку Князєвої О.А., механізм управління підприємством формується, починаючи із обрання об'єкта, який виступає вихідним компонентом та визначається функціонуванням економічної складової, відображає наявність і негативні впливи ризиків і невизначеності зовнішнього середовища [164].

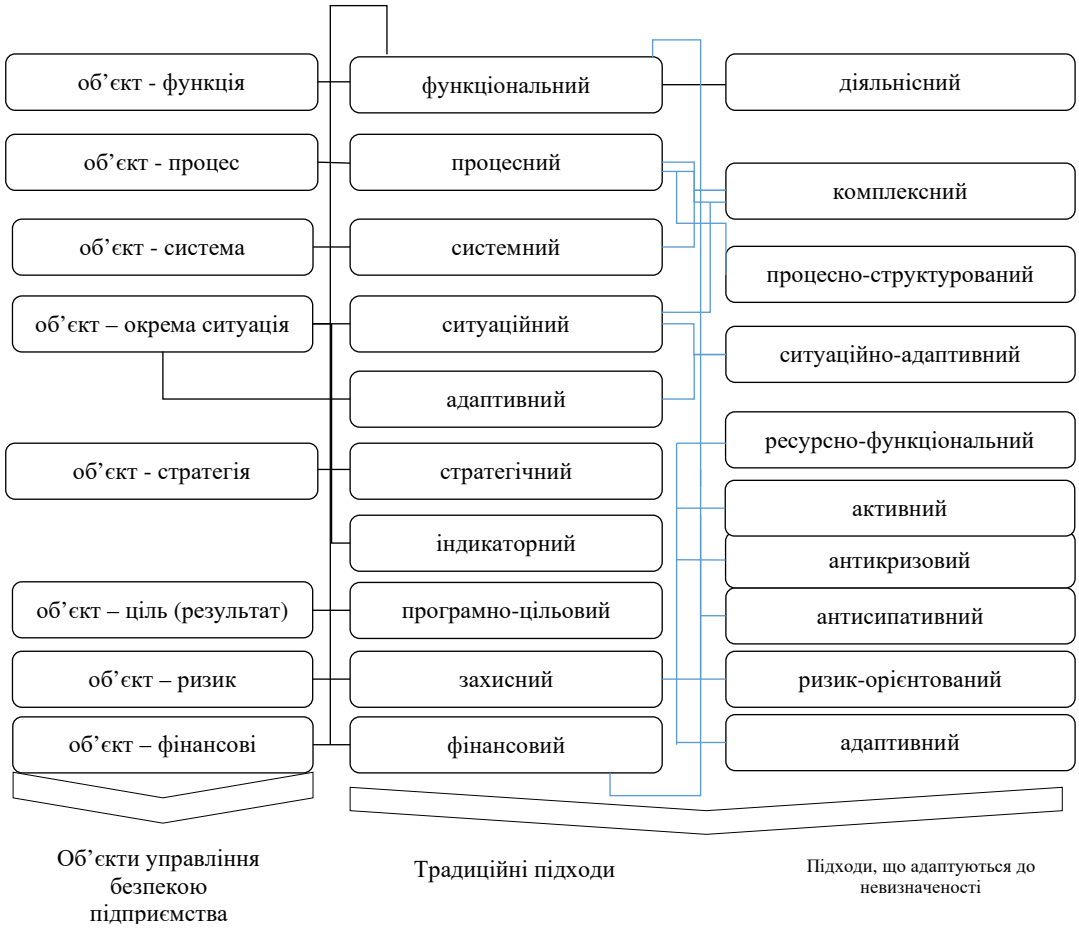


Рис. 3.9. Адаптація традиційних підходів до управління безпекою підприємства за невизначених умов

(авторська розробка)

У разі, якщо об’єктом захисту на підприємстві є функції, які ним виконуються, доцільний до використання функціональний підхід до управління безпекою (наразі – діяльнісний підхід), при обранні процесу, як об’єкта безпеки, зазвичай використовується процесний підхід, а в умовах невизначеності краще застосовувати процесно-структурований та комплексний підхід. Якщо захисту підлягає конкретна ситуація, дієвими є ситуативний, адаптивний, індикаторний підходи, проте, в умовах динамічності середовища, краще використовувати два підходи, що поєднуються у ситуаційно-адаптивному підході. У разі орієнтованості на захист власної стратегії підприємства, дієвим є стратегічний підхід, при захисті цільового результату як об’єкта безпеки – програмно-цільовий й, трансформований до сучасних умов функціонування підприємства ресурсно-функціональний. Найчастіше при управлінні безпекою об’єктом виступає ризик, який залягає в основу розуміння порушення безпеки – небезпеки, у такому разі в управлінні безпекою підприємства доцільно традиційно використовувати захисний підхід або ж, за мінливих умов, – ризик-орієнтований. Структурний та функціональний підходи доцільно трансформувати в один та використовувати при захисті об’єкта управління безпекою підприємства – фінансового ресурсу.

Безпека поліаспектна, складається з множини елементів, компонентів, що пов’язані між собою, тому для забезпечення та управління нею треба мислити системно, комплексно досліджувати процеси, явища, елементи як взаємопов’язані складники цілісної системи. Зв’язок між елементами доцільно вивчати, використовуючи системний аналіз, який проводитиметься із застосуванням сукупності методів і способів дослідження складних об’єктів, процесів, багаторівневих та багатокомпонентних систем, що спираються на комплексний підхід, врахування взаємозв’язків і взаємодії між елементами системи як у середині системи, так і поза її межами. Вважається, що саме системний аналіз важливий для ефективного планування, управлінні операційною діяльністю та прийнятті рішень.

Результатом онтологічного дослідження, нами пропонується тривектроне управління безпекою підприємства, що включає: ресурсно-діяльнісну направленість – захист складових безпеки; гармонізаційну направленість – захист інтересів стейкхолдерів; захистну направленість від умов функціонування – уникнення, усунення, запобігання (або інші варіанти) ризиків, загроз, невизначеностей, що окреслює площину безпеки (рис. 3.10) [218].

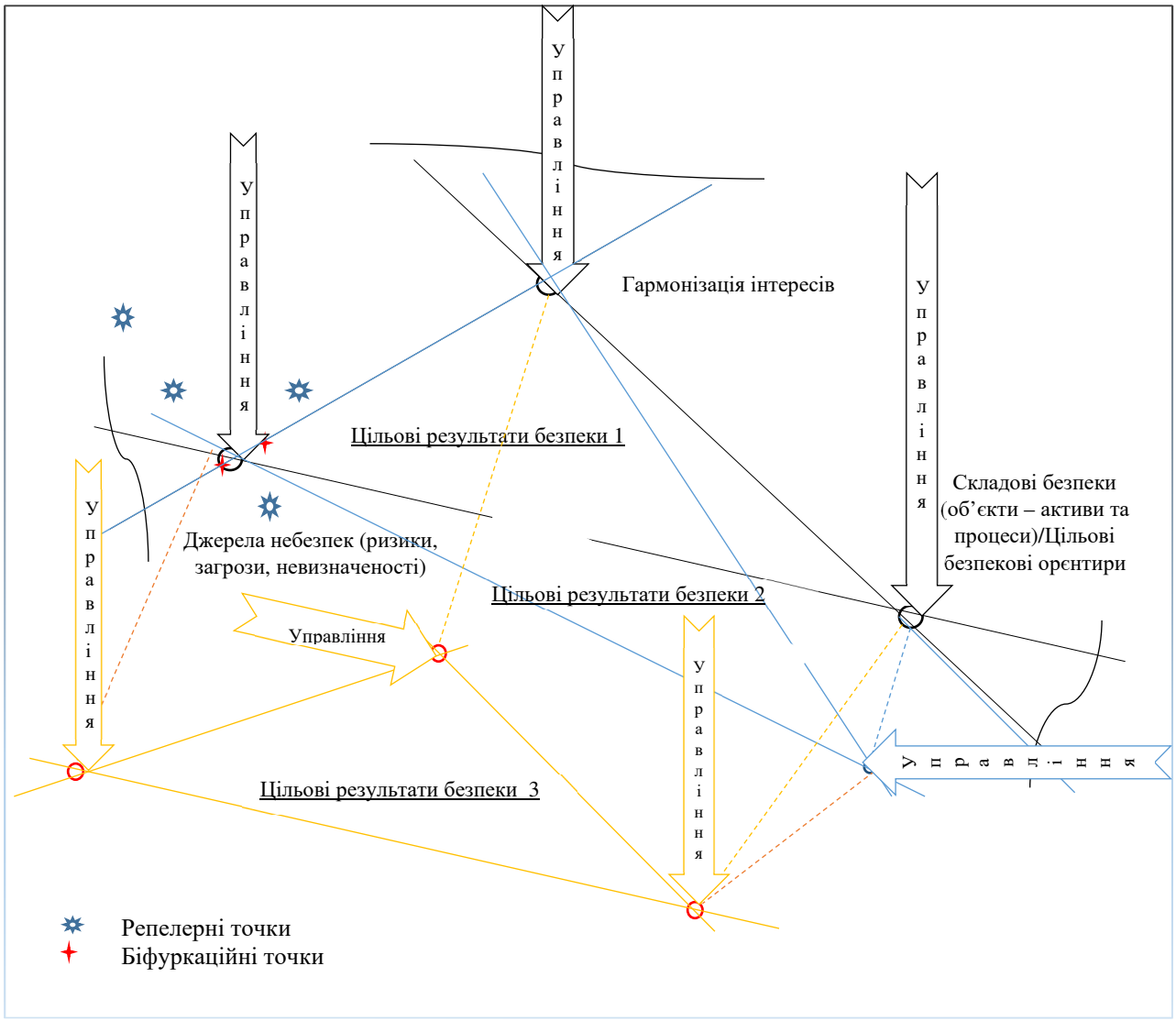


Рис. 3.10. Концепт траєкторії площин станів безпеки під дією тривекторного синергетичного управління (гармонізація інтересів – захист від небезпек – захист складових)

(авторська розробка)

Схематично площина сфорована точками перетину заданих векторних-параметрів, в центрі яких – цільові результати управління безпекою, які нами було попередньо визначено у розділі 1 роботи після опрацювання теоретичних підходів до трактування безпеки. Цільові результати безпеки зміщуються в межах руху площин під дією управління заданих векторів, змінюються кількісно, але незмінно мають забезпечувати прибутковість та рентабельність, розвиток, конкрентоспроможність; стійкість; платоспроможність; інтереси стейкхолдерів.

Чіткість досягнень мети, яка поставлена до управління безпекою підприємства реалізовується методологією дослідження проблемного питання.

З метою побудови міцного методологічного базису управління безпекою підприємства, доцільно здійснити критичний аналіз напрацювань науковців щодо методів оцінки та управління безпекою. З огляду на множинність методів, згаданих у науковій літературі, зупинимося на найбільш прийнятних до використання за сьогоденних умов функціонування підприємств.

Вважаємо за ціль методології – вивчення способів, засобів, методів, прийомів наукового пізнання, що є ключем до розв’язання пробемного питання, усунення прогалини, а також шляхом для отримання нових знань про реальну дійсність проблематики дослідження за конструюювання методів.

Спрощено науковцями методологія розуміється як сукупність методів, що використовуються в процесі наукових досліджень.

Метод є способом дослідження фактів, процесів і явищ, який встановлює системний підхід до їхнього вивчення з метою з’ясування істини, є інструментом для вирішення головного завдання науки – відкриття об’єктивних законів дійсності [178, с. 74; 182, с. 25].

Ознайомившись із Законом України “Про введення воєнного стану в Україні” та Господарським кодексом України, розуміємо воєнний стан, як

нагальний захід, особливий правовий режим через збройну агресію або загрози нападу на територіальну цілісність держави та посягання на незалежність, на меті якого упередження від такого роду загроз, після введення його з’являються тимчасові обмеження окремих конституційних прав та свобод людей, прав та законних інтересів юридичних осіб [210; 211].

З причин сьогоденної невизначеності нами запропоновано враховувати їх, включно до ризиків і загроз, щоб складати цілісну картину умов функціонування підприємства сфери електронних комунікацій. Метод для аналізу VUCA, на даний момент вважаємо найбільш прийнятним до застосування, за результатами якого можна провести оцінку невизнченостей.

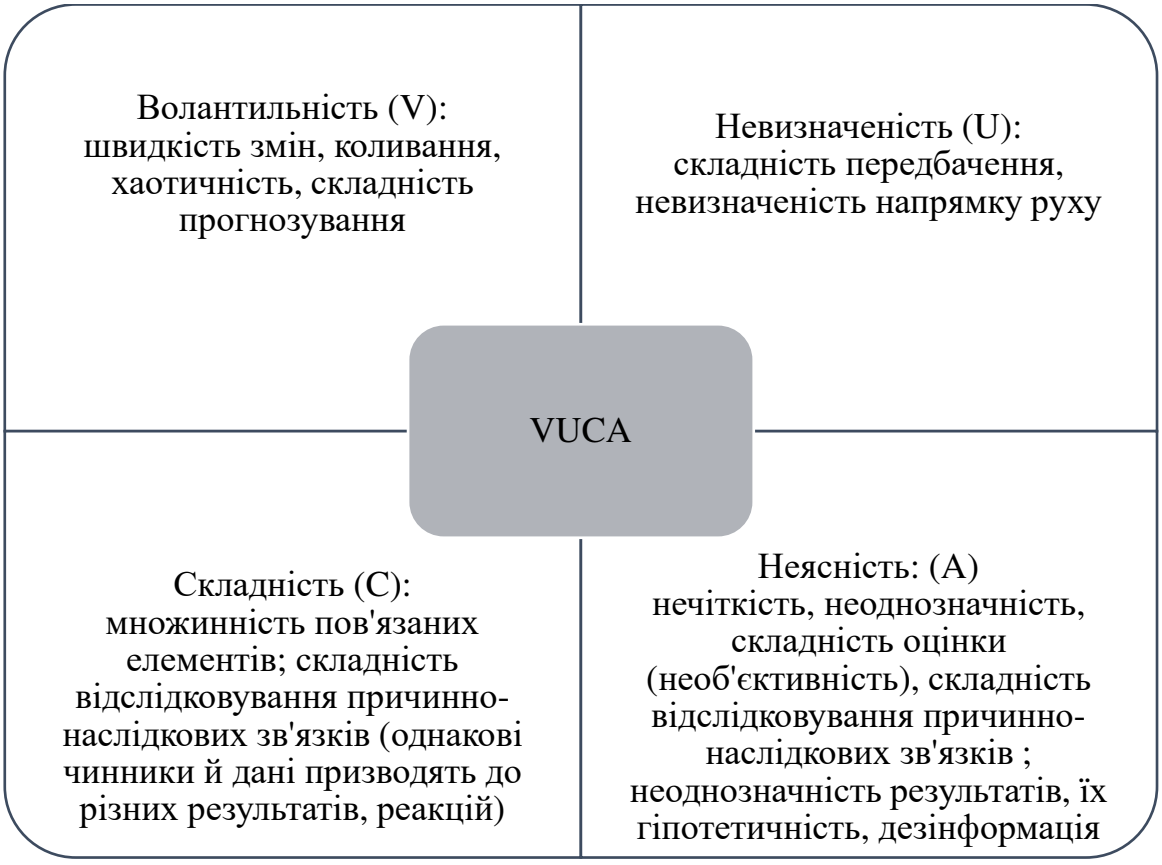


Рис. 3.11. Матриця VUCA-аналізу невизначених умов функціонування підприємства

(складено автором за [126])

Розглядаючи безпеку підприємства в цілому, системно для оцінки невизначеностей варто звернути увагу на працю Єршової Н.Ю, в якій

невизначеність результатів (діагноситики, D) запропоновано оцінювати за величиною ентропії.

Загрози найбільше впливають на безпеку підприємства з причини їх реальності, максимальної наближеності до змін негативного характеру, безпосередній негативній дії на роботу підприємства.

Вважаємо за необхідне для кращої оцінки загроз і ризиків проводити таксономію загроз, під якою розумітиметься їх систематизація та класифікація для чіткості їх розуміння та ступеня нанесення шкоди. Таксономія дозволить швидше ідентифікувати загрози, тобто типізувати, надавати характеристику для покращення та швидкого пошуку заходів щодо їх ліквідації, усунення, адаптації, прийняття.

Ідентифікація небезпек – пошук типу небезпек із наданням характеристик для пропозицій, розробки заходів щодо боротьби та протидії або ж усунення їх наслідків.

Квантифікація (quantification) – акт вимірювання або оцінки розміру об’єкта, явища, дії [212]. Для ризиків квантифікація є кількісною характеристикою, яка конкретизує, що саме оцінювати, вимірювати, чисельно вказує на рівень (ступінь) ризику.

Динамічність середовища, раптові зміни явищ, процесів, призводять до складнощів з їх вимірюванням, оцінкою, Ляшенко О.М. запропоновано кваліметричний метод (лат. “quolis” – якість та грецьк. “metron” – міра) оцінки процесів у разі швидкоплинності змін, які на думку науковиці, є якісними за своєю природою, тому й важковимірюваними. Також метод є прийнятним для співставлення впливу на об’єкт дослідження декількох чинників. Метод відповідає принципам комплексності, оцінка проводиться, починаючи із ієрархічної структуризації показників із фіксацією абсолютних та еталонних значень для яких приймаються вагові коефіцієнти [49, с.155; 51].

Доцільним елементом в управлінні ризиками підприємства, на думку науковиці Гусєвої О.Ю., є діагностика, проведення якої дозволяє

структурувати процес оцінки поточного рівня організації управління ризиками на підприємстві та досягнутого ним рівня економічної стійкості з урахуванням структурованих факторів ризику, що має на меті виявлення стратегічних пріоритетів і перспектив подальшого розвитку управління ризиками в умовах цифрової економіки [199].

Прийняття рішень менеджерами та керівниками компаній щодо рівня ризику, Ваніна Д.А. вважає наступні: уникнення ризику; утримання ризику; передача ризику (страхування, хеджування, аутсорсинг); зниження ризику (диверсифікація, введення лімітів; формування резервів та зменшення часу знаходження в небезпечних зонах) [220].

У документі Американської Асоціації Інженерних товариств “Аналізи ризику. Процеси та застосування”, концепція радіаційного ризику включає два елементи – оцінка ризику (Risk Assessment) і управління ризиком (Risk Management). Не дивлячись на те, що товариством розглядається ризик техногенного характеру, імпонує надане у документі визначення оцінки ризику – як наукового аналізу генезису та масштабів ризику в конкретній ситуації, а також управління ризиком – як аналізу ризикової ситуації та розробки рішень, направлених на мінімізацію ризику.

На нашу думку, управління ризиками за визначеннями є: процесом, заходами, діяльністю, при чому підприємствам уникнути їх доволі складно, а управляти ними – реально й вкрай важливо [208].

Часто для управління ризиками використовується адаптивний, консервативний, активний підходи. За адаптивного підходу підприємство намагається пристосуватися до ситуації та змін в оточенні, спроможне контролювати лише частину ризиків, розробляє стратегію, що фіксує вірогідні відхилення по відношенню до цілей підприємства з прописаними адаптативними заходами щодо пристосування до таких змін.

Активний підхід дозволяє підприємству реагувати на ризики ще до їх появи, здійснюючи постійний моніторинг, контроль та розробку плану, програми управління для завчасного уникнення ризик-подій.

За використання консервативного підходу підприємство чинить опір наслідкам від дії реалізованих ризиків або таким, що мають високу ймовірність настання, несучи при цьому суттєві збитки. Однак у динамічному середовищі даний підхід не спрацьовує, тому що зміни відбуваються надшвидко і підприємство не встигає на них реагувати.

Комітетом організацій-спонсорів Комісії Тредвея – COSO (The Committee of Sponsoring Organizations of the Treadway Commission) розроблено "Інтегровану концепцію управління ризиками підприємства" (COSO ERM Framework), яка забезпечує комплексний, вибудований на принципах підхід до управління ризиками в організаціях, Концептуальна основа COSO ERM складається з восьми компонентів [221]:

1) внутрішнє середовище (сприйняття ризиків персоналом, ризик-апетит культура та етика управління ризиками, кадрова політика та практика, розподіл відповідальності та організаційної структури для управління ризиками);

2) постановка цілей (цілі слугують основою для виявлення та оцінки ризиків та визначені до настання ризиків на різних рівнях, включаючи стратегічні, операційні, звітні, комплаєнс цілі);

3) ідентифікація подій (визначення потенційних подій (внутрішніх або зовнішніх), які відкривають можливості, або ж становлять загрози, а також ризики, які можуть вплинути на досягнення цілей організації);

4) оцінка ризиків (оцінка ймовірності та впливу ризиків з позиції впливу на цілі організації, зокрема – величину потенційних втрат або прибутків, що притаманні окремим ризикам з визначенням їх пріоритетності за їх значущістю);

5) реагування на ризики (підбір методу реагування на ризики, щоб уникнути, пом'якшити, прийняти або передати ризики, при чому заходи стратегічно обираються відповідно до ризик-апетиту та допустимого рівня);

6) заходи контролю (політики, процедури та механізми, які розробляються керівництвом з метою зменшення ризиків та забезпечення

досягнення цілей, при чому контрольні заходи можуть включати превентивні, детективні та коригувальні);

7) інформація та комунікація (своєчасне та прозоре інформування зацікавлених сторін, персоналу сприяє вчасному реагуванню на зміни та виконанню ними функціональних обов'язків);

8) моніторинг (відстеження, оцінка ефективності процесу управління ризиками в організації шляхом перегляду, коригування дій з управління ризиками для його фективності).

Ризик-апетит, або схильність до ризику – сукупна величина за всіма видами ризиків, визначена наперед та в межах допустимого рівня ризику, щодо яких страховик прийняв рішення про доцільність/необхідність їх утримання з метою досягнення його стратегічних цілей та виконання плану діяльності страховика [229].

Макарчуком І. та Федуловою І. ризик-апетит визначено наступним чином: "як досягнення: інтересів зацікавлених сторін; стратегічних цілей діяльності підприємства; максимально допустимого рівня втрат у процесі досягнення стратегічних цілей") [230, с.53]. Автори вважають, що до кожного показника ризику визначатися діапазон результатів у вигляді статистичного розподілу. Доцільність рішення щодо управління безпекою досягається при максимальному значенні комбінуваного критерію, що розподіляє критерій Байєса (вибір рішення за найкращим результатом) та мінімальне значення критерію дисперсії (приняття рішення за найменших відхілень від запланованих результатів). Кількісними показниками ризик-апетиту називають цільові показники діяльності компанії – дохід, прибуток, платоспроможність, вартість капіталізації компанії, покриття капіталу [231, с.47].

Знову ж таки підтверджується вага досягнення цілей підприємства як результату управління безпекою, що доводить важливість та доцільність обрання нами цільових результатів безпеки як орієнтирів руху до безпечного стану функціонування підприємства.

Ризик-апетит може визначатися якісно (описово) та кількісно (вимірно) за наступними методами визначення схильності до ризиків [230, с. 155]:

– вартість заходів з управління ризиком (співставлення вартості управлінських заходів з величиною ризику);

– історичність аспектів розвитку (ретроспективний погляд на ризики, ймовірність настання в різні періоди часу);

– поточний стан підприємства (загальні витрати за окремими ризиками);

– метод аналогії (співставляються загальновідомі статистичні дані за підприємствами в межах галузі, вони мають не перевищувати середні показники);

– експертний метод (оцінка ризик-апетиту проводиться експертами);

– стрес-тестування (побудова моделі розвитку, базаючись на чинниках з найгіршими наслідками, що визначають ризик-апетит);

– комбінований метод (використання різних методів).

Для підприємства ризик-апетит цільових безпекових орієнтирів, які попердньо обрані нами, розраховуватиметься як сума за ризиками втрати платоспроможності, рентабельності, стійкості.

Оцінка ризиків безпеки системи ІТ-підприємства, на думку Карпович І.М., Гладкої О.М., Наконечної Ю.А., має проводитися комплексно, зважаючи на ризики та загрози, вразливості та збитки, визначаючи кількісний вимір ризику за формулою 3.1 [224, с.71]:

$$r = \lambda P_T P_r(\text{с}), \tag{3.1}$$

де λ – величина збитків внаслідок порушення безпеки активу;

P_T – ймовірність загрози

$P_r(\text{с})$ – функція, що описує ймовірність реалізації загрози для активу залежно від витрат на засоби захисту.

Інвестиції покращують стан безпеки, вкладення в захист зменшують ймовірність реалізації загрози, проте, за вищенаведеною формулою ототожнюються ризик та загрози, нами пропонуємо їх розділяти та аналізувати загрози у складі ризиків, як похідні від них.

Станадартом ISO:31000 “Управління ризиками” визначено, що організації (не залежно від типу) стикаються із зовнішніми та внутрішніми чинниками, які є перешкодою у досягненні підприємствами цілей. Також вважається, що управління ризиками є [223]:

- повторюваним процесом, допомагає в розробці стратегії та досягненні цілей, сприяє обгрунтованості рішень;
- є складовою частиною у діяльності підприємства, включає взаємодію із зацікавленими сторонами;
- є частиною загального управління, що розглядається на всіх рівнях підприємства, що удосконалює управління підприємством вцілому;
- враховує внутрішнє та зовнішнє середовище підприємства (поведінку, соціокультурні чинники).

Стандартом передбачено принципи, структура та процес, на яких має грунтуватися управління ризиками, при чому підприємство на власний розсуд обирає прийнятні елементи, які можуть враховуватися частково чи повністю, можуть бути адаптовані до організації для покращення ефективності та послідовності управління (рис. 3.12).

Ризик за стандартом – вплив невизначеності на цілі, а саме відхилення від очікуваного результату є ефектом, який може бути позитивними, негативним і, відповідно до ефекту, відкривати можливості чи спричиняти появі загрозі. Управління ризиками – скоординована діяльність щодо реагування (спрямування), контролю (заходи щодо утримання та/або зміни) ризиків в організації [223].

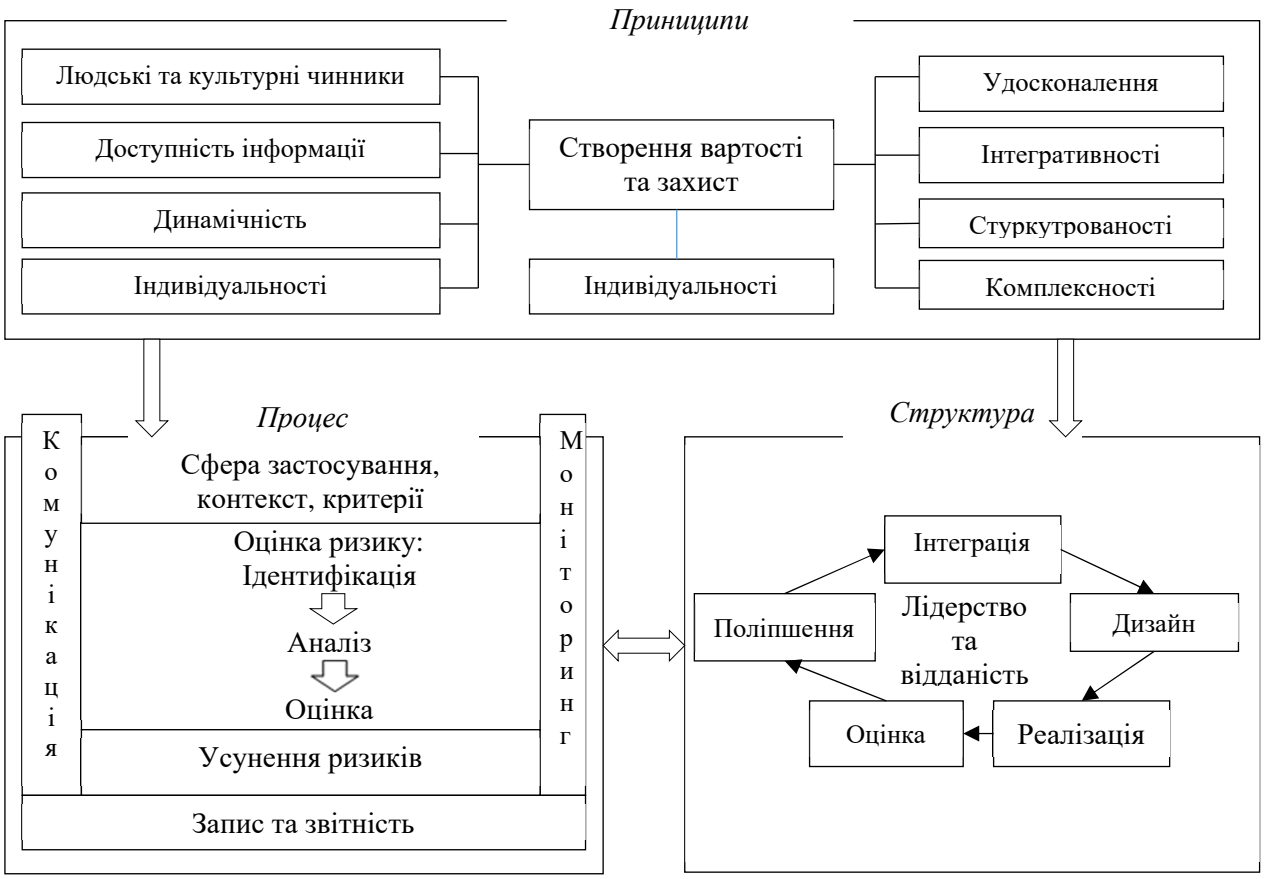


Рис. 3.12. Компоненти управління ризиками: принципи, процес, струкутра за ISO:31000

(складено автором за [223])

Акцентуємо увагу, що документом до процесу управління ризиками включено взаємодію із зацікавленими сторонами, які можуть впливати на рішення щодо діяльності підприємства. Вкотре підтверджується вага обраного нами цільового спрямування управління безпекою із врахуванням інтересів стейкхолдерів.

Метод “Дельфі” – систематичний, інтерактивний метод прогнозування, який спирається на думки групи експертів, більш обґрунтований, ніж індивідуальне опитування через те, що дозволяє учасникам коментувати відповіді один одного, переглядати власні прогнози та думки в режимі реального часу [220; 239].

Метод “Події-наслідки” (HAZOR – Hazard and Operability Studies) – полягає в критичному аналізі діяльності підприємства на предмет можливих несправностей і виходу з ладу обладнання шляхом розчленовування складних виробничих систем на більш прості окремі елементи, кожен із яких піддається ретельному аналізу з метою виявлення та ідентифікації всіх небезпек і ризиків [240, с. 87]. Похідним від методу “Події-наслідки” є SWIFT, за яким опитування проводиться за попередньо підготованим переліком питань, що наводять на відповідь. Обидва методи є більш прийнятними для оцінки ризиків технічного спрямування.

Традиційним методом оцінки ступеня ризику є статистичний, що базується на теорії ймовірностей розподілу випадкових величин, полягає у дослідженні статистики втрат (негативних наслідків прийняття й реалізації рішень) [232; 240, с. 44]. Метод грунтується на інформації про ризики в ретроспективі, що дозволяє підприємствам оцінювати ймовірність їх реалізації у майбутньому. З урахуванням націленості досягнень результатів сталого розвитку, доцільним до використання є метод оцінки механізму управління за статико-динамічним підходом [238; 401].

Аналіз чутливості полягає у дослідженні змін вхідних параметрів на результати підприємства на основі визначення залежності показників ефективності господарської діяльності від варіацій (як правило від ±5% до ±10%) одного з параметрів при незмінних інших. Метод часто використовується для оцінки проєктів [241, с. 100; 242].

Наступний метод – аналіз сценаріїв, який є подібним до аналізу чутливості, відмінність якого полягає у визначенні загального ризику, в противагу дослідженню впливу окремого фактора на результат при використанні методу чутливості. Метод полягає у виявленні чутливості очікуваного результату до змін величин змінних (параметрів) та вимірі можливих інтервал-значень цих змінних [243, с. 72].

Метод “дерева рішень” полягає у формуванні гілок, які вибудовуються за принципом найменшого ризику з існуючих, використовуючи спеціальні

методики розрахунку ймовірності. Компонентами графіку “дерева рішень” є: три поля (поле можливих альтернатив, поле можливих подій, поле очікуваних результатів) та три компоненти (точка приняття рішень, точка можливостей та безпосередньо “гілка рішення”) [244, с. 152; 245, с.59].

Матричний аналіз “наслідок – ймовірність” дозволяє скласти матрицю ризиків, попередньо дослідивши середовище функціонування підприємства (контекст ризику), ризик-чинники, провівши оцінювання за ймовірністю ризик-подій та їх дії (наслідків) з окресленням меж негативних наслідків (рівень). Після чого пропонуються заходи управління ризиками, які розподіляються між ланками у межах повноважень та узгоджуються рішення з інтерсами стейкхолдерів для їх затвердження.

Серед розглянутих методів чільне місце посідає PESTLE-аналіз, який використовується для аналізу та оцінки ризиків, які виникають внаслідок впливу на підприємство зовнішніх факторів, особливо якщо потрібно провести оцінку для організації, що представляє свої послуги (товари) на міжнародному ринку. Акронім PESTLE розшифровується наступним чином [246; 247]:

P (Political) – чинники впливу інституцій на макрорівні: податкова політика, трудове законодавство, екологічне законодавство, торгові обмеження, тарифи, реформи та політична стабільність;

E (Economic) – чинники включають економічне зростання, процентні ставки, коливання валюти, інфляцію, рівень заробітної плати, тривалість робочого дня та вартість життя, торгову політику, економічні тенденції, що впливає не лише на підприємство, а вцілому на галузь;

S (Social) – чинники враховують соціо-культурні аспекти, свідомість здоров'я та безпеку, темпи зростання населення та різні демографічні показники, соціальні тенденції та проблеми, пов’язані зі здоров’ям, освітою та способом життя;

T (Technological) – екологічні та природоохоронні чинники, а також наявні продукти та послуги, технологічний прогрес та інновації, нові

технології, автоматизація, загрози безпеці даних та інші технологічні ризики чи можливості;

L (Legal) – чинники враховують закон, дії уряду, нормативні акти та вимоги щодо надання ЕК послуг, яке може вплинути на діяльність підприємств сфери електронних комунікацій.

E (Environmental) – чинники включають усвідомлення зміни клімату, сезонні або рельєфні зміни, які можуть вплинути на методи роботи та надання ЕК послуг, враховуючи проблеми сталого розвитку суспільства.

Метод цінний для аналізу та оцінки зовнішнього середовища, особливо в умовах нестійкого політичного ландшафту, геополітичного наруження, реформ у країні, які на сьогодні відбуваються. При проведенні комплексної оцінки ризиків (наслідок, ймовірність, ризик) та ідентифікації риків варто брати до уваги доцільність використання розглянутих нижче методів для аналізу та оцінки ризиків (табл. 3.1)

Таблиця 3.1

Доцільність використання методів для аналізу та оцінки ризиків

Методи	Комплексна оцінка ризиків			Ідентифікація
	Наслідок	Ймовірність	Рівень	
Метод “Дельфі” (Delphi method)	–	–	–	+
Статистичний метод аналізу ризику	+	+	+	+
Кваліметричний метод	+	–	+	–
Події-наслідки (HAZOR – Hazard and Operability Studies)	+	+ –	+ –	+
SWIFT	+	+	+	+
Аналіз сценаріїв	+	+	+	+
Аналіз дерева подій	+	+	+	+
Аналогій	+	+	+	+
Аналіз чутливості	+	+	+	+
Поточний стан підприємства (загальні витрати за окремими ризиками)	+	+	+	+
Стрес-тестування	+	–	–	–
Комбінований	+	+	+	+

продовження таблиці 3.1

Дерево рішень	+	+	+	–
Матриця “наслідок–ймовірність”	+	+	+	+
Аналіз за стандартом ISO	+	+	+	+
PESTLE аналіз	+	–	+	+
VUCA, BANI (для оцінки невизначеностей)	+	–	–	–

(узагальнено та складено автором за [236 -242])

Дука А.П. пропонує картографувати ризики, кожному із чинників надавати рівень ймовірності настання за частотою подій (наслідків) [220]:

– часто (постійні небезпеки);

– ймовірно (небезпека часта, спостерігається кілька разів за життєвий цикл);

– можливо (кілька разів впродовж діяльності);

– рідко (малоймовірне настання, одноразово впродовж життєвого циклу);

– практично неймовірно (малоймовірні наслідки, події, можливо, не настануть).

Категорії серйозності за ефектами, в результаті дії чинника ризику визначені як [225]:

– катастрофічні (висока ймовірність, швидкість втрат активів, збитки);

– критична (висока ймовірність, швидкі втрати);

– гранична (затримка у досягненні цілей);

– низька (затримка увиконанні завдань);

– незначна (несуттєві наслідки).

Проте, категорії серйозності катастрофічні та критичні за рівнем шкоди дублюються, тому доцільно або переглянути випадки їх настання й уточнити назви, або ж об’єднати.

При проведенні аналізу оцінка ризиків потенційних втрат від реалізації і порівнюється із ризиками.

Індикатори безпеки підприємства, як правило, розмежовувать за кількісними інтервалами:

– оптимальні значення – інтервал величин у межах сприятливих умов для функцінування підприємства;

– порогові значення – величини, за яких виникають несприятливі умови для функціонуванння підприємства;

– граничні значення – величини, за межами яких відбуваються негативні дії, загрози бізнес-процесам та вцілому функціонуванню підприємства.

Ляшенко О.М. вважає, що економічна безпека досягається керованістю процесу взаємоузгодження економічних інтересів стейкхолдерів як зовнішнього, так і внутрішнього середовища підприємства, який має на меті протистояння загрозам економічній безпеці підприємства та потребує необхідних для такого протистояння ресурсів [51, с.60].

Інтереси підприємства, на думку Мельник К.М.: “є орієнтиром розвитку та відображають характер його економічних відносин, потребу підприємства у безпечному та сталому розвитку в умовах нестабільного зовнішнього середовища і є основою забезпечення фінансової безпеки” [249, с. 42]. Фінансові інтереси підприємства вбачає у максимізації прибутку, зростанні ринкової вартості підприємства, забезпеченні основним і оборотним капіталом, забезпеченні інвестиціями.

Узгодженість інтересів стейкхолдерів найкраще проводити за матричним методом, визначаючи взаємодію на основі цільової співставності внутрішніх та зовнішні інтересів стейкхолдерів.

Екзоінтереси підприємства-постачальника електронних комунікаційних послуг формуються:

споживачами (якість послуги, тарифи на послуги, покриття мережею);

постачальниками (надійність ланцюгів постачання);

інституціями (податкова політика, екологічна політика, преференції, обмеження);

виробниками комплементариних товарів (засоби, приссторї, обладнання, для надання інноваційних послуг);

конкурентами (цінова політика, ступінь монополізованості);

Ендоінтереси окреслюює оточення всередині підприємства:

– персонал (рівень заробітної плати, дивіденди, кар'єрні перспективи, ергономіка, робочий мікроклімат);

– апарат управління, засновники, інвестори, акціонери (прибуток, рентабельність, стійкість, розвиток, платоспроможність).

Вертикалі узгодженості екзо- та ендоінтересів стейкхолдерів підприємств-постачальників електроних комунікаційних послуг представлено на рис. 3.13.

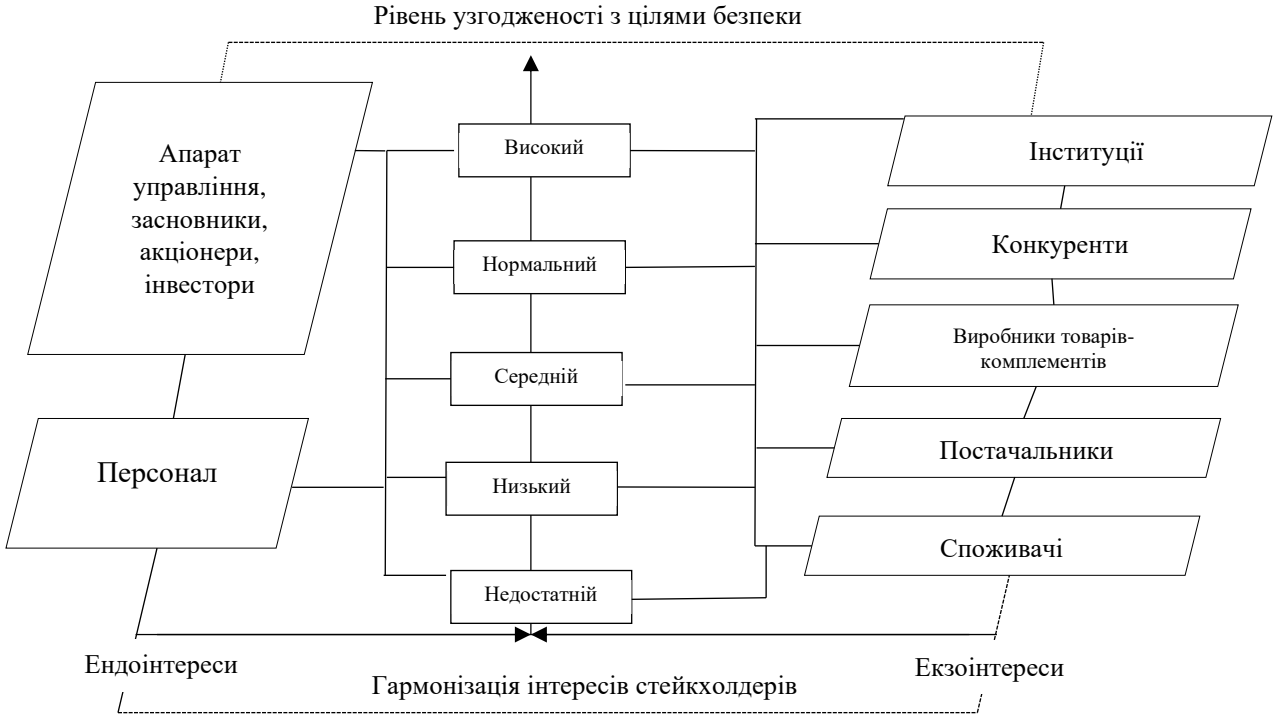


Рис. 3.13. Вертикалі гармонізації екзо- та ендоінтересів стейкхолдерів підприємств-постачальників електронних комунікаційних мереж та послуг

(авторська розробка)

Рівні гармонізації інтересів внутрішнього та зовнішнього оточення можна визначати за відсотком гармонізації інтересів:

високий (гармонізація екзо- та ендоінтересів стейкхолдерів підприємства – більше 75%);

нормальний (узгодженість екзо- та ендоінтересів стейкхолдерів підприємства – від 60 до 75%);

середній (узгодженість екзо- та ендоінтересів стейкхолдерів підприємства – від 40 до 60%);

низький (узгодженість екзо- та ендоінтересів стейкхолдерів підприємства – від 25 до 40%);

недостатній (узгодженість екзо- та ендоінтересів стейкхолдерів підприємства – до 25%).

Гармонізація інтересів стейкхолдерів може визначатися як функція критеріїв результативності та ступеня задоволення потреб стейкхолдерів (формула 3.2):

$$SI = f(RK, IR), \tag{3.2}$$

де SI – гаронізація інтересів;

RK – критерій результативності;

IR – рівень задоволеності потреб стейкхолдерів.

Підсумовуючи результати дослідження методології щодо управління та забезпечення безпеки підприємства, можемо стверджувати про важливість цілепокладання у формуванні орієнтирів як визначників безпеки, які нами представлено у досягненні результатів: платоспроможність, стійкість, розвиток, конкурентоспроможність, прибутковість та рентабельність, а також через гаромонізацію інтересів екзогенних та ендогенних стеккхолдерів. Обов'язковим залишається дослідження ризиків та загроз із їх розмежуванням для розуміння підходів щодо управління у конкретній ситуації та врахування невизначенсті оточення середовища функціонування

підприємств-постачальників електронних комунікацій. Сформований онтологічний базис слугуватиме фундаментом для емпірично нового бачення концепту управління безпекою підприємства, практичний базис виступатиме захисними стінами для ініціації його реалізації функціонуючих підприємств в умовах підвищеної турбулентності, що спичинена не тільки ймовірністю появи ризиків, дії загроз, а й невизначеністю.

3.3. Методологія управління безпекою підприємства

Методологія та методи, що нами розглянуті в попередніх розділах дозволяють викласти нове бачення концепту управління безпекою підприємства в нестабільних умовах функціонування підприємства.

Схиляємося до того, що наукова категорія "концепція" доволі ємна, містить у своїму корені ідейну основу теорії, включає сукупність поглядів на процеси і явища, є способом розуміння та пояснень, тлумачень цих явищ і подій. Концепція економічної безпеки підприємства Дуб Б.С. визначається як [11, с. 11]:

по-перше, система теоретико-методологічних бачень економічної безпеки підприємства, на базі яких будуються цілі й завдання, методи, принципи, концептуальні моделі, положення щодо управлння;

по-друге, неформальний документ для відображення ключових положеннь управління економічною безпекою підприємства;

по-третє, систематизовані, єдино та цілеспрямовані бачення щодо подолання проблем безпеки підприємства.

Концеп-побудова має грунтуватися на принципах:

– системності (рішення локальних завдань підпорядкувані рішенням загальних проблем для досліджуваної системи взаємоповязаних елементів);

– комплексності (аналіз безпеки торкається всіх видів та форм відносин по виробництву продукції та наданню послуг);

– постійності (перманентний аналіз на базі отриманих та нокопичених результатів щодо безпеки).

З урахуванням теореичних та практчних напрацювань у результаті дослідження нами пропонується методологія управління безпекою іпдприємства. Беручи до уваги теоретичні знахідки щодо безпекових питань, варто дотримуватись наступних принципів при побудові концепту: узгодженість цілей управління із цільовими показниками; гармонізованість інтересів підприємства та стейкхолдерів; реальність та досяжність результів безпеки; достовірність; пріорітетність цілей.

В умовах динамічних змін, які викликані глобалізацією, діджиталізацією, інтеграційними процесами, формуються нові парадигми суспільного та економічного розвитку, якими ініціюються нові виклики, на які мають реагувати підприємства сфери електронних комунікацій. Зміни безумовно призводять до перетворень, потребують нових поглядів та рішень у управлінні безпекою заради пристосування, адаптацій та життєздатності підприємства у відповідь на виклики сучасності.

Назрілість питань безпеки беззаперечна, тому варто розглянути, як традиційні підходи, так і новітні щодо управління у ключі сучасних тенденцій та варіативності умов XXI століття, формувати на їх основі нові бачення щодо вирішення прогалин у безпеці.

З метою чіткого розуміння методології управління безпекою підприємства, вбачаємо за доцільне поетапно окреслити складові її формування.

1. Теоретичний базис (категоріальний апарат понять “безпека”, “управління”).

2. Оточення, умови, дії, інтереси стейкхолдерів

3. Складові безпеки

4. Ризики та загрози, перехідні точки – біфуркації та репелерні.

1) Оскільки підґрунтям для методології слугують категорія безпека, вартує спиратися на ознаки безпеки функціонуючого підприємства, нами було виокремлено: здатність до розвитку, стійкість, платоспроможність; прибуток та

рентабельність, конкурентоспроможність, інтереси. Саме ознаки описуватимуть стан безпеки.

2) Стан безпеки залежить від дії оточення, зокрема нами виділено чинники впливу, невизначеність, окремо слід розглянути ризики та загрози, які нами розмежовуються наступним чином: якщо характерна ймовірність настання події – ризик, якщо подія настала та відбуваються зміни – загроза. Слід зазначити, що множинність комбінацій внутрішніх чинників перетворює їх на загрозу.

У разі низької поінформованості про підприємство, умов його функціонування, оточення, а також обставин непереборної сили йтиметься про невизначеність.

3) Управління – це процес, який має вхідні та вихідні ресурси, що корелюватимуть із складовими, які забезпечують безпеку підприємства, на виході, результатом управління буде розвиток, стійкість, платоспроможність, прибуток та рентабельність, конкурентоспроможність, інтереси (отримується результат (ефект), що відповідатиме ознакам безпеки, які окреслено поняттям).

Ґрунтовний аналіз теоретичних напрацювань дозволив окреслити площину безпеки. Узагальнюючи результати дослідження теоретичних (теорії: економічна теорія, теорія менеджменту, теорія фірм, теорія прибутків, еволюційна теорія, інноваційна теорія, теорія нестабільності, теорія інформації, теорія сталого розвитку, загальна теорія систем, підприємницька теорія, теорія ризиків, теорія стійкості систем, теорія структурного функціоналізму) та методологічних засад управління безпекою підприємства (методи: прогнозування; логічний; аналогії; графічний; історичний, морфологічний; моделювання; конкретизації; ентропії; статистичний; узагальнення; формалізації, групування, порівняння, систематизації; економіко-математичний, аналіз і синтез; індукція та дедукція; наукової абстракції, модель формування безпекової площини за метриками безпеки), вдалося обґрунтувати та сформувати теоретико-методологічноу концепцію управління безпекою підприємств за умов невизначеності (рис. 3.14.).

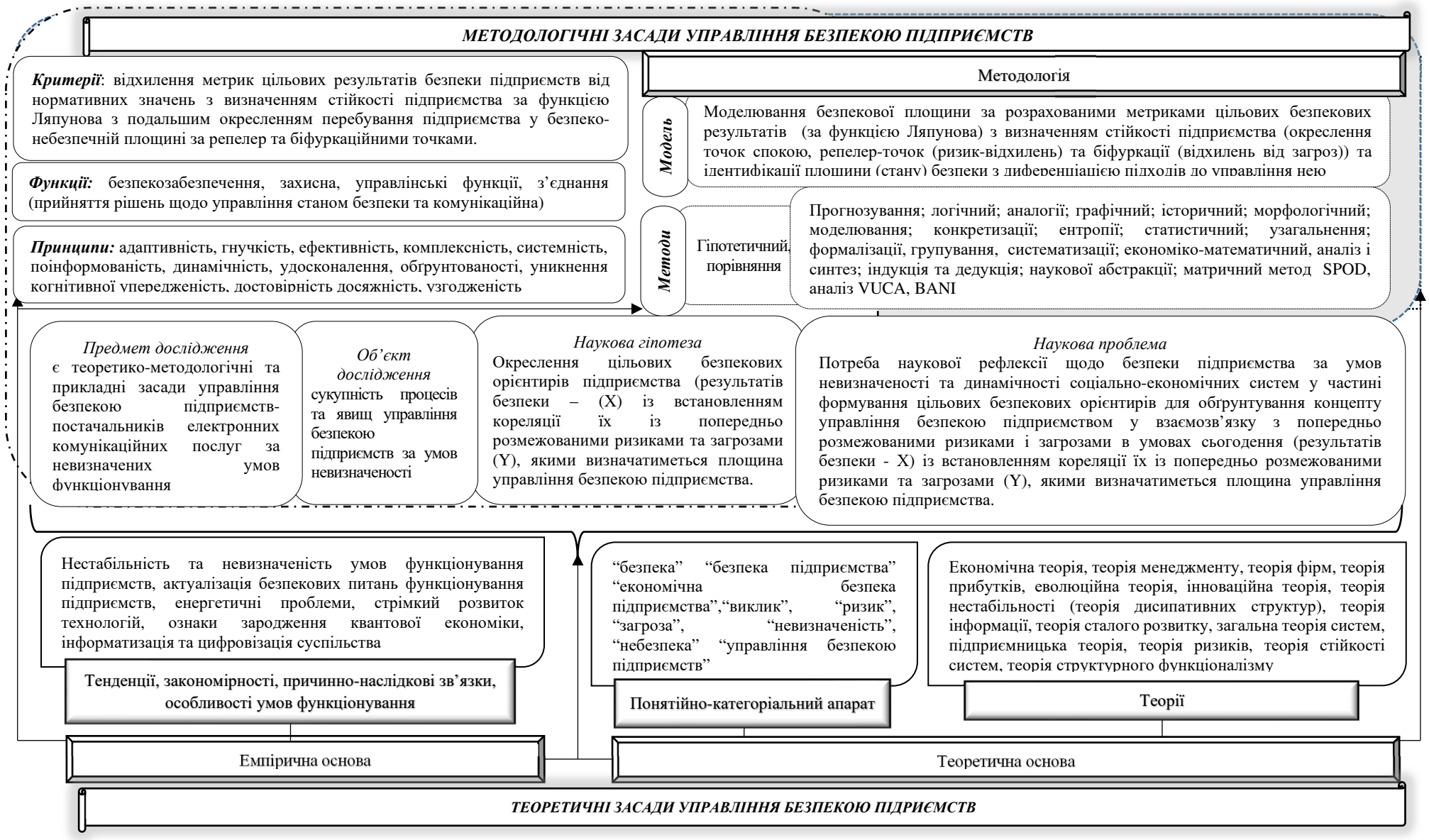


Рис. 3.14. Теоретико-методологічна концепція управління безпекою підприємств за умов невизначеності *(авторська розробка)*

Стейкхолдери

- 1 - Постачальники мереж та послуг електронних комунікцаій
- 2 - Споживачі електронних комунікаційних послуг
- 3 - Регулятор (Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку;
- 4 - Центральний орган виконавчої влади у сферах електронних комунікацій та радіочастотного спектра)
- 5 - Асоціації ("Телас", Інтеренет асоціація України, Асоціація правовласників та постачальників контенту, "Телекомунікаційн палата України", "Укртелемережа", Асоціація учасників ринку бездротових мереж передачі даних)
- 6 Заклади вищої освіти (Державний університет інформаційно-комунікаційних технологій, Національний університет "Львівська політехніка", Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського" та ін.
- 7 Підприємства-користувачі послугами електронних комунікацій
- 8- Власники інфраструктури електронних мереж та комунікацій
- 9 -Інституції (Кабінет Міністрів України, Міністерство фінансів України, Верховна Рада України, Державна податкова служба)
- 10 - Національна рада України з питань розвитку науки і технологій
- 11 - Міністерство розвитку економіки, торгівлі та сільського господарства України
- 12 - Міжнародний союз електрозв'язку
- 13 - Міністерство цифрової трансформації України
- 14 - Світовий банк
- 15 - Бізнес-структури
- 16 - Інвестори
- 17 - Кредитори
- 18 - Керівники
- 19 - Власники

Вето-гравці

- 18 - Міністерство цифрової трансформації
- 19 - Міністерство фінансів України
- 20 - Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку
- 21 - Державна податкова служба України
- 22 - Кабінет Міністрів України

Рис. 3.15. Стейкхолдери та вето-гравці ринку постачання електронних комунікаційних мереж та послуг

(складено автором)

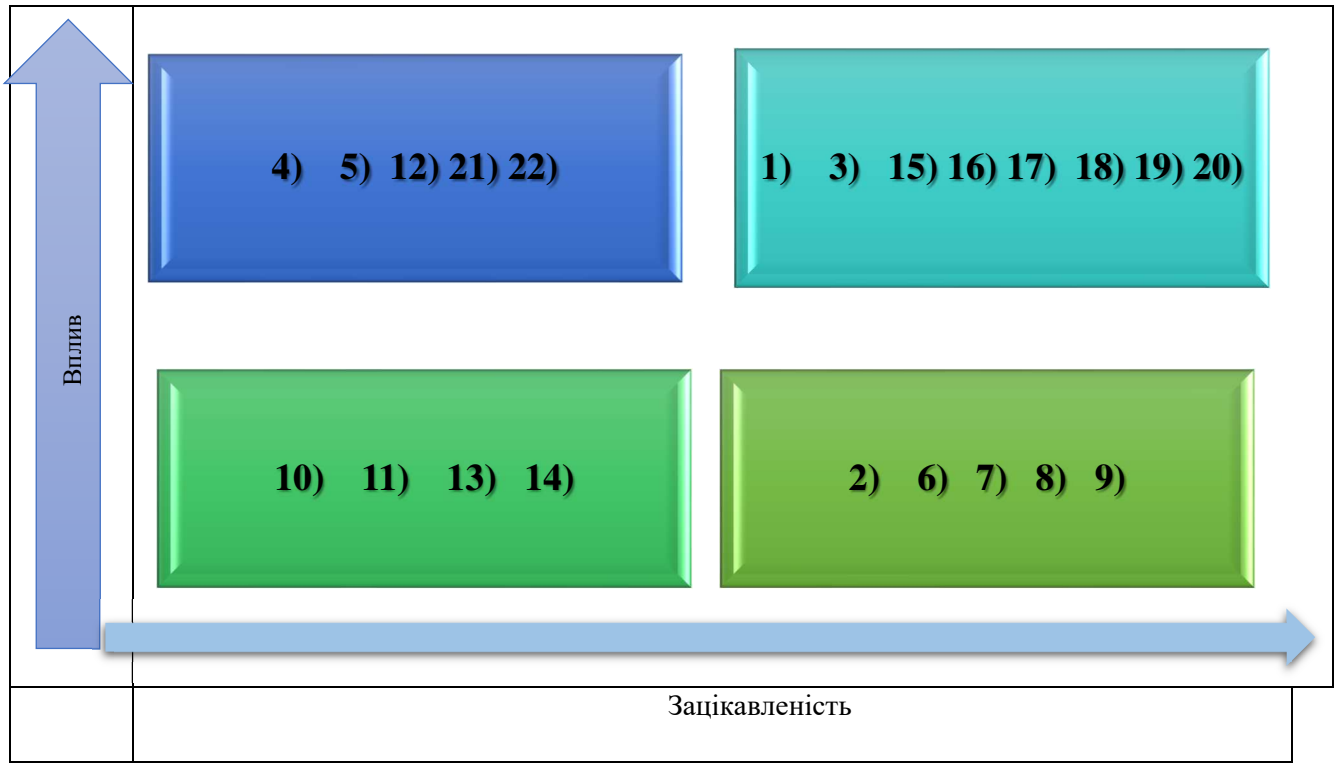


Рис. 3.16. Аналіз стейкхолдерів за рівнем зацікавленості та впливовості *(складено автором)*

Важливо правильно визначитися із ступенем впливу зацікавлених сторін на функціонування підприємства та прийняття рішень, визначитися із дотичними сторонами та ідентифікувати значущість конкретного стейкхолдера.

Ідентифікацію стейкхолдерів доцільно провести на основі типології за впливом на компанію (влада), за відносинами із зацікавленими сторанами (легітмність), вимог, претензій до компанії зі сторони стейкхолдерів (терміновість). Перебування у кожному із трьох типів формує найбільший пріоритет стейкхолдерів і врахування їх точки зору на вирішення проблемних питань та управління. Теорія значущості за типологією поділу стейкхолдерів широко викоритовується у практиці та формується як діаграма перетину перебування стейкхолдерів у конкретному типі (рис. 3.17)

Рис. 3.17. Ступінь значущості стейкхолдерів за типологією: влада, легітимність, терміновість (за Мітчелом)

(складено автором)

Атрибути: "влада" визначає здатність стейкхолдерів отримати бажаний результат (можливість прийняття управлінських рішень, фінансова винагорода); "легітимність" – ступінь відповідності юридичним нормам і нормам поведінки, прийнятим у конкретному суспільстві; "терміновість" – нагальна увага до вимог стейкхолдерів.

Отримуємо, що в прямокутнику перетину всіх атрибутів перебувають: власники, інвестори, регулятор, тому при прийнятті рішень та розгляді проблемних питань їх вимоги та бачення прийматимуться до уваги першочергово. Саме дані стейкхолдери формують пріоритетність цільових результатів діяльності, за якими будуть обиратися метрики їх забезпечення для подальшого аналізу та оцінки.

Графічне представлення гармонізації інтересів стейкхолдерів щодо цільових результатів діяльності підприємства, як інтересу підприємства та інтересів стейкхолдерів через рівень їх задоволення, представлено на рис. 3.18.

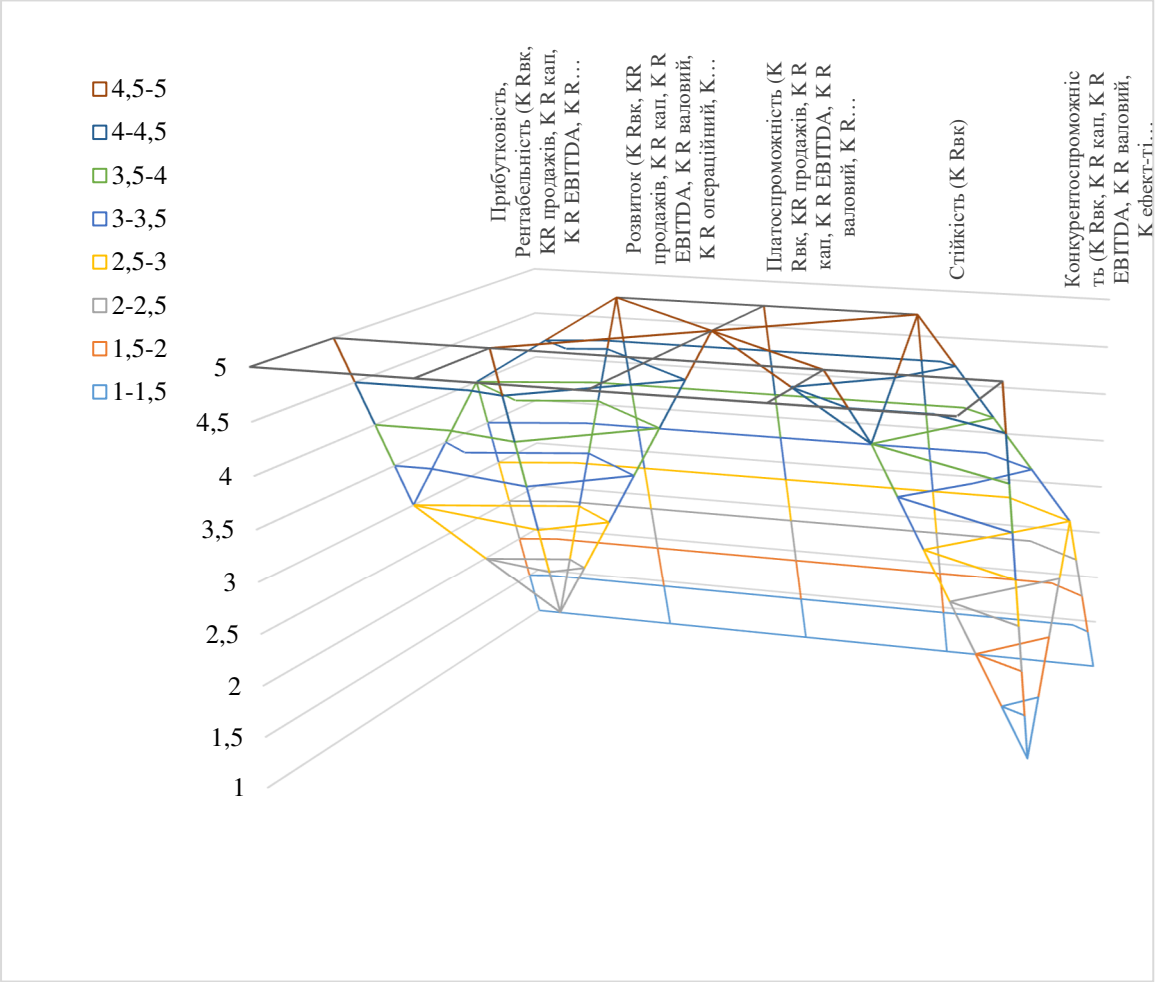


Рис. 3.18. Пріоритетність інтересів стейкхолдерів щодо цільових результатів безпеки підприємства

(авторська розробка)

Опитування стейкхолдерів дозволило чітко окреслити цільові результати діяльності, які засвідчуватимуть безпечність функціонування підприємства, важливо, що вони співпадають з результатами емпіричних досліджень (за етимологією поняття безпеки, сутності, змісту). Результати опитування щодо ваги цільових результатів вказують на те, що власники, персонал, інвестори в питанні функціонування підприємства вбачають однаково важливими (5): прибутковість, рентабельність, розвиток, платоспроможність, стійкість. Постачальники вважають найважливішими: платоспроможність (5), стійкість (4), прибутковість та рентабельність (3), розвиток (2) та конкурентоспроможність (1), бачення регулятора дещо

відмінні від інших зацікавлених сторін, їх цікавлять перш за все розвиток, платоспроможність, стійкість (5), далі – прибутковість рентабельність (4) й конкурентоспроможність (3).

Одночасно, кожен із цільових результатів, виходячи із складових, узагальнено представлно стейкхолдерами із зазначенням пріоритетної, найбільш показової метрики, що вимірюватиме цільовий результат безпеки
За кожним цільовим результатом стейкходерами закріплено значущі показники результативності.

4) нами попередньо розглядалися складові, які і будуть вхідними ресурсами (інвестиційно-інноваційна, інтелектуальний капітал, фізична (фізична (силова)), інтерфейсна (репутаційна), інформаційна, фінансова, екологічна, енергетична, електронно-комунікаційна, техніко-технологічна)

5) Процес забезпечення безпеки підприємства тривекторний:

Перший процес – забезпечення;

Другий процес – операційний (основний);

Третій – управління (прийняття рішень).

Кожен із процесів забезпечуватиметься на рівнях управління:

перший процес – рівень управління 3 (задачі, операційні картки, інструкції, розподіл на підпроцеси);

другий процес – рівень 2 (політики щодо управління безпекою)

третій процес – рівень 1 (управління: плани, розпорядження, рішення, стратегії).

Логічним продовженням ланцюга буде інтерпретація функцій управління за рівнями.

Рівень 1 управління, який відповідає за розробку планів, прийняття рішень щодо безпеки виконуватиме функцію планування щодо управління безпекою.

На рівень 2 та 3 припадатиме функція організації безпекових питань

Рівні 1, 2 відповідатимуть за мотивацію, окрім цього мотивація буде торкатися ресурсів на підприємстві, точніше конкретно людського ресурсу.

І, на останок, всі рівні мають контролювати безпечність процесу надання послуги, тільки за контрольованості процесів на всіх рівнях на підприємстві можна досягти безпеки.

Концепт методології управління безпекою залежатиме від конкретної ситуації, тому підходи, концепції мають набувати нових форм, адаптуватися до мінливості оточення, наразі – до умов невизначеності, які ще більше потребують трансформаційних змін в управлінні.

За результатами онтологічного, емпіричного базису методології щодо управління безпекою дозволяє структуризувати та систематизувати бачення концепт-методології управління безпекою підприємства (рис. 3.19).

Моніторинг ризиків та загроз безпеки підприємства, її складових у сучасних невизначених умовах посилення негативних явищ та процесів є значущим в управлінні безпекою.

Безпосередньо складові безпеки містять у собі ресурси, якими управляють, ризики та загрози окреслюватимуться навколо стану безпеки й формуватимуть небезпеки підприємства, так само й чинники, умови невизначеності. Теоретичний базис, виходячи із поглядів на безпеку та сеансами, які вкладаються в розуміння поняття, дозволили сформувати онтологічний базис управління безпекою підприємства.

Підходи до управління різнитимуться та варіюватимуть в залежності від рівня безпеки, що визначатиметься складовими безпеки, які окреслюються колом метрик, індикаторів за кожною групою складових у межах параметричних даних із співвідношенням до критеріальних значень за критичністю, що визначатимуть перебування значення у зоні ризику або загрози. Тобто, до кожного конкретного стану безпеки підприємства обиратиметься підхід, що прийнятний за конкретних умов функціонування досліджуваних підприємств та показників безпеки за складовими, і пропонує поліваріантність управління у межах визначених безпекових станів, що особливо актуально у сучасних невизначених умовах функціонування підприємств, постійних змінах оточення.

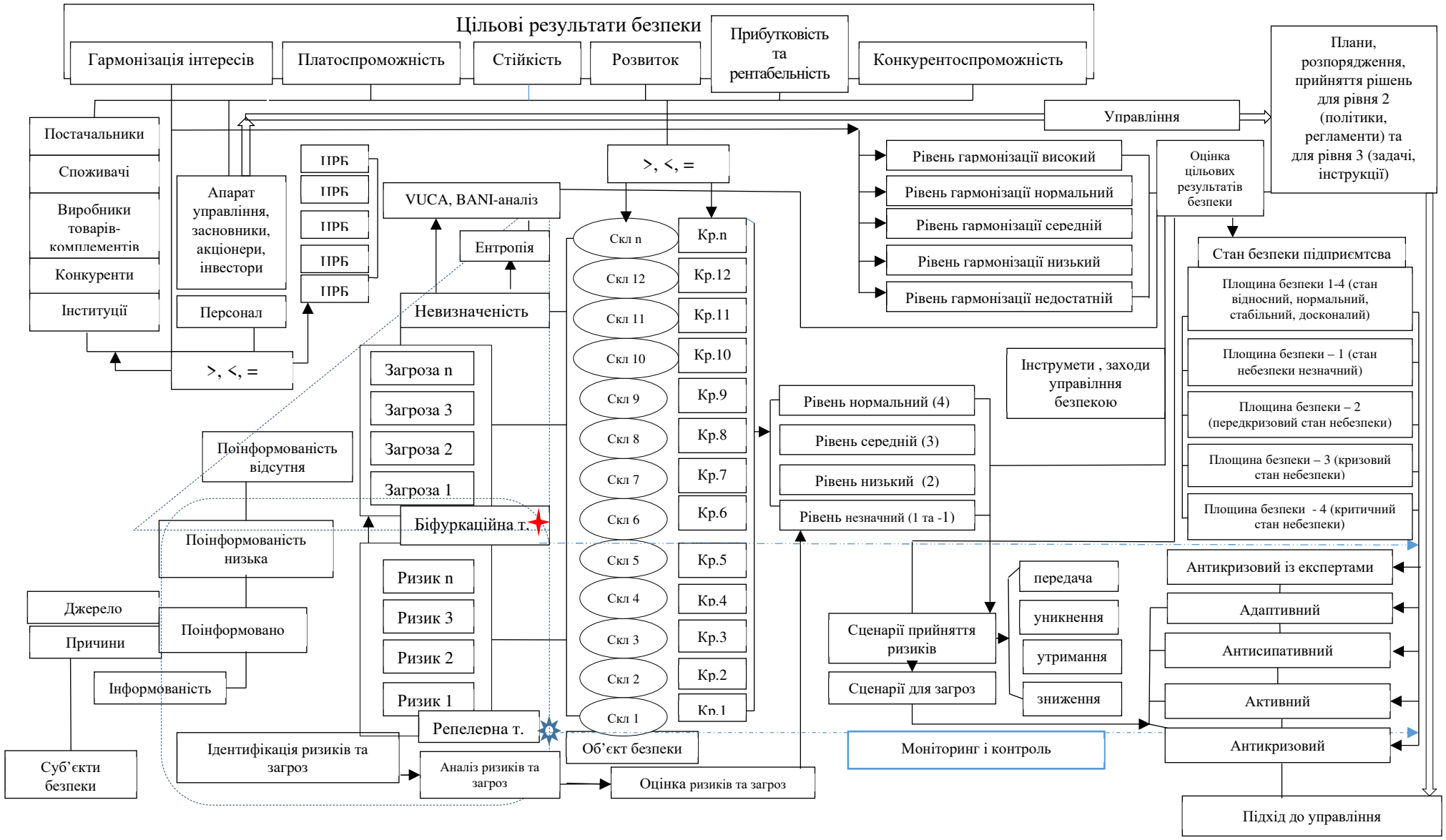


Рис. 3.19. Теоретико-методологічна компонентна площина управління безпекою підприємств *(авторська розробка)*

Індикатори складових безпеки доцільно визначати за коефіцієнтним аналізом з метою порівняності значень та їх співвідношення так як згладжується так звана різнорідність компаній (за розмірами) чого не можна досягти при порівнянні абсолютних показників результатів діяльності підприємств. Коефіцієнтний аналіз прийнятний в управлінні для швидкого управління, тобто експрес-рішення, а у разі потреби дієвого та грунтовного прийняття управлінських рішень розраховані коефіцієнти слугуватимуть основою для глибинних подальших досліджень безпеки підприємства, у нашом випадку станів, з використанням індикаторного підходу, скорингових моделей, кластеризації, регресійного аналізу. Джерелами вихідної інформації для розрахунків слугуватимуть звіти про фінансові результати, звіти про власний капітал, баланс, звіти про рух грошових коштів, звіти про якість надання електронних комунікаційних послуг (форма 11-ЯТП), зведені звіти про діяльність у сфері електронних комунікацій, що надані регулятором (НКЕК), щорічні статистичні звіти, оприлюднені службою статистики, дані Антимонопольного комітету, мережева статистика даних щодо запитів та активності користувачів електронних комунікаційнх послуг, дані додатків, віртуалізовані мережеві дані, що обробляються в перефирійній хмарі та формують великі дані (Big-data), законодавчі та нормативно-правові акти, стандарти, якими регулюються питання функціонування постачальників послуг електронних комунікаційних послуг та встановлюються граничні та нормативні показники результатів діяльності, показників [320].

Алгоритм оцінки станів безпеки-небезпеки підприємств-постачальників електронних комунікаційних послуг представленона рис. 3.20.

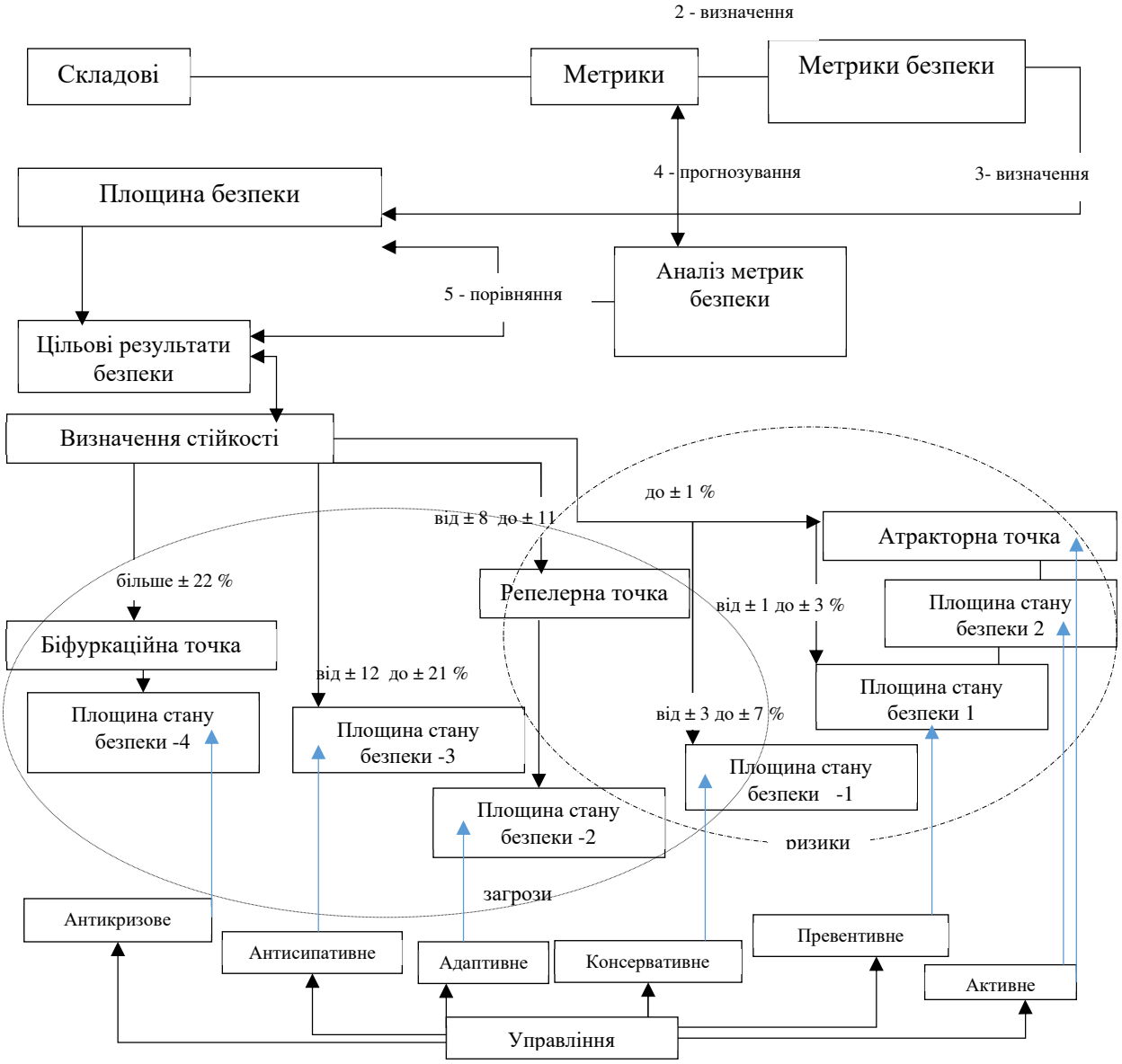


Рис. 3.20. Алгоритм оцінки станів безпеки-небезпеки підприємств *(авторська розробка)*

Досягнення результатів безпеки запропоновано визначати за метриками безпеки та алгоритмом оцінки станів безпеки-небезпеки, що представляє карту руху в площинах безпеки (небезпеки), в залежності від відхилень цільових безпекових орінтирів від нормативних значень (з орієнтацією на порогові), ідентифікує точки репелер та біфуркації для визнчення стану безпеки з подальшим прийняттям рішення щодо управління безпекою, пошуком підходу

до управління, що гарантовано повертатиме підприємство у новий стійкий стан функціонування [235; 237].

Висновки до третього розділу

Узагальнено та виокремлено зв'язки у структурі категорій безпеки, теоретичний блок методології управління безпекою підприємства вибудовано навколо наукових напрацювань питань безпеки, за яким узагальнено понятійний апарат безпеки підприємства, визначено елементи та складові (ризики, загрози, виклики, невизначеність, цільові безпекові орієнтири, об'єкти, суб'єкти упраління, стейкхолдери), за якими формується площина безпеки підприємства, що дозволило сконструювати онтологічний базис методології управління безпекою підприємства.

Відзначено, що ціллю безпеки управління підприємствами є результат, як: безпека в стійкості, безпека в платоспроможності, безпека в прибутковості, безпека у розвитку, безпека в конкурентоспроможності, безпека у гармонізації інтересів, окрім того, супутньо проводиться моніторинг ризиків, загроз, невизначеностей, поєднання яких посилює турбулентність середовища. Запропоновано визначати репелерні та біфуркаційні точки, які відповідно ідентифікуватимуть ризики та загрози, зважаючи на стійкість підприємства до умов функціонування. Сформовано композитарний зв'язок між складовими безпеки, метриками безпеки та цільовими безпековими результатами й мережева складова ємність цільових результатів управління.

Проведено дослідження підходів до управління підприємством для окреслення безпекових підходів, в результаті яких прослідковується трансформація традиційних методологічних підходів управління підприємствами до невизначеності середовища функціонування підприємства, які можуть обиратися та використовуватися підприємствами для управління безпекою в залежності від безпекового об'єкта, на який безпосередньо скеровано управління, а також умов функціонування.

Запропоновано концепт траєкторії площин станів безпеки та управління ним під дією тривекторного синергетичного управління (гармонізація інтересів - захист від небезпек – захист складових).

Запропоновано узгоджувати інтереси стейкхолдерів із інтерсами підприємства, які окреслюють цільові результати безпеки та визначають метрики безпеки підприємства та визначати інтереси стейкхолдерів за матричним методом, на основі цільової співставності внутрішніх та зовнішніх інтересів стейкхолдерів. Веритикалі гармонізації інтересів вимірюються рівнями: недостатній, низький, високий, середній, нормальний, попередньо врахувавши ступінь значущості стейкхолдерів за типологією: влада; легітимність; терміновість з подальшим визначенням гармонізації інтересів стейкхолдерів (цільові результати безпеки та рівень задоволеності результатами).

Запропоновано методологію управління безпекою підприємств, зважаючи на інформованість, ризики та загрози, складові (критерії), оцінки ризиків та сценарії прийняття рішень, зважаючи на відповідність цільових результатів безпеки нормативним значенням та рівню задоволеності стейкхолдерів результатами (рівня гармонізації інтересів стейкхолдерів), що дозволить враховувати, як ризики так і загрози з визначенням репелер та біфуркаційних точок, за якими вибудовуватиметься безпекова площина та визначатиметься стан безпеки.

Основні ідеї та наукові положення, презентовані у даному розділі, викладені у піблікаціях та працях [208; 218; 226; 227; 228; 235; 237; 238; 314; 326; 329; 330; 332; 363; 402]

РОЗДІЛ 4
АНАЛІЗ СЕРЕДОВИЩА ФУНКЦІОНУВАННЯ ТА ОЦІНКА СТАНУ БЕЗПЕКИ ПІДПРИЄМСТВ-ПОСТАЧАЛЬНИКІВ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ ПОСЛУГ

4.1. Аналіз стану ринку постачання електронних комунікаційних мереж та послуг

Динамічність, трансформаціні зміни, глобалізація та інформатизація суспільства, стрімкий розвиток технологій, зміни технологічних укладів та перехід у нову епоху діджиталізації з використанням штучного інтелекту, нанотехнологій, повсякчасним користуванням глобальною мережею для задоволення нової базової потреби суспільства – постійного перебування на зв'язку призвів до високої затребуваності в електронних комунікаційних послугах.

Уявлення про світ змінюються у відповідності до сучасних вимог суспільства щодо безпеки життя, функціонування господарюючих суб'єктів, безпечного пересування та користування електронними комунікаційними послугами. Невизначені умови, які, на жаль, наразі склалися в Україні шалено прискорили цифровізаційні процеси, так, Міністерство цифрової трансформації України, що створено у 2019 році, постійно працює над новими законопроєктами та розширеням переліку е-послуг задля забезпечення фізичної безпеки населення та потреби отримання адміністративних послуг громадянами, які перебувають поза межами країни через військові дії в Україні, а також забезпечення потреб у швидкому обслуговуванні через надання електронних послуг підприємствам (надання публічних е-послуг, е-ідентифікації, е-декларування через створений портал державних послуг "Дія").

Електронні послуги, діджитал-інновації в соціальній сфері є надійним підгрунтям для ефективного функціонування держави в умовах воєнного стану, а також для забезпечення потреб населення у адміністративних послугах. Безперечно, постачальники електронних комунікаційних мереж та послуг відіграють ключову роль у розбудові цифрової держави та глобальної діджиталізації.

Надійне та безпечне функціонування підприємств-постачальників елктрооних комунікаційних мереж та послуг – запорука розвитку економічних одиниць всіх рівнів. Гарантування безпеки постачальників електронних комунікаційних послуг відкриває нові можливості для підприємств, організацій через розширення спетру послуг та спрямованості підприємств удосконалювати виробництво, торгівлю, просування, логістику, а головне – забезпечувати безперебійне функціонування (у разі можливості продовження роботи у режимі онлайн, віддалено).

Україна, вбажаючи потребу у гармонізації стандартів, нормативно-правових актів із країнами Євросоюзу, впродовж останнього десятиріччя активно напрацьовує базис щодо відповідності до законодавчих актів та регуляторних положень у сфері електронних комунікацій. Аналіз звітів Національного інституту стратегічних досліджень, Міністерства цифрової трансформації, IT Research Ukraine дозволив виокремити напрацювання щодо останніх цифрових трансформаційних змін (табл. 4.1)

Таблиця 4.1

Інституційні зміни щодо впровадження цифрових інновацій та розширення переліку надання е-послуг

Напрацювання щодо розбудови цифровізації послуг	Націленість
Регіональна роумінгова угода в регіоні Східного партнерства (з 2016 р.)	Гармонізація ціноутворення та зниження тарифів на роумінг серед країн регіону
Меморандум між урядом та провідними операторами мобільного зв'язку щодо реорганізації радіочастот у діапазоні 900 МГц (2019 р.)	Забезпечення розширення покриття території країни мобільним зв'язком рівня 4G та широкосмуговим доступом до Інтернету
Проєкт Національної стратегії розвитку широкосмугового доступу до Інтернету (2019 р.)	Розбудова широкосмугового доступу до глобальної мережі

продовження таблиця 4.1

Проєкти з розвитку фіксованих і мобільних систем зв'язку Мінцифри та IT-компанії (2019 р.)	Реалізація проєктів з розвитку фіксованих і мобільних систем зв'язку
Підтримка проєкту EU4Digital (визнання довірчих послуг у відповідності зі статтею 14 Регламенту eIDAS під час засідання Комітету Ради асоціації ЄС – Україна) (2019 р.)	Україну обрано та запрошено до участі в пілотних проєктах по створенню транскордонних систем електронному підпису серед країн Східного Партнерства
Приведення у відповідність електронної комерції (з точки зору законодавства, стандартів, екосистем електронної комерції) між ЄС і країнами Україною (з 2020 р.)	Гармонізація систем електронної торгівлі між Україною та ЄС є запровадження "електронного резидентства", що надає можливість нерезидентам дистанційно засновувати та провадити бізнес в Україні
ЄС проєкт EaPConnect (інтеграція із науково-дослідницькою мережею ЄС) (з 2020 р.)	Захист Інтернет-зв'язку великої ємності для передачі дослідницьких даних між Україною та загальноєвропейською мережею досліджень та освіти GÉANT
Розвиток електронних навичок (e-Skills)	Розбудова освітньої онлайн платформи "Дія. Цифрова освіта"
"E-Health" (з 2019 р.)	Розбудова електронної системи охорони здоров'я
Впровадження першої черги Єдиної інформаційної системи соціальної сфери (2023 р.). Проєкт "Автоматизація виплат ВПО в ЄІССС", European Socail Service Award в категорії Digital Transformation (2023 р.). Автоматизована система реєстрації гумдопомоги good.gov.ua (2023 р.)	Підтримка від держави
Defense tech проєктів в державі Brave1 (підтримка розробок) (2023 р.)	Розвиток кластер оборонних технологій
Recorded Future надає доступ до програмної платформи Intelligence Cloud (2023 р.)	Надання державним органам виконавчої влади та підприємствам розвідувальних даних для захисту критичної інфраструктури й розслідування воєнних злочинів
SAP ERP для середнього бізнесу GROW with SAP (2023 р.)	Підтримка цифрову стійкість критичної інфраструктури, спряє ефективним медичним закупівлям. Підтримка українських стартапів, долучення до глобальних акселераторів SAP.iO, в результаті експортери зможуть безоплатно приєднатися до бізнес-мережі SAP Business Network та отримувати підтримку програмного забезпечення й хмарних сервісів
План використання радіочастотного спектра, впровадження нових технологій в Україні (5G) (2023 р.)	Використання нових технологій в Україні для зменшення цифрового розриву між містами й селами, поліпшення якості електронних сервісів, доєднання до Єдиного цифрового ринку
Проєкт USAID "Кібербезпека критично важливої інфраструктури України" (2023 р. до 2030 р.)	Глобальна інноваційна візія WINWIN для розвитку країни у внутрішньо- та зовнішньополітичному контекстах. Пріоритетні напрями: medtech, edtech, AI, економіка без кордонів, biotech, greentech, кібербезпека, напівпровідники, fluid economy, цифрова економіка, agritech та ін.

(складено автором за [250; 251; 252; 254; 255])

Пришвидшує цифровізаційні зміни та розвиток цифрових інновацій, послуг в соціальній сфері, а також бізнесу бажання держави надавати послуги якісно та вчасно, без перепон та черг, попри повномасштабне вторгнення.

Досягти бажаної якості надання електронних послуг держава можне лише за належного функціонування операторів та провайдерів надання електронних та комунікаційних послуг, що доводить важливість їх захисту та безпеки.

Умови невизначеності, що виникли в результаті вторгнення Росії в Україну призвели до появи нових викликів та загроз, які потребують вирішення у глобальному масштабі, оскільки різко змінилися умови функціонування всіх підприємств. Після фінансово-економічної, коронакризи – це третя криза, яка потребує переосмислення в захисті економіки, суспільства, господарюючих суб'єктів.

Однозначно, що питання безпеки стають першочерговими до вирішення. Слід зазначити, що нині суттєво зростають ризики інформаційної безпеки функціонуючих підприємств, організацій, інституцій, що зумовлено переформатуванням роботи підприємств та організацій у режим он-лайн, починаючи із 2019 року. Звісно, що нині більшість організацій вимушені працювати в режимі онлайн (якщо можливо забезпечувати свою основну діяльність), тому збільшується кількість торговельних підприємств, які реалізують товар через власні інтернет-магазини, або ж торговельні майданчики.

Електронна комерція – це та чи інша транзакція, спрямована на отримання прибутку, яка здійснюється через мережу, завдяки якій користування послугою чи товаром передається від однієї особи до іншої [259338]. Електронний бізнес – бізнес-модель, в якій бізнес-процеси та комерційні транзакції автоматизуються за допомогою інформаційних систем. Одним з найбільш перспективних різновидів бізнесу наразі є електронна комерція, яка реалізується в процесі електронного обміну даними (в процесі якого здійснюється електронний документообіг, використовується електронна система платежів, проводяться електронні торгові операції), тобто через обмін товарами та послугами за допомогою електронних засобів комунікації [232].

Електронна комерція може здійснюватися як у вузькому, так і в широкому значеннях. У вузькому сенсі мається на увазі діяльність, яка здійснюється в

інформаційному полі глобальної мережі та із використанням цієї мережі. В широкому сенсі наряду з Інтернетом використовується інші електронні форми та електронні ресурси. У цьому випадку йдеться про розширення змісту “електронна економічна діяльність” за рахунок нових видів діяльності, зокрема йдеться про електронну банківську діяльність та розширення можливостей функціонування господарюючих суб’єктів у онлайн-форматі.

Нині Інтернет став значним соціально-культурним та економічним явищем, вагомість якого зростає щодня. Поряд із зростанням потреб економіки та суспільства відбувається процес трансформації інформаційних комп’ютерних технологій, у зв’язку з чим перехід на ведення підприємницької діяльності в мережі Інтернет стає незворотнім явищем [329].

Охоплюючи майже всі сфери життя, цифрові технології стали вважливим напрямом сучасної економіки. Так, зокрема, запровадження певних обмежень пов’язаних введенням воєнного стану в країні, призвело до ще більш активного переходу бізнесу на торговельні цифрові майданчики.

Зміни в споживацьких перевагах, теж стимулюють виробників відслідковувати вподобання та відповідно до них максимально наближати товар до такого, яким його вбачає покупець, щоб він користувався попитом та був затребуваним. Відслідковувати поведінку споживача, його вподобання, сучасні тенденції та тренди дозволяє саме реалізація та представлення товару на інтернет-майданчиках та інтернет-магазинах [327; 328].

Інтернет-бізнес став чи не єдиним можливим каналом збуту під час пандемії, одним з головних трендів у рітейлі, а для підприємців – активним джерелом доходу. Постійні ринкові зміни торкнулися як традиційних видів бізнесу, адаптувавши їх до нових напрямів ведення діяльності, так і принципово нових способів організації віртуального бізнесу [324].

Наразі чітко окреслилось розуміння того, на скільки інфокомунікації проникли у всі сфери, як послуги електронних комунікцій покращують якість життя та буденне існування.

Взаємне поєднання наземних, бездротових, супутникових мереж які є взаємодоповнюючими та залежними термінацією трафіку, взаємним доступом та використанням технологій та можливостей, дозволяє забезпечувати безперебійну роботу всіх підприємств та організацій, інституцій, тобто функціонування всіх підприємств на мікро- та макрорівнях. Саме тому доцільно приділяти належну увагу захисту підприємств зв'язку від загроз, щоб убезпечити функціонування торговельних підприємств та інших підприємств й організацій у глобальному просторі. Тобто, питання безпеки в нинішньому діджиталізованому та глобалізованому світі стає наріжним та потребує подальших досліджень у захисті підприємств-постачальників електронних комунікцаійних послуг для забезпечення безпечного функціонування усіх господарюючих суб'єктів у форматі онлайн в умовах сьогочасних викликів [344].

Тенденції розвитку сучасного світу відзначаються швидкоплинністю зміни технологій, техніки та потребою якісних послуг електронних комунікацій для розбудови електронного бізнесу, електронних послуг, цифрових послуг, цифрової держави, розумних міст, використання технологій 5G для конвергенції послуг. Тож, сфера електронних комунікацій відіграє особливу та важливу роль у розбудові глобального, цифрового, інформаційного суспільства, що забезпечується поєднанням можливостей використання нових розробок і технологій та наданням послуг під такі розробки споживичам.

Індустрія електронних комунікацій включає мобільний (передача голосу, тексту), фіксований зв'язок (фіксований домашній широкосмуговий зв'язок та фіксований голосовий), при чому продовжуються підключення до мобільних послуг, за даними Statista, споживачі послуг отримують понад 100 екзабайт на місяць та активно зростає попит на широкосмугові підключення через зрстаючі потреби населення та бізнесу у високій якості передаі великих та ємних обсягів даних, яка забезпечуться швидкістю. Увагу зосереджено на підключеннях до 5G, оскільки програми штучного інтелекту потребують мобільних підключень за даною технологією. У програмах розвитку сектору електронних комунікацій

зазначається, що використання 5 G до 2030 року має становити більше 50% від мобільних підключень світу [276], тому у програмі співпраці з ЄС Міністерством цифрової трансформації одним із пунктів зазаначається запуск технології 5G в Україні, а також та приєднання до транспортних 5G коридорів ЄС.

Електронні комунікаційні мережі та послуги, нові розробки у галузі технологій, такі як штучний інтелект (AI) та Інтернет речей (IoT) формують нові погляди на розвиток бізнесу, споживачів – на можливості використання нових сервісів та послуг для виконання роботи, ігор, перемовин. Затребуваність підключення до Інтернету залишається високою саме через потребу у використанні нових розробок та послуг (штучний інтелект, інтернет речей, великих даних, хмарних сервісів). Тому задля задоволення потреб споживачів постачальники електронних комунікаційних мереж дбають про оновлення, впровадження мереж нового покоління – 5G у мобільному секторі, що забезпечує високу швидкість з несуттєвими затримками передачі даних та розгортанням волоконно-широкосмугових мереж, які забезпечують ультрашвидке з'єднання.

Нині Міністерство цифрової трансформації – основний драйвер та інституція у провадженні державної політики у сфері розвитку цифрової інфраструктури та електронних комунікаційних мереж та послуг, розбудови екосистеми інформаційно-комунікаційних технологій.

Тобто із часів пандемії формувалася воронка можливостей для розширення переліку цифрових послуг та сервісів, отримання яких здійснюється постачальниками електронних комунікаційних мереж та послуг, тому безпека їх функціонування стає пріоритетним завданням для держави.

Огляд та аналіз ринку постачання послуг електронних комунікацій дозволить сформувати загальну картину стану розвитку, проаналізувати умови та середовище функціонування постачальника електронних мереж та послуг для подальшого дослідження питань безпеки функціонування підприємств, що надають послуги у сфері електронних комунікаційних послуг.

Регуляторні питання щодо визначення та аналізу ринків електронних комунікаційних послуг вирішує Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку (НКЕК) [261]. Комісія проводить аналіз стану ринку електронних комунікацій, ідентифікацію, визначає перелік послуг на ринку, формує звіти, використовуючи статистичну інформацію, яка надходить від постачальників послуг у сфері ЕК.

За переліком видів економічної діяльності коду 60 відповідає вид діяльності – електрозв'язок, який містить у собі наступне [268]:

Діяльність у сфері проводового електрозв'язку (61.10)

Діяльність у сфері безпроводового електрозв'язку (61.2)

Діяльність у сфері супутникового електрозв'язку (61.3)

Інша діяльність у сфері електрозв'язку (61.9)

За результатами аналізу та огляду ринку електрозв'язку, даних щодо реєстрації постачальників електронних комунікцаій послуг та або мереж Національної комісії електронних комункацій отримуємо наступні дані щодо основного переліку послуг постачальників електронних комунікацій (талб. 4.2).

Із введенням у дію ЗУ "Про електронні комунікації" поняття "оператор" та "провайдер" було замінено на "постачальників електронних комунікаційних послуг", які виступають на ринку суб'єктами господарювання та фактично мають право надавати електронні комунікаційні послуги на власних мережах та (або) на мережах інших постачальників електронних комунікаційних послуг. Постачальники мереж є господарюючими суб'єктами, що послуги доступу до власної електронної комунікаційної мережі та засобів з використання віртуальних мереж [378; 379].

Варто зазначити, що нині значно спрощено реєстрацію постачальника електронних комунікаційних послуг, заявка може подаватися через портал "Дія", Центр надання адміністративних послуг, через нотаріуса. Система оподаткування залишається незмінно або загальна (18% від обсягу прибутку),

або ж пропонується 3 група єдиного податку, за умови відповідності вимогам перебування у даній групі оподаткування.

Обов'язковою умовою є інформування НКЕК через заповнення відповідної електронної заяви щодо початку діяльності із зазначенням переліку видів електронних комунікаційних послуг, які визначено комісією після підтвердження включення, до реєстру постачальником послуг подаються звіти (форма 1-Т про фінансові результати діяльності, а також якість послуг – 11-ЯТП).

Наразі буквені коди видів діяльності гармонізуються із міжнародними та означають наступне [268; 269]:

1) IA – Internet Access;
2) IC – Interpersonal Communications;
3) TS – Transmission Services (for M2M, IoT);
4) TB – Transmission Services (for Broadcasting);
5) NA – Network Access;
6) OS – Operational Servicing;
7) AS – Associated Services.
8) S – Services (послуга надається постачальником електронних комунікаційних послуг);
9) N – Networks (послуга надається постачальником електронних комунікаційних мереж.

Даний перелік не є вичерпним, постачальники послуг можуть доповнити його довільно описавши послугу, якщо її немає в зазначеному переліку.

Таблиця 4.2

Перелік видів електронних комунікаційних послуг

Тип послуги	Код	Назва	Мережа
Послуги доступу до мережі Інтернет	IA.S1	послуга доступу до мережі Інтернет	мобільного зв'язку, фіксованого зв'язку, безпроводового доступу супутникового зв'язку
Послуги міжособистісних електронних комунікацій	IC.S1	послуга міжособистісної електронної комунікації з використанням нумерації	мобільного зв'язку, фіксованого зв'язку безпроводового доступу, супутникового зв'язку, конвергентного зв'язку, віртуальна
	IC.S2	послуга міжособистісної електронної комунікації без використання нумерації	фіксованого зв'язку, безпроводового доступу, супутникового зв'язку, віртуальна
Послуги, що складаються повністю або головним чином з передачі сигналів, у т. ч. і для здійснення міжмашинної взаємодії	TS. S1	послуга передачі сигналів у електронних комунікаційних мережах для здійснення міжмашинної взаємодії та/або IoT	мобільного зв'язку, фіксованого зв'язку, безпроводового доступу, супутникового зв'язку
	TS.S3	послуга передачі сигналів у електронних комунікаційних мережах для надання в користування каналів, VPN, тощо	мобільного зв'язку, фіксованого зв'язку, безпроводового доступу, супутникового зв'язку
Послуги, що складаються повністю або головним чином з передачі сигналів, у т. ч. для мовлення	TB.S1	послуга передачі сигналів у електронних комунікаційних мережах для потреб мовлення	мобільного зв'язку, фіксованого зв'язку, безпроводового доступу, супутникового зв'язку
Послуги доступу до електронних комунікаційних мереж та їх інфраструктури	NA.N1	послуга доступу до елементів електронної комунікаційної мережі та пов'язаних з нею засобів і послуг	мобільного зв'язку, фіксованого зв'язку безпроводового доступу, супутникового зв'язку
	NA.N2	послуга доступу до мережі Інтернет іншим постачальникам мереж та/або послуг	фіксованого зв'язку, супутникового зв'язку
	NA.N3	послуга доступу до фізичної інфраструктури, включаючи споруди, кабельні каналізації і щогли	мобільного зв'язку, фіксованого зв'язку, безпроводового доступу, супутникового зв'язку
	NA.N4	послуга доступу до мережі обміну Інтернет-трафіком (IXP)	може передбачати: фізичне/логічне взаємоз'єднання мережі постачальника електронної комунікаційної мережі з мережами постачальників та/або послуг ін. держав.
	NA.N5	послуга доступу до відповідних систем програмного забезпечення, включаючи системи операційної підтримки	мобільного зв'язку, фіксованого зв'язку, безпроводового доступу, супутникового зв'язку
	NA.N6	послуга доступу до цифрових інформаційних систем та баз даних для попереднього замовлення, надання, замовлення, надсилання запитів на здійснення технічного обслуговування та ремонту, а також виставлення рахунків	мобільного зв'язку, фіксованого зв'язку, безпроводового доступу, супутникового зв'язку
	NA.N7	послуга доступу до ресурсу нумерації, який забезпечує ідентифікацію мереж чи систем, що надають еквівалентну функціональність	мобільного зв'язку, фіксованого зв'язку, безпроводового доступу, супутникового зв'язку
	NA.N 8	послуга доступу до мереж фіксованого і мобільного зв'язку, в тому числі для роумінгу	мобільного зв'язку фіксованого зв'язку
	NA.N9	послуга доступу до систем умовного доступу до послуг цифрового телерадіомовлення	мобільного зв'язку фіксованого зв'язку безпроводового доступу супутникового зв'язку
	NA.N10	послуга доступу до послуг віртуальних мереж	мобільного зв'язку, фіксованого зв'язку, безпроводового доступу, супутникового зв'язку.
Інші послуги	OS.S1	послуга технічного обслуговування і експлуатації електронних комунікаційних мереж	мобільного зв'язку, фіксованого зв'язку, безпроводового доступу, супутникового зв'язку
	AS.S1	пов'язана послуга	мобільного зв'язку, фіксованого зв'язку, безпроводового доступу, супутникового зв'язку

(систематизовано та складено автором за [268; 269; 270])

Ринок постачальників електронних комунікаційних мереж та послуг розширюється, кількість підприємств, осіб-підприємців за розмірами наведений у таблиці 4.3

Таблиця 4.3

Кількість підприємств та фізичних осіб-підприємців сфери інформації та телекомунікацій за розмірами

Розмір підприємства	Підприємство / ФОП	Роки				
		2010	2015	2019	2020	2021
Суб'єкти великого підприємництва	Підприємства	9	6	9	8	9
	Всього	9	6	9	8	9
Суб'єкти середнього підприємництва	Підприємства	409	338	355	348	364
	Фізичні особи-підприємці	1	4	5	1	1
	Всього	410	342	360	349	365
Суб'єкти малого підприємництва (з них суб'єктів мікропідприємництва)	Підприємства	12771 (10728)	13273 (11530)	15553 (13717)	15698 (13912)	16011 (14239)
	Фізичні особи-підприємці	42787 (41239)	102515 (102467)	190225 (190078)	218133 (218034)	267756 (267642)
	Всього	55558 (53441)	115788 (113997)	205778 (203795)	233831 (231946)	283767 (281881)

(складено автором за [271; 267])

Слід відзначити спрощення реєстрації постачальників даних послуг з метою відповідності вимогам щодо розбудови конкурентноого ринку електронних комунікаційних мереж та послуг, за даними НКЕК станом на кінець 2023 року зареєстровано 4113 постачальників електронних комунікаційних мереж та послуг (рис. 4.1).

Приріс зареєстрованих суб'єктів господарювання у 2023 році в абсолютному вираженні склав 2077 по відношенню до 2022 року, показник кількісно вирівнявся до довоєнного значення, що засвідчує затребуваність послуг, стабільний розвиток сектору ІКТ, підвищення конкуренції на ринку.

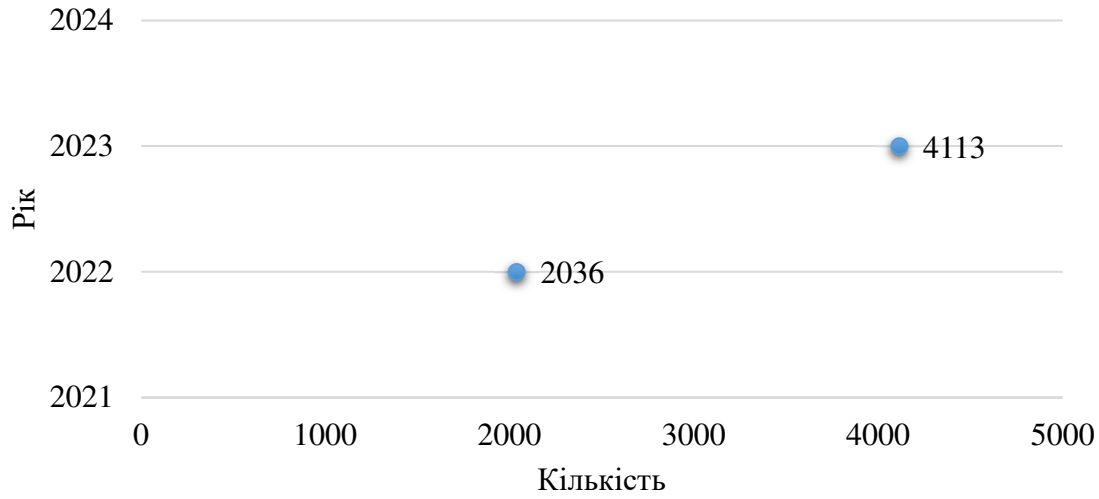


Рис. 4.1. Зареєстрована кількість суб'єктів господарювання з надання електронних комунікаційних послуг у 2022 та 2023 рр.

(складено автором за [271; 295])

Разом із зростанням кількості зареєстрованих суб'єктів-постачальників електронних комунікаційних послуг збільшувались доходи, спостерігається їх позитивна динаміка. Доходи від послуг зв'язку, у порівнянні з 2022 роком збільшилися на 31% та склали 130,5 млрд грн (рис. 4.2).

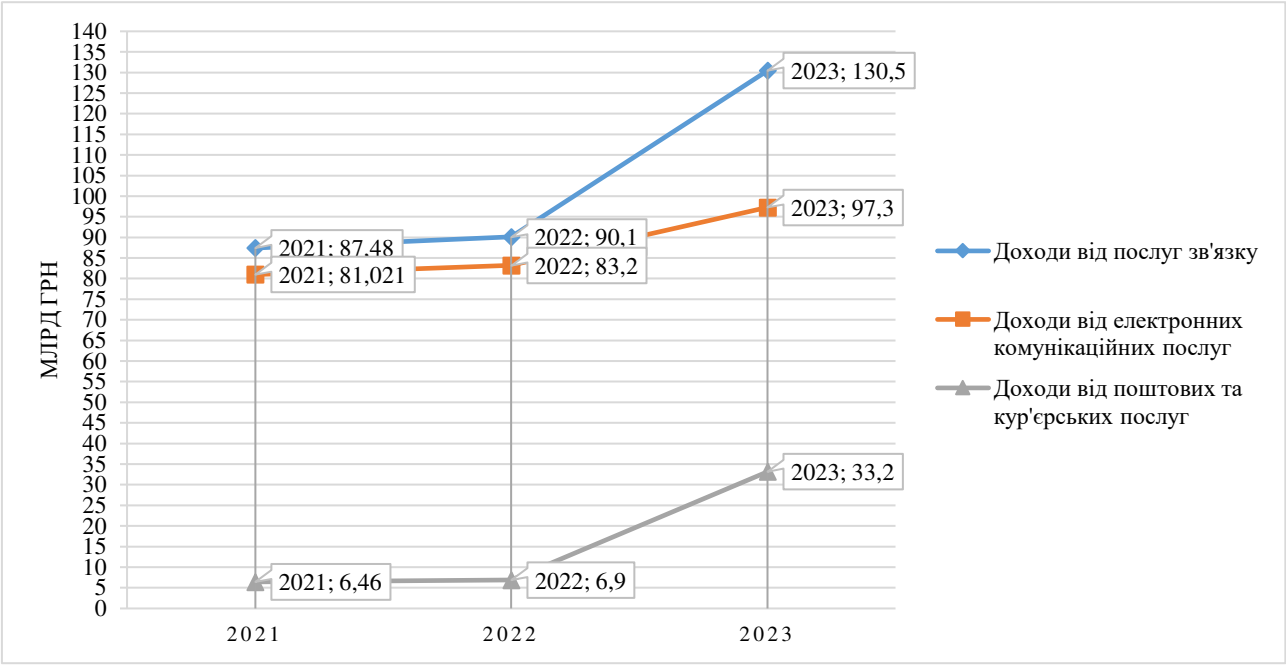


Рис. 4.2. Динаміка доходів сфери зв'язку за 2021-2023 рр., млрд грн

(складено автором за [303;304;305;306])

Темп росту доходів від надання електронних комунікаційних послуг за 2023 рік по відношенню до попереднього року становив 116,95%, доходи зросли із 83,2 млрд грн до 97,3 млрд грн відповідно. Суттєві зміни доходів відбулися за рахунок надання ноштових та кур'єрських послуг, так у 2023 році по відношенню до 2022 року доходи збільшилися на 26,3 млрд грн, темп росту склав 481,16%, що пояснюється підвищенням попиту на поштові послуги та потребою у пересиланні предметів побуту, посилок, речей через вимушене внутрішнє та зовнішнє переміщенням осіб з окупованих територій, а також з територій активних бойових дій.

Впродовж аналізованого періоду відбулися зміни в структурі доходів, отриманих від надання електронних комунікаційних послуг (рис. 4.3).

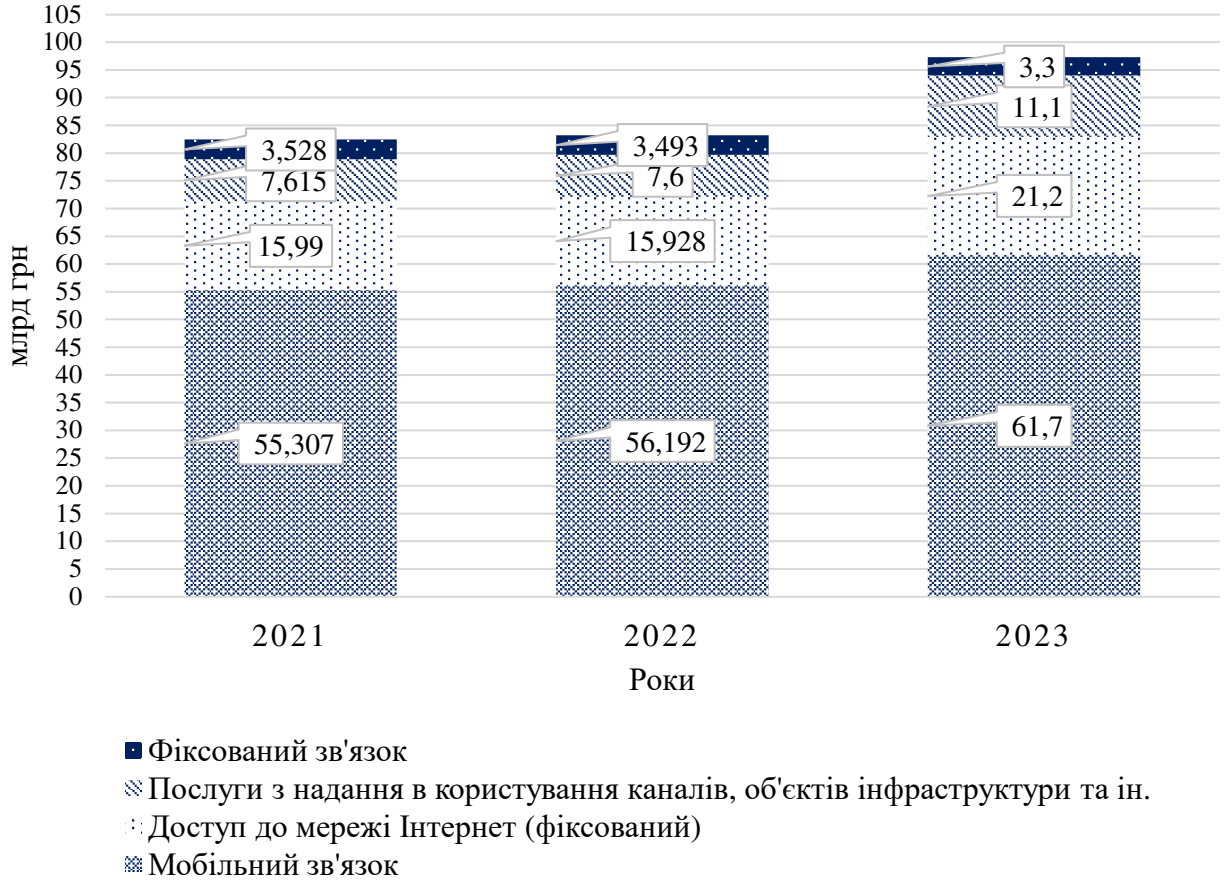


Рис. 4.3. Динаміка та структура доходів від надання електронних комунікаційних послуг (за видами) впродовж 2021-2023 рр., млрд грн

(складено автором за [298; 299; 300; 305; 306])

Мобільний зв’язок зберігає тенденцію збільшення доходів від надання послуг, темп росту у 2023 році по відношенню до 2022 року склав 109,8%, (відповідно доходи становили 61,7 млрд грн по відношенню до 56,192 млрд грн), обсягів передачі даних, особливо з використанням мобільного Інтернету, що пояснюється зростанням користування послугою міжнародного роумінгу. Впродовж 2023 року в середньому у національному роумінгу фіксувалося близько 1 млн користувачів за добу, а у міжнародному – 4 млн користувачів.

За рахунок фіксованого доступу до мережі Інтернет отримано 21,2 млрд грн у 2023 році (темп росту склав 133,1 % по відношенню до обсягів доходів у 2022 році). Спостерігається зростання доходів від послуги з надання в користування каналів, об’єктів інфраструктури, обсяг становив 11,1 млрд грн у 2023 році проти 7,6 млрд грн у 2022 році.

Слід зазначити, що на сьогодні найбільш затребуваною споживачами електронних послуг залишається послуга Інтернет, завдяки якій бізнес та населення спроможні залишатися на зв’язку в надскладних умовах, працювати віддалено, навчатися, спілкуватися, провадити діяльність, а підприємства функціонувати.

Міністерство цифрової трансформації, зважаючи на загрози перебоїв постачання електричної енергії, зарегулювали питання часткового вирішення даної проблеми шляхом енергоефективного підключення споживачів до послуг за технологією xPON-мережі. Проте, окрім переваг у можливості отримання послуги до 72 годин, таке рішення призвело до формування викликів для операторів, оскільки регулятор таким чином порушував право на конкуренцію постачальників, що викликає суперечності із ЗУ “Про електронні комунікації”. Порушення було задокументовано та відображено у листі Інтернет Асоціації України до Мінцифри, в якому були перелічені наступні спірні питання: “xPON створюють умови для порушень прав споживачів; створюють умови порушення економічної конкуренції, а також права постачальників електронних комунікаційних послуг, які використовують технології інші, ніж xPON; створюють умови для відволікання обмежених адміністративних, фінансових і

технічних ресурсів держави і операторів від забезпечення пріоритетного енергорезервування зазначених об'єктів критичної інфраструктури, що погіршує безпеку держави під час війни" [266].

Крім того, Асоціацією наголошено на удосконаленні операторами питань енергоживлення власних мереж незалежно від технологій, які ними використовувалися, одразу після повномасштабного вторгнення.

Зважаючи на потребу у використанні технології PON для забезпечення безперебійного надання послуг та безпечного функціонування підприємств та організацій в умовах воєнного стану, доцільно розглянути існуючі технології з подальшим аналізом їх використання постачальниками послуг Інтернет в Україні.

PON-технологія (Passive Optical Network) – це технологія пасивної оптичної мережі, що відноситься до мережевої архітектури, яка використовує оптичні волокна для доставки даних кінцевим користувачам.

Pon-технологій передачі Інтернет-сигналу до споживача з часу їх появи суттєво еволюціонували (рис. 4.4)

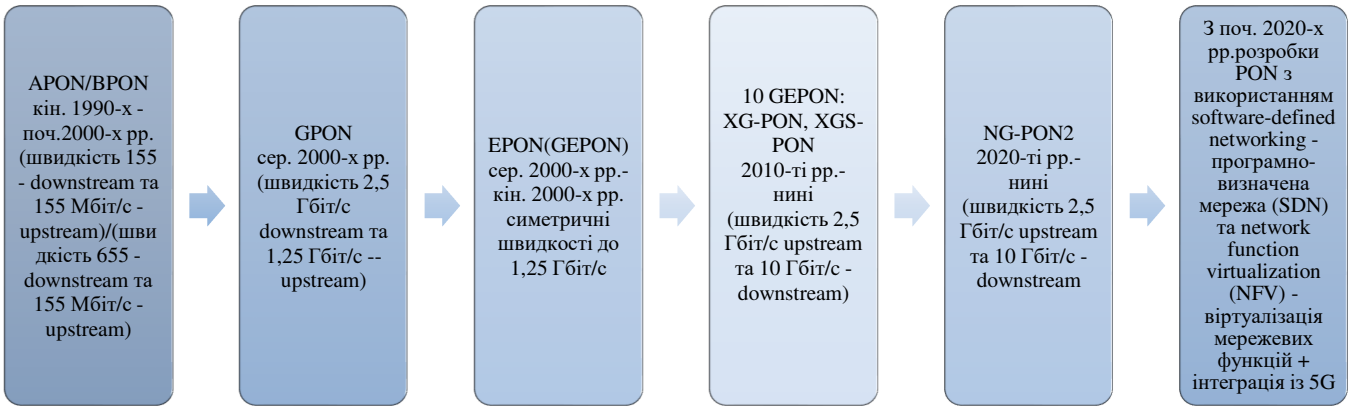


Рис. 4.4. Еволюція Pon-технологій передачі Інтернет-сигналу до споживача як сучасна потреба перебування на зв'язку

(складено автором за [273; 275; 276; 277; 278])

Технології PON різняться за швидкістю, аналізуючи основні характеристики технологій вдалося з'ясувати, що основними технологіями, які використовувалися впродовж 1990-2020 рр. у світі є наступні:

– APON, ще відома як ATM PON (Asynchronous Transfer Mode), одна із перших реалізацій технології PON, розгорнута наприкінці 1990-х рр. та стандартизована Міжнародним союзом електрозв'язку (МСЕ) (станадрт ITU-T G.983), що використовує асинхронний режим передачі (ATM) зі швидкістю низхідного потоку до 622 Мбіт/с і до 155 Мбіт/с висхідного потоку (надання широкосмугового доступу до Інтернету населенню та бізнесу);

– BPON (Broadband) – одна із перших версій реалізацієї технології PON, розгорнута з середини 2000-х рр., (станадрт ITU-T G.983), що використовує мультиплексування з часовим поділом каналів (TDM – Time Division Multiplexing) для передачі даних зі швидкістю низхідного потоку до 622 Мбіт/с і до 155 Мбіт/с висхідного потоку.

Технології APON та BPON нині неконкурентні за швидкісю із новими технологіями GPON, 10G-PON, якими пропонуються більш високі швидкості, збільшена пропускна здатність. Однак APON і BPON відіграли значну роль у ранній розробці та розгортанні технології PON, проклавши шлях до широкого впровадження мереж "оптоволокно до будинку" (FTTH) і "оптоволокно до приміщення" (FTTP) в усьому світі.

Далі розвиток Pon-технологій з передачі Інтернет-сигналу відповідно до потреб споживача та ринку у відповідностідо появи стандартів передачі даних та інноваційних технологічних розробок у галузі зв'язку:

– GPON (Gigabit Passive Optical Network) – гігабітна пасивна оптична мережа зі швидкістю низхідного потоку до 2,488 Гбіт/с та до 1,244 Гбіт/с висхідного потоку (використовується підприємствами, малим бізнесом)

– 10 GEPON (10 Gigabit Passive Optical Network) – 10-гігабітна пасивна оптична мережа стандартизована Інститутом інженерів з електротехніки та електроніки (IEEE) та Міжнародним союзом електрозв'язку (МСЕ) (стандарт IEEE 802.3av, ITU-T G.987), що більш відома як XG-PON або XGS-PON, похідна

GPON з більшою швидкістю низхідного потоку до 10 Гбіт/с та до 2,5 Гбіт/с висхідного потоку (зазвичай використовується в корпоративних мережах, багатоквартирних будинках, житлових районах з високою щільністю забудови);

– EPON, відома ще як GEPON-технологія (Gigabit Ethernet PON), стандартизована (IEEE – The Institute of Electrical and Electronics Engineers) (стандарт IEEE 802.3ah), що підтримує симетричні швидкості до 1 Гбіт/с як для низхідного, так і для висхідного трафіку (розгортається в бізнес- і корпоративних мережах, в житлових приміщеннях);

– NG-PON2 (Next Generation Passive Optical Network 2 (ITU-T G.989-series) система PON з номінальною сукупною пропускною здатністю 40 Гбіт/с у низхідному напрямку і 10 Гбіт/с у висхідному напрямку, стандартизована Міжнародним союзом електрозв'язку (МСЕ) (стандарт ITU G.989) [276];

– WDM-PON (мультиплексування з поділом по довжині хвилі) – технологія, що використовує мультиплексування з поділом по довжині хвилі (WDM) для збільшення пропускної здатності мережі, швидкостість може досягати кілька гігабіт на секунду на кожну довжину хвилі;

– TWDM-PON (мультиплексування з часовим і хвильовим розділенням) є вдосконаленою технологією PON, яка поєднує в собі методи мультиплексування з часовим поділом (TDM) і WDM, здатна підтримувати кілька довжин хвиль і часових інтервалів, при чому досягаючи ще більш високої швидкості та пропускної здатності у порівнянні з традиційними технологіями PON (можливість використання для житлових приміщеннях, а також розгортання високопродуктивних мереж підприємств і мегаполісів).

Міжнародним союзом електрозв'язку надана рекомендація ITU-T G.9802.1, що описує загальні вимоги до оптичних розподільних мереж (ODN) на основі мультиплексованих пасивних оптичних мереж з розділенням по довжині хвилі або WDM-PON. Система WDM PON (WRP) на основі WR-ODN складається з мультиплексування довжини хвилі кількох закінчення каналів (CT), кожна з яких забезпечує двонаправлене з'єднання через пару довжин хвиль, що утворюють пару каналів (CP). Використання технології WDM, WDM

PON дозволяє операторам підтримувати мінімальну кількість волокон, що призводить до значного зниження операційних витрат, наразі технологія важлива для інфраструктури 5G [275].

Наразі великі постачальники електронних комунікаційних хмарних послуг, зокрема, Amazon Web Services (AWS), Microsoft, Google і Facebook (Meta Platforms), використовують програмні контролери для зв'язку з базовим обладнанням і визначає, як маршрутизувати трафік в мережі (SDN). SDN – це розділення мережі на окремі площини управління (програмне забезпечення) та передачі даних (апаратне забезпечення). Перевагами програмно-визначених мереж (SDN) є нижча сукупна вартість володіння, відкритість і можливість програмування, гнучкість і маневреність, автоматизація і прозорість мережі [273; 278].

Не зважаючи на важкі умови функціонування, постачальники електронних комунікаційних послуг спромоглися пристосуватися, адаптуватися, до викликів, продовжуючи надавати послуги, а також сервіси населенню та бізнесу. Для стійкого забезпечення клієнтам доступу до Інтернет, постачальникам послуг, як нами зазаначалося вище було рекомендовано перейти на енергоощадливу та енергоефективну технологію xPON, динаміку та структуру фіксованого доступу до Інтернет у розрізі технологій використання за 2021-2023 рр., представлено на рис. 4.5.

Впродовж минулого року технічно модернізувалися лінії фіксованого доступу до Інтернет відповідно до потреб у продуктивних, енергонезалежних, енергоефективних мережах з одночасним усуванням наслідків пошкоджень мереж та інфрастуктури в результаті обстрілів та бойових дій, що потребувало значних капітальних вкладень.

За результатами дослідження динаміки та структури розподілу точок фіксованого доступу до Інтернет за технологіями, користуються попитом волоконно-оптичні підключення, так у 2023 році частка яких склала 88,1% (7,1 млн. од) від загальної кількості підключень і розподілилася між технологіями FTTx (46,8%) та xPON (41,3%).

Цифровізація, гармонізація із стратегічним баченням розбудови загальноєвропейської енергоефективної мережі в поєднанні з викликами енергосистемі України в результаті бойових дій на території країни, посилюють потребу впровадження енергоефективних технологій через ймовірність руйнування об'єктів енергетичної інфраструктури та пришвидшують гігібітне підключення до глобальної мережі.

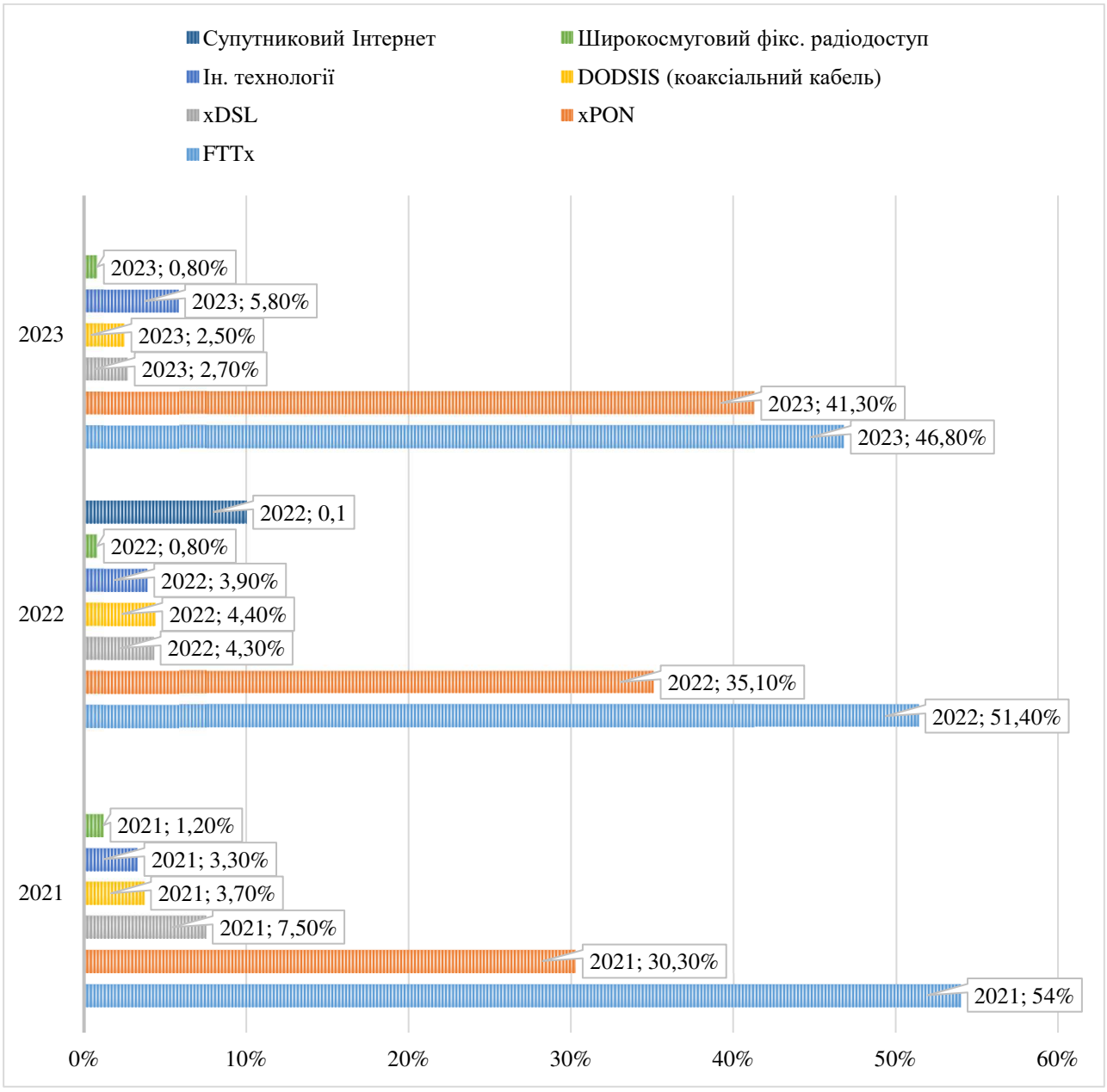


Рис. 4.5. Динаміка та структура фіксованого доступу до Інтернет у розрізі технологій використання за 2021-2023 рр.

(побудовано автором за [298; 299; 300; 301])

У 2023 році використання волоконно-оптичного кабелю за технології xPON зросло на 17,7%, а FTTx скоротилося на 9%. Варто зауважити, що із отриманих у 2023 році 97,3 млрд грн доходів від послуг електронних комунікацій, 36,9 млрд грн (приріст на 4,2% до 2022 р.) припадає на мобільний Інтернет та 21 млрд грн на фіксований (приріст на 33%).

Попит на доступ до мережі Інтернет сприяє появі нових постачальників послуг, так в Україні зареєстровано більше, ніж 8000 постачальників електронної комунікаційної послуги Інтернет. Глобальна мережа складається із кількох незалежних систем, які з'єднуються в одну, відповідно Інтернет-постачальники працюють на трьох рівнях Tier-1, Tier-2, Tier-3, опис рівнів наведено у табл. 4.4.

Таблиця 4.4

Ієрархія рівнів Інтернет-провайдерів

Назва рівня	Характеристика
Tier-1	Міжконтинентальні глобальні провайдери, які об'єднують весь трафік, забезпечуючи передачу даних по всьому світу. Обмін інформацією між континентами відбувається за допомогою підводної кабельної лінії електронних комунікацій, що лежить на дні океанів. Провайдери першого рівня обмінюються даними безпосередньо через однорангову піринговy мережу та виступають рівноправними учасниками з'єднання.
Tier-2	Національні постачальники послуг зв'язку, що купують трафік у провайдерів першого рівня та продають регіональним компаніям-постачальникам послуг ЕК.
Tier-3	Місцеві (локальні) провайдери, що надають послугу підключення до інтернету кінцевому користувачеві, залежать від постачальників перших двох рівнів.

(складено автором за [264; 277])

Оскільки швидкість інтернет-з'єднання є найкращим показником якості послуги, нами проаналізовано швидкість завантажень та вивантажень даних при підключенні до постачальників електронних комунікацій (табл. 4.5), за фіксацією та виміром швидкості онлайн інтернет-трафіку – спідтест (від англ. "speed test" – тест швидкості).

Таблиця 4.5

Швидкість Інтернету постачальниками електронних комунікацій в Україні

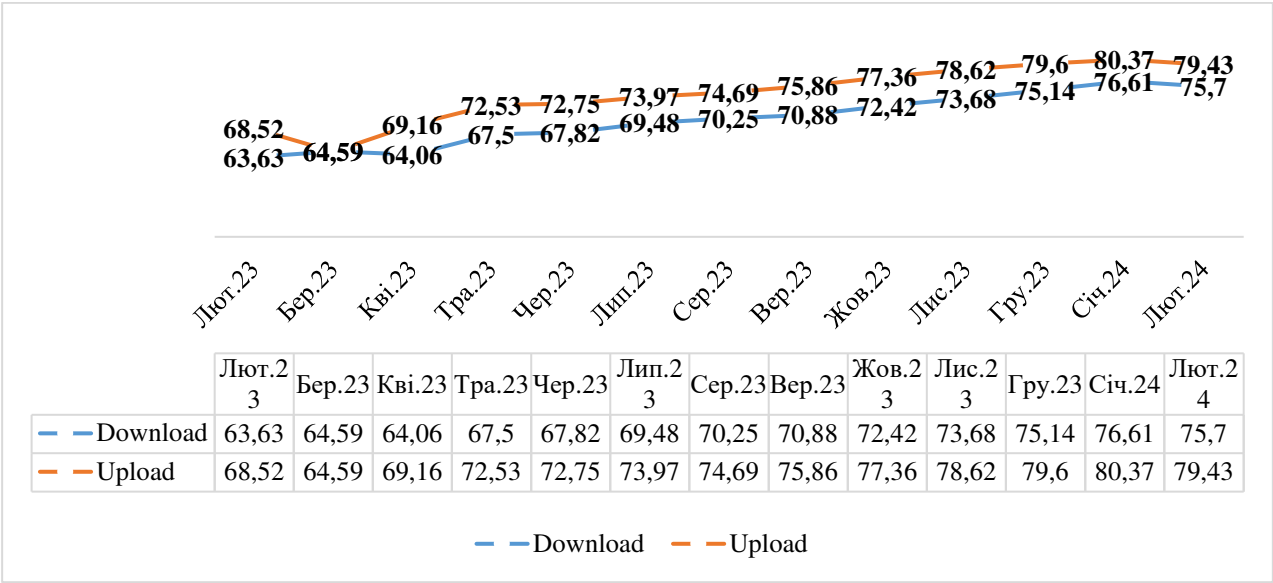
№ з/п	Оператор	Швидкість завантаження (Download)	Швидкість відправлення (Upload)	Pon-технологій передачі Інтернет-сигналу
1.	АТ “Київстар”	34.35	36.42	FTTx/GEPON/Ethernet
2.	ПАТ “ВФ Україна”	30.51	21.25	Оптика/PON
3.	ТОВ “Лайфселл”	12.61	4.34	2G/3G/4G
4.	АТ “Укртелеком”	44.37	46.19	GPON
5.	ІСП “Триолан”	87.05	77.82	Ethernet, GEPON
6.	ТОВ “Ланет Нетворк”	153.96	145.59	EPON
7.	ПАТ “Індастріальна Медіа Нетворк”	151.06	181.80	GPON/ Ethernet
8.	ТОВ “НПП “ТЕНЕТ”	55.33	52.58	GPON
9.	ТОВ “ВОЛЯ-Кабель”	65.22 Мбіт/с	36.27	FTTx/GEPON/Ethernet
10.	ІСП “Фрегат”	39.44	36.02	Можливість підключення GPON
11.	ТК група “Vega”	96.36	103.01	FTTx/GEPON/Ethernet
12.	ТОВ “Фрінет”	62.04	77.19	Оптика/PON, Ethernet/FTTx
13.	ТОВ “First Telecommunication Company”	58.13	51.98	FTTx/GEPON/Ethernet
14.	ПАТ “Датагруп”	43.14	50.15	FTTx/GEPON/Ethernet
15.	ДП “Уарнет” НТЦ	49.49	45.52	Radio/Wi-Fi (outdoor)
16.	НВО “Інформаційні технології”	37.96	33.72	Ethernet з можливістю переходу на PON

(складено автором за [279; 280; 283; 284; 285; 286; 287; 288; 289; 290; 291; 292; 293; 294])

Швидкості завантаження даних download та відправлення вихідних даних – upload є показниками, за якими обирається Інтернет провайдер, часто фіксується час проходження пакету даних від пристрою глобальною мережею до сервера та їх повернення – ping (швидкість вказує на час очікування завантаження сторінки).

За результатами тестування, найшвидше послуга Інтернет надається провайдером фіксованого широкосмугового доступу “Ланет”, при чому провайдер залишається лідером впродовж останніх років та має швидкісну спроможність близько 400 Мбіт/с. Телекомунікаційна група “Vega” наступна за швидкістю зі спроможність близько 350 Мбіт/с, а наступна компанія “Індастріальна Медіа Нетворк” (IPnet) із швидкістю близько 325 Мбіт/с. Результати тестування швидкості завантажень та відправлень дещо відрізняються, проте підтверджують заявлені компаніями швидкісні спроможності. Попри значну кількість підключень споживачів до провайдерів Volia, Triolan та “Фрінет” (O_3), швидкість надання компаніями послуги залишається доволі низькою, хоча вони мали б працювати у напрямку її збільшення.

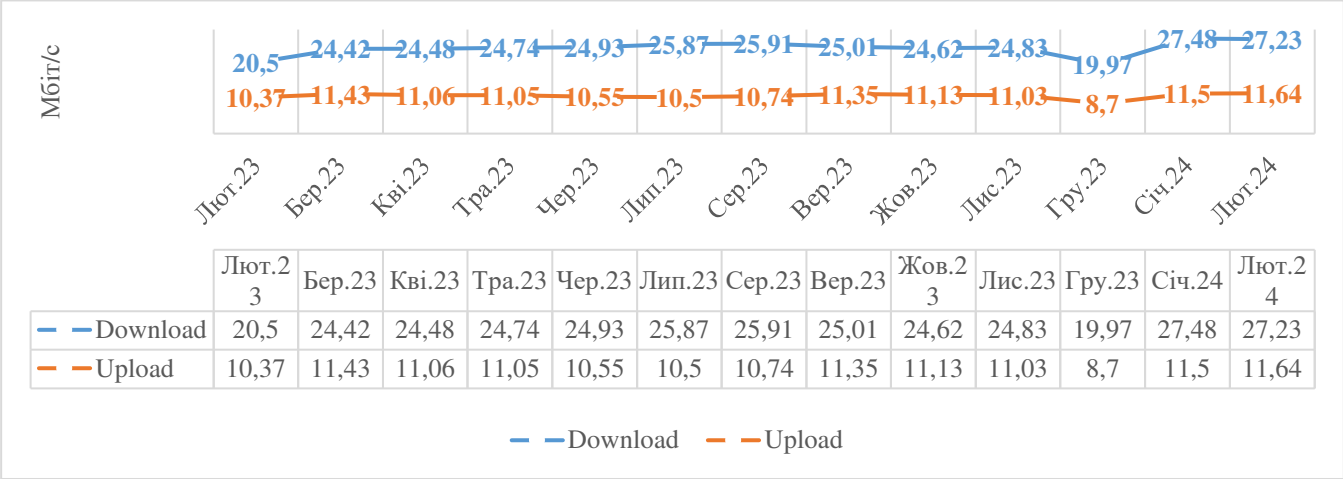
За даними світового рейтингу тестування швидкості Інтернет Speed Test Global Index Україна посідає 88 місце за швидкістю мобільного Інтернету та відповідно 76 за фіксованим широкосмуговим доступом до глобальної мережі (рис. 4.6 та рис. 4.7)



	Лют.23	Бер.23	Кві.23	Тра.23	Чер.23	Лип.23	Сер.23	Вер.23	Жов.23	Лис.23	Гру.23	Січ.24	Лют.24
Download	63,63	64,59	64,06	67,5	67,82	69,48	70,25	70,88	72,42	73,68	75,14	76,61	75,7
Upload	68,52	64,59	69,16	72,53	72,75	73,97	74,69	75,86	77,36	78,62	79,6	80,37	79,43

Рис. 4.6. Середня швидкість фіксованого широкосмугового Інтернету (лютий 2023 – лютий 2024 рр.), Мбіт/с

(побудовано автором за [279])



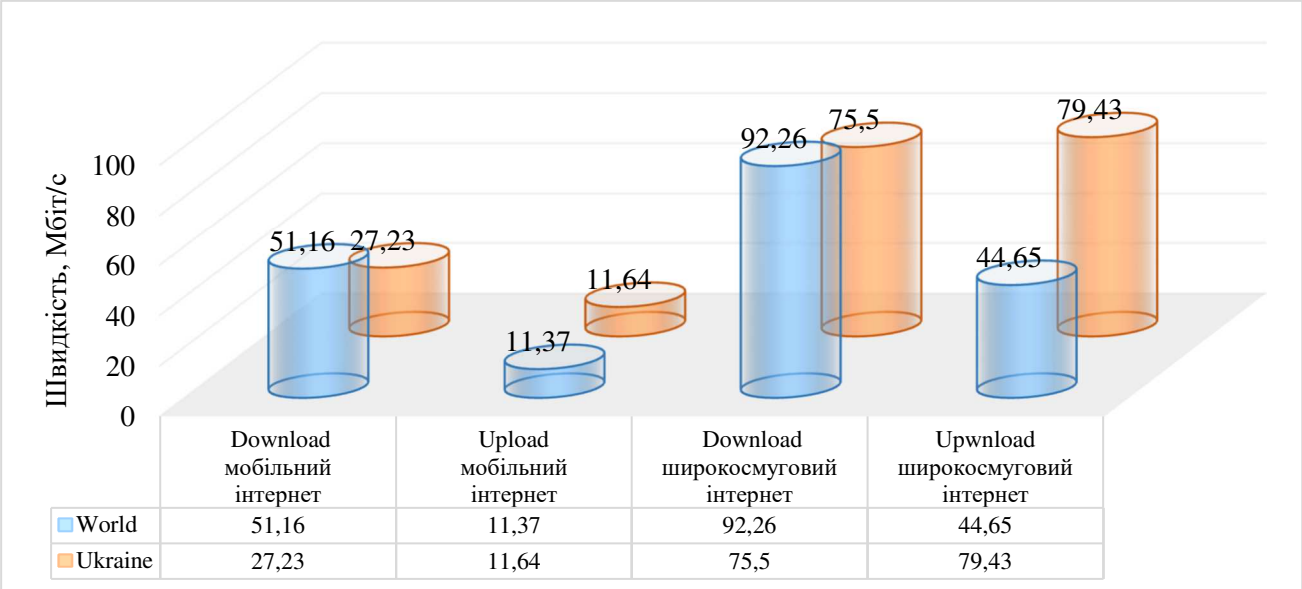
	Лют.23	Бер.23	Кві.23	Тра.23	Чер.23	Лип.23	Сер.23	Вер.23	Жов.23	Лис.23	Гру.23	Січ.24	Лют.24
Download	20,5	24,42	24,48	24,74	24,93	25,87	25,91	25,01	24,62	24,83	19,97	27,48	27,23
Upload	10,37	11,43	11,06	11,05	10,55	10,5	10,74	11,35	11,13	11,03	8,7	11,5	11,64

Рис. 4.7. Середня швидкість мобільного Інтернету (лютий 2023 – лютий 2024 рр.), Мбіт/с

(побудовано автором за [279])

Для участі у рейтингу локації повинні мати щонайменше 300 унікальних результатів від користувачів мобільного або фіксованого широкосмугового зв'язку.

Зважаючи на орієнтир оцифровізації послуг та визнання країни лідером у цифровій розбудові держави, проведемо аналіз середніх значень швидкості мобільного та широкосмугового Інтернету у світі та Україні (рис. 4.8).

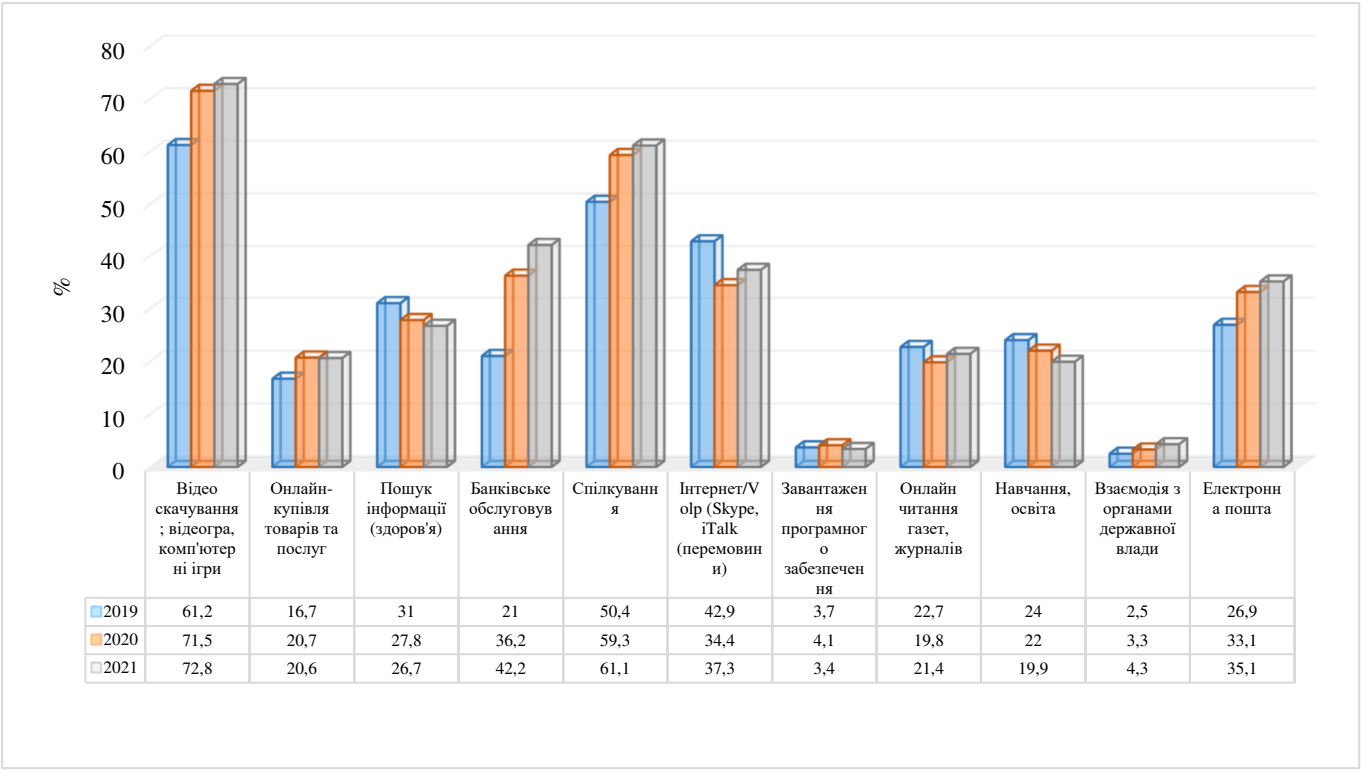


	Download мобільний інтернет	Upload мобільний інтернет	Download широкосмуговий інтернет	Upwnload широкосмуговий інтернет
World	51,16	11,37	92,26	44,65
Ukraine	27,23	11,64	75,5	79,43

Рис. 4.8. Середні значення швидкості мобільного та широкосмугового Інтернету в світі та Україні (лютий 2023 – лютий 2024 рр.), Мбіт/с

(побудовано автором за [279])

Швидкісна спроможність широкосмугового доступу до Інтернет на рівні завантажень становить 92,26 у світі та 75,5 Мбіт/с в Україні, а відправлень – 44, 65 та 79,43 Мбіт/с відповідно. Із передачею даних та завантаженням гірше у разі користування мобільного Інтернету, а саме: завантаження – 51,16 в світі та 27, 23 Мбіт/с в Україні та майже однаково під час відправлень – 11,37 та 11,64 Мбіт/с відповідно (рис. 4.9). Зважаючи на те, що країна розбудовується та розвивається, почала впроваджувати розробки, технології дещо пізніше від високорозвинутих, можемо вважати, що місце у рейтингу та задукоментовані швидкості засвідчують спроможність країни діджиталізуватися.



	Відео скачування; відеогра, комп'ютерні ігри	Онлайн-купівля товарів та послуг	Пошук інформації (здоров'я)	Банківське обслуговування	Спілкування	Інтернет/Volp (Skype, iTalk (перемовини)	Завантаження програмного забезпечення	Онлайн читання газет, журналів	Навчання, освіта	Взаємодія з органами державної влади	Електронна пошта
2019	61,2	16,7	31	21	50,4	42,9	3,7	22,7	24	2,5	26,9
2020	71,5	20,7	27,8	36,2	59,3	34,4	4,1	19,8	22	3,3	33,1
2021	72,8	20,6	26,7	42,2	61,1	37,3	3,4	21,4	19,9	4,3	35,1

Рис. 4.9. Динаміка Інтернет-запитів користувачами глобальної мережі впродовж 2019-2021 рр.

(побудовано автором за [281])

Досліджуючи розріз користування послугою Інтернет, найбільший відсоток клієнтів (мається на увазі населення, що користується Інтернет) запитують скачування відео, комп’ютерних ігор 61,2 % в 2019 р., при чому послуга користується попитом, відсоток скачувань зріс до 72,8%. На другому місці – спілкування 50,4% та 61,1% у 2019 та 2021 рр. відповідно), перемовини в

онлайн режимі – 42,9% у 2019 до 37,3% у 2021 рр., електронна пошта у 2019 р. 26,9% та 35,1% у 2021 р. Найбільш популярним контентом для аудиторії залишаються розваги та спілкування.

За аналізом підключень (у особи наявний один мобільний або смарт-телефон не менш, як із однією Sim-карткою для власного користування), спираючись на дані Міжнародного союзу електрозв'язку, розподіл за місцевістю вказує на випередження підключень у міській зоні в противагу сільській (91,3% проти 89,6%), за гендером – підключень жінок більше, ніж чоловіків (91% жінок проти 90,4% чоловіків), але це пояснюється кількісним переважанням населення жіночої статі на території країни (рис. 4.10).

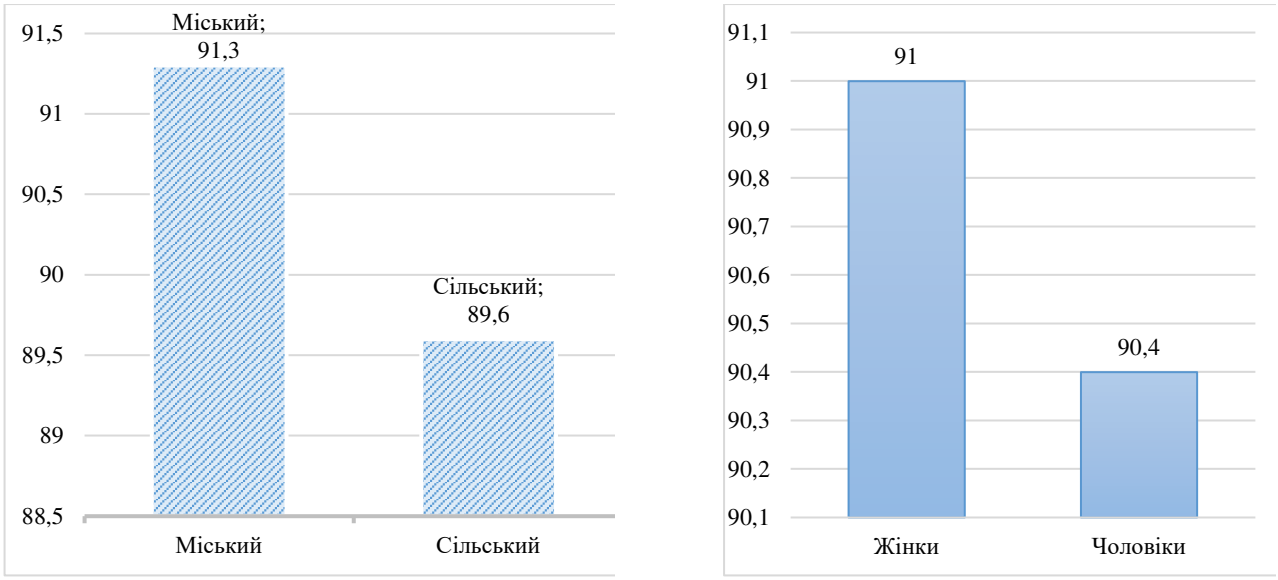


Рис. 4.10. Кількість осіб-власників мобільних або смарт-телефонів за місцевим охопленням та статтю в Україні у 2021 р., %

((побудовано автором за [296; 297])

Сумарно за всіма активними аналоговими фіксованими телефонними лініями налічується 1,739 млн користувачів, користувачів мобільного стільникового зв'язку - 49,304 млн. осіб, підписок на фіксований, а також мобільний широкосмуговий доступ – 7,19 млн й 4,5 млн користувачів відповідно.

Як нами вже з’ясовано впродовж останніх років продовжує зберігатися позитивна динаміка у використанні голосового зв’язку, кількість підписок у 2022 році у розрізі: стаціонарний, мобільний стільниковий зв’язок, фіксований і мобільний широкосмуговий зв’язок представлено на рис. 4.11.

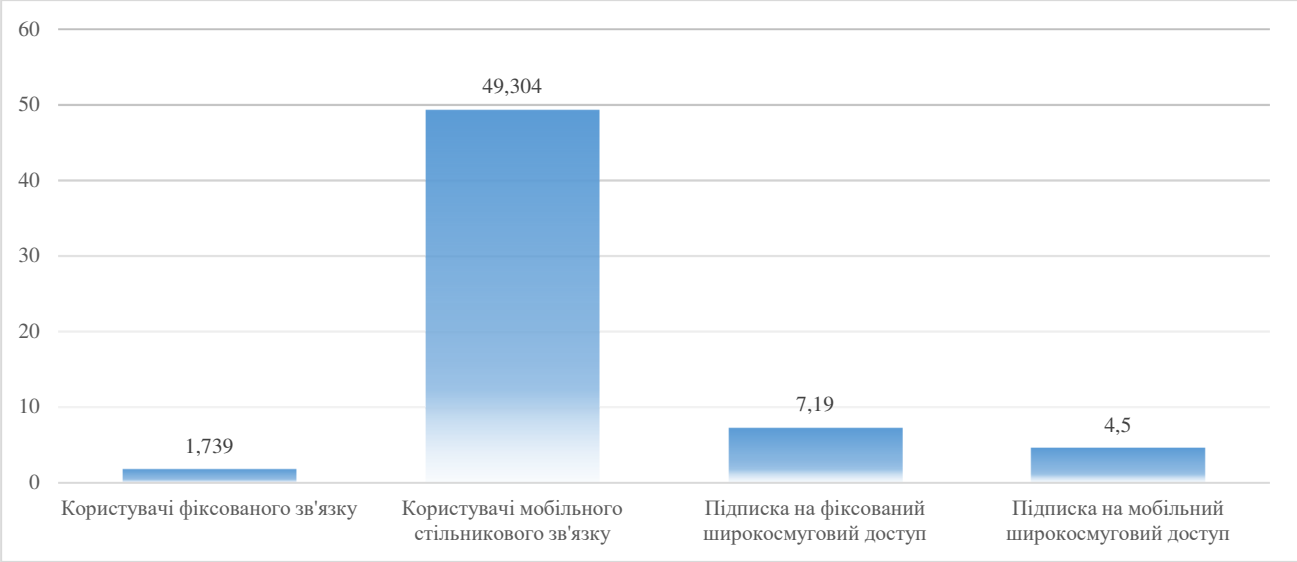


Рис. 4.11. Кількість користувачів фіксованого, мобільного стільникового зв’язку та підписок на фіксований і мобільний широкосмуговий доступ за 2022 р., млн. користувачів

((побудовано автором за [296; 298])

Відображення підписок на передачу голосу через IP (VoIP), на фіксовану бездротову локальну мережу (WLL), еквівалентів голосового каналу ISDN, фіксованих публічних таксофонів і підписок на супутниковому зв’язку, наданих у фіксованих місцях, де підтримується голосовий зв’язок дозволяє зробити висновок, що мобільний зв’язок є більш затребуваним через доступність послуги не залежно від місця перебування користувача (за умов доступності послуг, покриття) у порівнянні із фіксованим зв’язком. Проте, у разі доступу до глобальної мережі, ситуація складається навпаки, підписок на фіксований широкосмуговий доступ більше, переважаючи у 1,6 разів підписки на мобільний широкосмуговий зв’язок, що пояснюється по-перше, ранніми підключеннями до фіксованих ліній передачі, по-друге – більш високою якістю послуги, а саме

швидкістю передачі даних, що нами розглядалося раніше (швидкості завантажень, вивантажень даних).

Доцільно проаналізувати ринок, основних постачальників електронних комунікаційних послуг, динаміку доходів, яких пердставлено у табл. 4.6.

Таблиця 4.6

Динаміка доходів основних постачальників електронних комуніаційних мереж та послуг за 2021-2023 рр.

Постачальник	Тип компанії за розміром	Роки					
		2021		2022		2023	
		Обсяг доходів, грн	Відносний приріст	Обсяг доходів, грн	Відносний приріст	Обсяг доходів, грн	Відносний приріст
ПрАТ “КИЇВСТАР”	Велике та середнє підприємництво	28 559 150 000	14%	30 900 973 000	8%	33 165 048 000	7%
ПрАТ “ВФ Україна”	Велике та середнє підприємництво	19 358 958 000	12 %	18 802 655 000	-3 %	20 265 622 000	8 %
ТОВ “ЛАЙФСЕЛЛ”	Велике та середнє підприємництво	8 482 687 000	24 %	9 411 748 000	11 %	11 712 123 000	24 %
АТ “УКРТЕЛЕКОМ”	Велике та середнє підприємництво	5 279 923 000	-3 %	4 394 064 000	-17 %	4 164 529 000	-5 %
ДП “УКРАЇНСЬКИЙ ДЕРЖАВНИЙ ЦЕНТР РАДІОЧАСТОТ”	Велике та середнє підприємництво	756 756 000	7 %	936 724 000	24 %	2 021 544 000	116 %
ТОВ “ВОЛЯ-КАБЕЛЬ”	Велике та середнє підприємництво	2 057 306 000	2 %	1 935 690 000	-6 %	1 911 457 000	-1 %
ТОВ “ЦЕНТР ГЛОБАЛЬНИХ ПОВІДОМЛЕНЬ Україна”	Велике та середнє підприємництво	1 528 424 000	19 %	1 296 828 000	-15 %	1 573 524 000	21 %
ПрАТ “ДАТАГРУП”	Велике та середнє підприємництво	1 374 015 000	7 %	1 204 752 000	-12 %	1 561 840 000	30 %
ТОВ “ХУАВЕЙ Україна”	Велике та середнє підприємництво	1 308 037 000	0 %	1 293 587 000	-1 %	1 178 548 000	-9 %
ТОВ “ПРОКСІМУС”	Велике та середнє підприємництво (мале та мікро-підприємство до 2022 р.)	298 614 700	266 %	241 989 400	-19 %	770 222 000	218 %
Інші постачальники	–	12 684 129 300	–	14 074 576 600	–	18 975 543 000	–
Всього	–	81 688 000 000	–	83200000 000	–	97300000 000	17%

(складено автором за [306])

Серед лідерів за обсягами доходів у галузі залишається так звана “четвірка”: ПрАТ “Київстар”, ПрАТ “ВФ Україна”, ТОВ “ЛАЙФСЕЛЛ”, АТ “УКРТЕЛЕКОМ”. Слід відзначити, що не дивлячись на надскладні умови функціонування компаній-постачальників послуг, відзначається позитина динаміка доходів компаній у електронно-комунікаційний сектор, так ПрАТ “ВФ Україна” у 2023 році збільшила доходи у порівнянні з 2022 роком на 8%, в рік повномасштабного вторгнення агресора на територію країни відбулося зниження доходів на 3%. Найбільших фінансових втрат у рік вторгнення зазнали АТ “Укртелеком” (-17%), ТОВ “Воля-Кабель” (-6%), ТОВ “Центр глобальних повідомлень Україна” (-15%), ПрАТ “Датагруп” (-12%), ТОВ “Проксімус” (-19%), ТОВ “Хуавей Україна” (-1%).

Майже всі підприємства відновили приріст доходів вже через рік, окрім: АТ “Укртелеком”, відносний приріст на 5% менше за 2022 рік, ТОВ “Воля-Кабель” на 1% та ТОВ “Хуавей Україна” на 9% приріст менше, ніж у 2022 році.

Частки постачальників на ринку надання електронних комунікаційних послуг за обсягами доходів у 2023 р. розподілилися наступним чином (рис. 4.12).

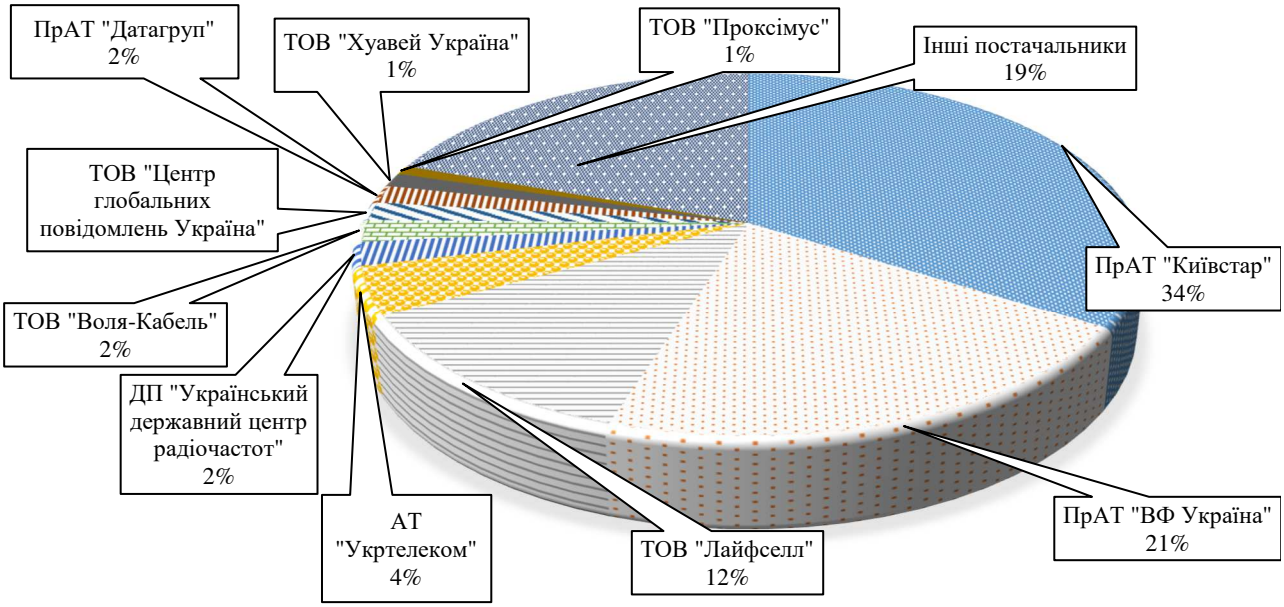


Рис. 4.12. Структура ринку постачальників електронних комунікаційних послуг за обсягами доходів у 2023 р.

(побудовано автором за [298; 305])

Аналізуючи частки постачальників послуг на ринку виокремлюється трійка: ПрАТ “Київстар”, ПрАТ “ВФ Україна”, ТОВ “ЛАЙФСЕЛЛ”, долі яких складають 34%, 21% та 12% відповідно, а разом на них припадає 67% обсягів доходів у секторі електронних комунікацій. Попри темп інфляції, що сумарно за 2022 та 2023 рр. склав 31,7%, доходи зросли на 17%, що підтверджує потребу населення та бізнесу перебування на зв’язку. Крім того, постачальниками розбудовується та відновлюється мережа, обсяги капіталовкладень у минулому році склали 18,9 млрд грн, що у 1,5 рази більше від обсягів інвестицій у 2022 році.

Огляд та аналіз стану сектору електронних комунікаційних послуг дозволив зробити висновок про позитивну динаміку, оскільки загальні доходи у 2023 році зросли на 17% та склали 97,3 млрд грн, що пов’язано із приростом за рахунок:

– у першу чергу, доступу до фіксованої мережі Інтернет (обсяг доходів – 21,2 млрд грн, приріст доходів по відношенню до 2022 року на 33%);

– зростання доходів від мобільного зв’язку на 9,8% (виручка у 2023 році становила 61,7 млрд грн проти 56,7 у 2022 році) за рахунок активного користування національного роумінгу та міжнародного, кількість користувачів становила близько 2 млн та 4 млн на добу, а доходи від міжнародного роумінгу у 2023 році зросли на 1,3 рази та становили 3,69 млрд грн проти 2,91 млрд грн у 2022 році;

– збільшення доходів від надання послуг: технічного обслуговування на – 8,6%, користування ліній електрозв’язку мереж електронних комунікацій на – 2,9%, користування каналів електрозв’язку на – 1,3%, користування кабельної каналізації електрозв’язку на – 2,9%.

Зменшення доходів на 5,7% відбулося за послугою фіксованого голосового зв’язку, обсяг яких у 2023 році склав 3,3 млрд грн через зменшення попиту на фіксовану телефонію. Відтік клієнтів відбувається з причини руйнувань інфраструктури мережі та довготривалістю відновлення ліній зв’язку, які надаються за аналоговими технологіями. В свою чергу це пояснює зростання

попиту на технології xPON на 17,7%, яка наразі сприймається як можливість енергоефективного та стабільного користуватися послугою Інтернет у разі відсутності енергопостачання.

Слід відзначити також роботу у напрямку забезпечення безперебійної роботи, передусім для об'єктів критичної інфраструктури, яким має надаватися зв'язок у разі пошкоджень або руйнувань об'єктів енергетики. Постачальники модернізують мережі, а також закуповують генератори, за даними НКЕК, ПрАТ "Київстар", ПрАТ "ВФ Україна", ТОВ "Лайфселл", АТ 'Укртелеком", ПрАТ "Датагруп" збільшили кількість генераторів до 6 049 од. (більше на 2 549 од., ніж у 2022 році), акумуляторних батарей — до 385 551 од. (збільшили кількість на 129 584 од. у порівнянні з 2022 роком) [305].

Слід зазначити на розгортання мереж нового покоління 3, 4 та 4,5G національними постачальниками електронних комунікаційних послуг в Україні. (рис. 4.13)

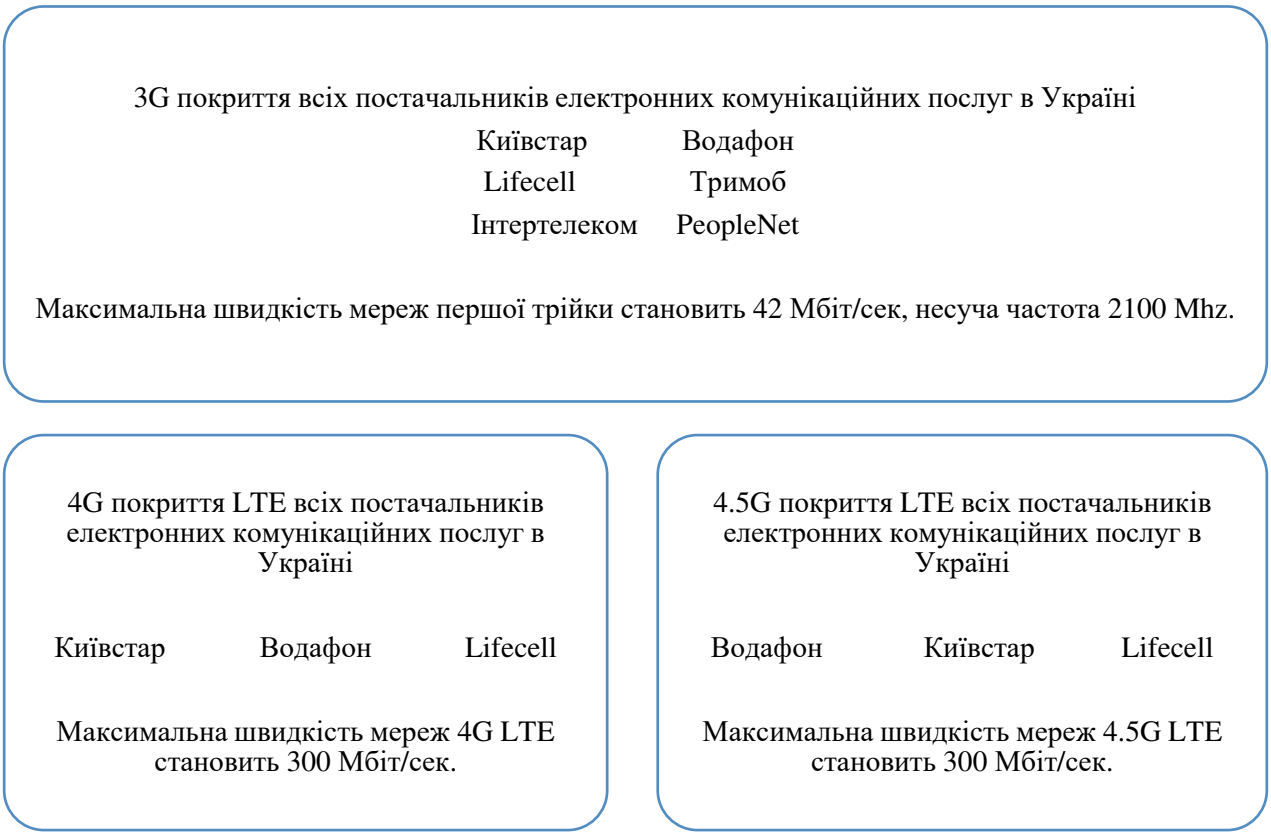


Рис. 4.13. Розподіл розгортання мережі 3 та 4G підприємствами-постачальниками електронних комунікаційних послуг в Україні

(складено автором)

Послуга 4 та 4,5G (LTE Advanced) надається трьома постачальниками, які відповідно є основними гравцями на ринку послуг зв'язку, які працюють в межах діапазонів: LTE діапазон 3 – 1800 Mhz; діапазон LTE 7 – 2600 МГц; діапазон LTE 8 – 900 МГц, а максимальна швидкість мереж 4.5G LTE становила 300 Мбіт/сек [319]. Подвоєння швидкості забезпечувалося агрегацією несучих частот: LTE band 3 – 1800 Mhz і LTE band 7 – 2600 Mhz (доступ можливий у містах з покриттям у двох діапазонах), крім того, сигнал діє на відстані 35 км від базової станції.

Отже, компанії "Київстар", "Водафон", "Лайфселл" є лідерами на ринку постачальників електронних комунікаційних послуг через прогресивність використання технологій, що особливо важливо в умовах цифровізаційних змін, розбудови е-держави, активного використання розумних мереж, великих даних, штучного інтелекту з причин затребуваності якісного швидкісного зв'язку для можливості їх використання.

4.2. Моніторинг безпекової площини українських підприємств-постачальників електронних комунікаційних послуг

Наша країна постала перед викликами, які впливають на процеси, що відбуваються на всіх рівнях: глобальному, міжнародному, державному, на рівні суб'єктів господарювання, суспільства, а також окремого індивіда. Постає проблема захисту інформаційного поля, оскільки надзвичайний інтерес щодо порушення функціонування суб'єктів господарювання виникає у кіберпросторі, нині надзвичайно високими є ризики у функціонуванні об'єктів критичної інфраструктури та підприємств.

Глобалізація та цифровізація, пандемія, війна підкреслили важливість питань, що стосуються базового соціального забезпечення, котрі визначаються

рівнем доступу до інфраструктури (в сфері транспорту, зв'язку, освіти, здоров'я, фінансів), а також зачіпають господарюючі суб'єкти [358; 367].

Сфера електронних комунікацій слугує невід'ємним компонентом у діяльності всіх підприємств, крім того, відіграє особливу роль, оскільки забезпечує безперебійне функціонування всіх економічних суб'єктів в нестійких умовах функціонування. Крім того, галузь зв'язку визначається критично важливим сектором, оскільки забезпечує допоміжну функцію у всіх секторах інфраструктури, оскільки саме за рахунок послуг електронних комунікацій стає можливим виконання певних задач на відстані (проведення зустрічей, підписання документів, укладання угод, оплати, замовлення, купівель і т.д.)

Законодавчо роль інформаційних технологій визначено Законом України "Про критичну інфраструктуру" [256], де інформаційні технології виокремлено як один із 16 критично важливих секторів критичної інфраструктури. За Законом України серед критично важливих послуг – інформаційні послуги та електронні комунікації. У переліку секторів (підсекторів), основних послуг критичної інфраструктури країни знаходиться й інформаційний сектор (рис. 4.14).

Крім того, функціонування господарюючих суб'єктів нині відбувається на межі активної євроінтеграційної гармонізації законодавства та формування відповідності у провадженнях діяльності, до вимог ринку, а також нагальною потребою в адаптації до невизначених умов сучасності, в яких перебувають всі без виключення підприємства та організації.

Електронні комунікаційні послуги, що надаються постачальниками зв'язку, наразі забезпечуються завдяки взаємному поєднанню мереж: наземних, бездротових, супутникових, які є взаємодоповнюючими та залежними термінацією трафіку, взаємним доступом та використанням технологій та можливостей задля якісного забезпечення своєї роботи – надання послуг, взаємопов'язаних цифрових й електронних операцій.

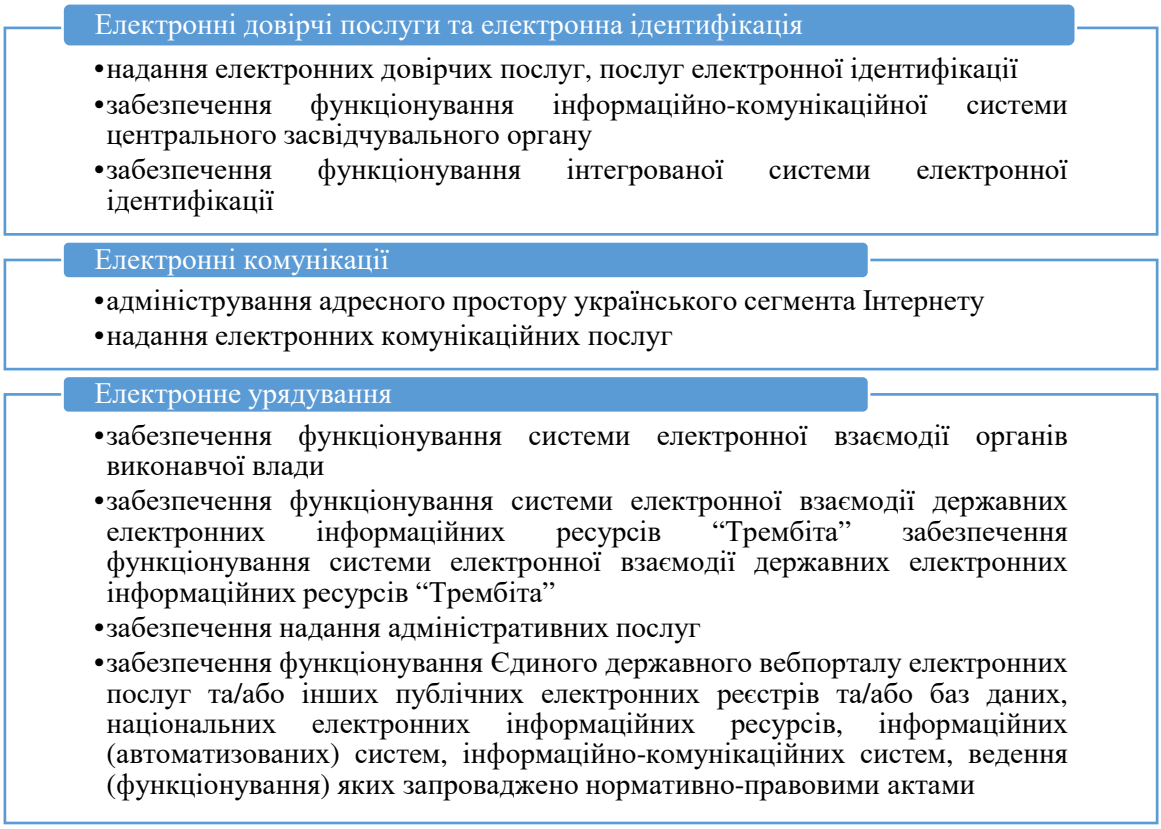


Рис. 4.14. Місце електронних комунікації у переліку секторів критичної інфраструктури країни

(складено автором за [256; 384])

Саме завдяки перебуванню на зв'язку населення та підприємств за умов невизначеності дозволяє підприємствам, установам, організаціям виконувати свої функціональні обов'язки, продовжувати провадити діяльність. Тому надважливим залишається питання безпеки підприємств-постачальників на ринку електронних комунікаційних послуг. З метою визначення безпекової площини функціонування постачальників послуг сфери електронних комунікацій доцільно провести моніторинг результатів їх діяльності, оцінити показники безпеки за складовими з подальшим аналізом для виявлення прогалин й пошуку шляхів щодо їх усуненння. За результатами аналізу прибутку постачальників електронних комунікаційних послуг впродовж 2018-2022 рр., вдалося встановити, що за обсягами доходів впродовж досліджуваного періоду серед лідерів залишається компанія "Київстар" (табл 4.7, рис. 4.15).

Таблиця 4.7

Динаміка прибутку постачальників електронних комунікаційних послуг впродовж 2018-2022 рр., тис. грн

Постачальник електронних комунікаційних послуг	Роки									
	2018		2019		2020		2021		2022	
	Обсяг	Темп росту, %	Обсяг	Темп росту, %	Обсяг	Темп росту, %	Обсяг	Темп росту, %	Обсяг	Темп росту, %
ПрАТ “Київстар”	8 294 385	–	10 679 283	128,75	13 005 618	121,78	13 937 797	107,17	11 715 425	84,06
ПрАТ “ВФ Україна”	2 357 254	–	2 792 869	118,48	5 027 124	179	4 851 664	96,51	1 363 426	28,1
ТОВ “Лайфселл”	-608 416	–	-1 134 151	-186,41	6958	0,61	752 052	10808,45	1188104	157,98
ПАТ “Укртелеком”	576 175	–	-988 066	171,49	-2621669	265,33	512 226	19,54	-28 521 67	-556,81
“Датагруп”	29541	–	175811	595,14	232 879	132,46	204 586	87,85	-147 291	- 71,99

(складено автором за [306])

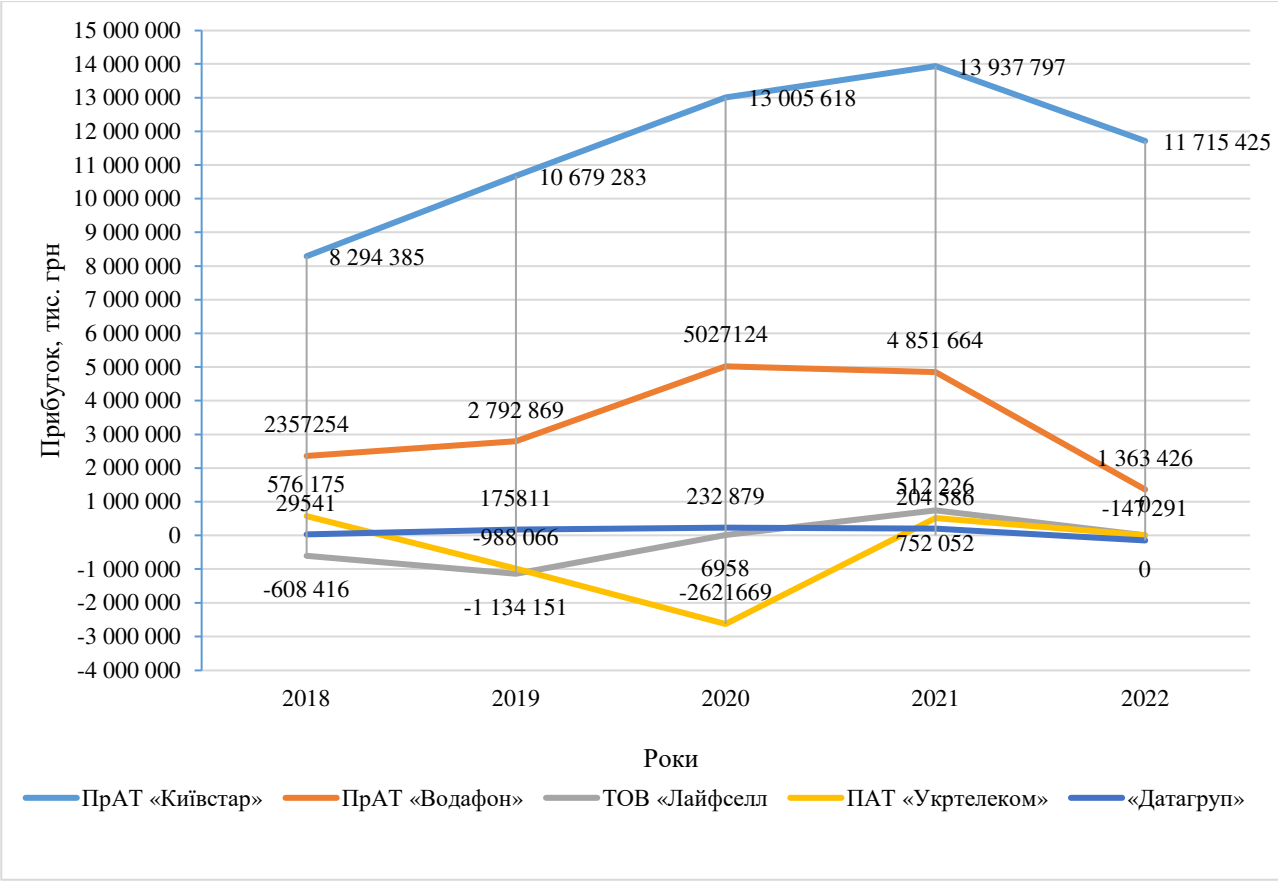


Рис. 4.15. Динаміка обсягів прибутку постачальників електронних та комунікаційних послуг впродовж 2018-2022 рр., тис. грн

(складено автором за [306])

Отже, лідером за обсягами доходів залишається компанія “Київстар”, упродовж досліджуваного періоду.

Складові безпеки, що замикають безпекову площину цільових результатів оцінюватимуться за коефіцієнтами, для того, щоб надати єдину вимірність. Крім того, відносні коефіцієнти надають більш інформативну картину щодо показників та віддачі від вкладень, затрат, зусиль, в противагу абсолютним, які демонструють загальну картину щодо досліджуваного показника.

Коефіцієнт лояльності клієнтів визначатиметься за результатами опитування, що проводитиметься через Net Promoter Score (NPS) (рис. 4.16)

Рис. 4.16. Індекс лояльності за результатами опитування

(складено за результати опитування за використання surveymonkey.com/mp/nps-calculator/)

У порожньому полі зазначається назва компанії постачальника продукту чи послуги. Задана шкала оцінок дозволяє респонденту обрати число від 0 (найменша ймовірність рекомендації) до 10 (найбільша ймовірність рекомендації), відповіді групуються за наступними групами споживачів:

1) задоволені споживачі – промоутери (споживачі послуг присуджують бал 9 або 10);

2) задоволені, проте нейтрально налашовані споживачі послуг, яких легко переконати перейти до іншого постачальника послуг, якщо зміниться ціна, якість чи спрацює реклама(бал 7 чи 8);

3) незадоволені споживачі – критики, обирають оцінку від 0 до 6.

Показник визначає ймовірність надання рекомендацій компанії, розраховується за наступною формулою (4.1):

$$\text{NPS} = \text{відсоткова частка промоутерів} - \text{відсоткова частка критиків} \quad (4.1)$$

Частка промоутерів визначається як (формула 4.2.):

$$\text{Частка промоутерів} = \left(\frac{\text{кіл–ть промоутерів}}{\text{загальна кіл–ть респондентів}}\right) \text{x } 100\ \% \quad (4.2)$$

Показник NPS варіює в межах від -100 до 100, та визначається кількісним вираженням оцінок клієнтів та їх розподілу (табл. 4.8).

Таблиця 4.8

Нормативні значення індексу лояльності за сферами

Показник	Професійні послуги (юридичні, страхові, фінансові, банківські)	IT-компанії (послуги зв'язку, виробники ком'пютерів)	Споживачі товарів та послуг (торгівля)
$NPS_{сер}$	+43	+35	+43
$NPS_{мед}$	+50	+40	+50
Верхній квартиль	+73 та більше	+64 та більше	+72 та більше
Нижній квартиль	+19 і менше	+11 і менше	+21 і менше

(складено автором за використання surveymonkey.com/mp/nps-calculator])

Даний показник входить до складової ринкової безпеки, результати оцінки якого наведеня у додатку Б.

Як зазначалося раніше, на ринку електронних комунікаційних послуг за обсягом доходів основним постачальником є "Київстар" тому доцільно

розпочати аналіз та оцінку безпеки функціонування з даного постачальника послуг електронних комунікацій. Компанія “Київстар” - найбільший постачальник електронних комунікацій в Україні, “Київстар”, працює на ринку починаючи з 2014 року. Станом на 2023 рік компанією обслуговується 24,3 млн споживачів мобільного зв’язку та понад 1,1 млн користувачів фіксованого Інтернету з використанням широкого спектру мобільних і фіксованих технологій, включаючи 4G, Big Data, Cloud solutions, сервісів кіберзахисту, цифрового телебачення та ін. Головним акціонером Київстар є глобальний цифровий постачальник ІКТ-послуг, акції якого котируються на фондових біржах NASDAQ (Нью-Йорк) та Euronext (Амстердам) [366]. Міжнародна група VEON надає конвергентне підключення та цифрові послуги близько 160 млн клієнтів в шести країнах (на території яких проживає 7% населення світу) [302; 303]. Динаміка основних фінансово-економічних показників постачальника електронних комунікацій “Київстар” представлена у табл. 4.9.

Таблиця 4.9

Динаміка основних фінансово-економічних показників постачальника електронних комунікацій “Київстар” тис. грн

Показники	Роки				
	2019	2020	2021	2022	2023
Активи (р.1300)	24 393 604	27 013 368	29 812 247	40 375 619	50 396 195
Гроші та їх еквіваленти (р. 1165)	898 072	1 219 310	1 707 773	4 684 591	7 372 688
Довгострокові зобов’язання (р.1595 р.II ПБ)	2 510 553	7 011 906	10 955 311	8 022 375	8 347 261
Короткострокові зобов’язання (р. 1600)	–	140 416	59 781	777 428	89 990
Чистий прибуток (р. 2350)	6 802 455	11 266 926	10 369 859	9 516 514	11 266 926

(складено за даними [307; 308; 309])

При розрахунку обсягу доходів постачальників електронних комунікацій враховуються отримання коштів: за ефірний час, за фіксовані лінії, роумінгу та доступу до мережі, за з’єднання, регулярних платежів, підключення до мережі та

разової плати за підписку на послуги, надання послуг ШСД Інтернету (FTTB), додаткові послуги; обладнання клієнтам: телефонних апаратів, модемів та ін.

Слід відмітити позитивну динаміку зростання активів компанії впродовж аналізованого періоду та збільшення чистого прибутку на 1 750, 412 млн грн у 2023 році у порівнянні із 2022 роком, початком повномасштабного вторгнення на територію України. Крім того, не зважаючи на серйозну кібератаку на "Київстар", яку було здійснено 12 грудня 2023 року, а також часткове руйнування інфраструкутури постачальника електронних комунікаційних послуг, компанії вдалося відновитися і навіть отримати приріс прибутку, виручка склала 0,7 млрд грн, а EBITDA – 0,8 млрд грн.

"Київстар" відновив свою мережу та послуги в кілька етапів протягом декількох днів після кібератаки, компанія вжила заходів щодо утримання клієнтів, запропонувавши спеціальної програми лояльності. Минулого року "Київстар" з метою розубудови стратегії "4G усюди" технологічно модернізував близько 4000 базових станцій 4G та встановив майже 1000 нових 4 G-сайтів [310].

З метою визначення безпеки за попередньо визначених складових для дослідження обрано індикатори, які кількісно визначатимуть вплив на безпеку функціонуючих підприємств за врахування їх відхилення від нормативних значень, тим самим вказуючи на точки біфуркації (перебування підприємства в зоні загрози) та точки репелерної (перебування у зоні ризиків) для виміру безпеки функціонууючого підприємства. Результати розрахунків за досліджуваними підприємствами надані в додатках.

Стейкхолдерами визначено пріоритетні складові, згруповано за впливом на цільови результати безпеки, що полегшить орацювання та врахує їх інтреси для забезпечення управління у єдиному напрямку: упередження ризиків, усунення загроз, забезпечення цільових результатів безпеки. Результати представлені в таблицях 4.11, 4.12, 4.13. З урахуванням інфляційних процесів, що відбуваться в країні через воєнні дії, доцільним окремо дослідити валютні ризики, оскільки валютні коливання чинять суттєвий вплив на доходи ти

прибутки підприємств-постачальників електронних комункацій, що пояснюється закупівлею устаткування у країн-партненрів національній валюті країни-постачальника, а також роумінгових послуг, що надаються країнами партнерами. Відбувається перерахування прибутків з коригуванням на валютні курсові різниці, тому даний ризик переходить у категорію загроз та потребує врахування при оцінці цільових результатів діяльності (табл 4. 10, табл 4.12, таблиця 4.13)

Таблиця 4.10

Фінансово-економічні показники ПрАТ "Київстар", тис. грн

за 2018-2022 рр.

Показники	Код рядка	Рік				
		2018	2019	2020	2021	2022
Середньорічна вартість основних засобів	р.1010	8 137 155	12 094 876	13 859 465	16 291 426	19 257 808
Активи	Р.1300	24 880 326	24 463 716	27 003 859	29 812 247	40 375 619
Власний капітал	Р. 1495	16 735 315	13 686 590	11 408 277	12 465 162	21 984 642
Чистий дохід від реалізації	Р. 2000	19 077 607	22 274 923	25 041 947	28 559 150	30 900 973
Собівартість реалізації продукції	Р.2050	7 701 134	7 753 253	8 506 957	9 810 231	13 073 367
Валовий прибуток(збиток)	Р.2090	11 376 473	14 521 670	16 534 990	18 748 919	17 827 606
Операційний прибуток	Р.2190	8 009 520	10 667 923	13 010 193	14 620 299	12 567 270
Чистий прибуток (збиток)	Р.2350 (2355)	6 837 961	8 938 154	10 322 053	11 266 926	9 516 514
EBITDA:						
прибуток до оподаткування	Р.2290	8 337 567	10 612 258	12 568 235	13 937 797	11 715 425
фінансові витрати	Р.2250	7 185	344 745	429 826	967 025	1 226 928
витрати на амортизацію	Р.2515	2 285 053	3 160 134	3 979 062	4 409 702	4 820 181
Витрати на оплату праці (вартість людського капіталу)	р.2505	1 167 816	1 419 434	1 709 248	2 020 724	2 807 406
Загальна сума інвестованого капіталу	р.3260	7 252 540	3 785 393	4 949 697	5 102 313	6 101 685

(розраховано автором за [336])

За даними таблиці 4.11, розраховуємо метрики цільових результатів безпеки ПрАТ "Київстар".

Таблиця 4.11

Метрики визначення досягнення цільових результатів безпеки підприємства-постачальника електронних комунікаційних послуг ПрАТ “Київстар”

Зацікавлені сторони	Показники (метрики)	Цільові результати безпеки підприємства	Роки						Ризики / загрози
			2018	2019	2020	2021	2022	Норма	
Кредитори Контрагенти Власники Керівники Регулятор	K_R послуг Чистий прибуток/ Чистий дохід від реалізації	Прибутковість Платоспроможність Розвиток	0,36	0,4	0,41	0,39	0,31	>0,05	Ймовірність/Втрата здатності генерувати грошовий потік та втрати фінансової потужності
Інвестори, кредитори Власники Керівники, Регулятор, Споживачі	$K_{R\ прод,\ роб,\ посл}$ Валовий прибуток(збиток)/ Собівартість реалізації послуг	Прибутковість Конкурентоспроможність	1,48	1,88	1,95	1,91	1,36	> 0,3 (збільшення в динаміці)	Ймовірність зменшення/ зменшення прибутку, зростання цін, ризик зростання тарифів на послуги, ризик втрати користувачів послуг
Власники Інвестори Акціонери Регулятор	$K_{Rвк}$ Чистий прибуток(збиток)/ Власний капітал	Прибутковість Платоспроможність Розвиток Стійкість, Конкурентоспроможність	0,45	0,15	0,21	0,65	0,55	> 0,2 (збільшення в динаміці)	Ймовірність/ втрата генерації прибутку за рахунок власного капіталу, ймовірність/ зростання боргового навантаження
Менеджер, кредитори, інвестори, конкуренти	$K_{R\ кап}$ Чистий прибуток(збиток)/ Баланс активів	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,28	0,09	0,1	0,32	0,27	> 0,1	Ймовіріність/ втрата генерації прибутку за рахунок активів підприємства
Інвестори, власники, Регулятор	$K_{R\ EBITDA}$ EBITDA/ Чистий дохід від реалізації	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,603	0,634	0,678	0,676	0,575	> 0, 46 (середнє за конкурентами галузі)	Ймовірність втрати /втрата спроможності до самофінансування, визначення ефективності майбутніх інвестув. Ймовірність зниження/ зниження операційної ефективності компанії
Конкуренти, власники, Регулятор, споживачі	$K_{R\ валовий}$ Валовий прибуток/ Чистий дохід від реалізації	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,96	0,97	0,66	0,97	0,58	> 0,5 або ж (середнє за конкурентами в галузі)	Ймовірність/ зниження ефективності компанії в продукуванні нових товарів, послуг по відношенню до конкурентів
Інвестори, кредитори, керівники	$K_{R\ операційний}$ Операційний прибуток/ Чиста виручка	Прибутковість Платоспроможність Розвиток	0,42	0,48	0,52	0,51	0,41	0, 218 (середнє за конкурентами в галузі	Ймовірність/ нестійкість бізнесу через коливання, (чим більші коливання, тим більший ризик, нестійкість бізнесу)
Інвестори, власники, регулятор	$K_{R\ ROIC\ (інвестованого\ капіталу)}$ Чистий прибуток/ загальна сума інвестованого капіталу	Розвиток Прибутковість	0,94	2,36	2,09	2,21	1,56	> 0,14	Ймовірність/ втратf ефективності інвестицій, ймовірінсть/ гальмування розвитку
Власники, кредитори, керівники, регулятор	$K_{фондовіддачі\ ОЗ}$ Чистий дохід від реалізації/Середньорічна вартість основних засобів	Розвиток Прибутковість	2,34	1,84	1,8	1,75	1,6	> 1,513 (середнє за конкурентами в галузі)	Ймовірність/ зниження забезпеченістю основними засобами, ймовірність/ зниження використання основних засобів
Персонал, власники	$K_{ефект-ті\ інтелектуального\ капіталу}$ Валовий прибуток/Вартість людського капіталу	Прибутковість Розвиток Конкурентоспроможність	9,74	10,23	9,67	9,28	6,35	> 4,37 (середнє за конкурентами в галузі)	Ймовірінсть/ зниження продуктивності та мотивації персоналу

(розраховано автором)

За результатами розрахунків, отримуємо, що компанія “Київстар” працює стабільно. Не відзначаються відхилення метрик від нормативних критеріальних для визначення точок біфуркації та репелеру.

Відзначаються високі ризикі від валютних коливань для компанії (табл.4. 12). Чутливість до ймовірної зміни обмінних курсів (що частка фінансових інструментів в іноземній валюті є постійною величиною на 31 грудня 2022 року і 31 грудня 2021 року)

Таблиця 4.12

Чутливість до ймовірної зміни обмінних курсів

Зміна курсу валют	2018		2019		2020		2021		2022	
	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув
Зміна обмінного курсу долара США	+10,00%	(37880)	+10,00%	(34655)	+10,00%	(47356)	+10,00%	(48 111)	+10,00 %	(30 771)
Зміна обмінного курсу євро	+10,00%	18 541	+10,00%	17 522	+10,00%	22967	+10,00%	23 115	+10,00 %	3 873
Зміна обмінного курсу долара США	-1,00%	3920	-1,00%	3567	-1,00%	4370	-1,00%	4 811	-1,00%	3 077
Зміна обмінного курсу євро	-1,00%	(1735)	-1,00%	(1965)	-1,00%	(2156)	-1,00%	(2 311)	-1,00%	(387)

(складено автором за [336])

Компанія “ВФ Україна” на сьогодні посідає друге місце за обсягом доходів у галузі зв’язку, як бренд з’явилася у 2015 році, активно розвивається, постійно пропонує цифрові рішення, намагаючись удосконалюватися задля утримання клієнтів, оскільки поступається за рівнем покриття мережею компанії Київстар. Компанія Vodafone приналежна азербайджанському холдингу NEQSOL, за розміром відноситься до великих має, у власності якої знаходиться компанія Smartflex із кількістю IT-персоналу – 387 осіб. Динаміка основних фінансово-економічних показників постачальника електронних комунікацій ПрАТ “ВФ Україна” за 2018-2023 рр. наведена в табл 4.13.

Таблиця 4.13

Динаміка основних фінансово-економічних показників постачальника електронних комунікацій ПрАТ “ВФ Україна” за 2018-2023 рр., тис. грн

Показник	2018	2019	2020	2021	2022	2023
Активи	24727291	24061896	37376208	35 959 561	40 094 776	32 412 556
Гроші та їх еквіваленти	2570228	1285927	2630440	2 539 723	4 775 787	3 401 872
Довгострокові зобов’язання	5669202	3691463	16975478	15 354 881	17 704 912	18 061 961
Короткострокові зобов’язання	7057501	6269928	4985682	–	–	–
Чистий прибуток	1897589	2099917	1314543	3 936 033	1 065 383	4 730 079

(складено за даними [334; 335])

Компанія ПрАТ “ВФ Україна” намагається розширити мережу надання фіксованого інтернету, збільшити свою частку на ринку, при чому не розбудовуючи нових мереж, а шляхом придбання у 2021 році “Vega”, а у 2023 році – “Фрінет”. Купівля компаній пояснюється стратегією розвитку конвергенції послуг, окрім того, на базі “Vega” розширюється покриття технологією GPON, минулоріч додатково введено у користування 1072 зони доступу до енергоефективного інтернету.

Не зважаючи, на суттєву частку на ринку, географію надання послуг, проаналізувавши ступінь відповідності захисту інформації міжнародним стандартам та сертифікаціям, відзначається комплаєнс-ризик, індекс захисту “C+”, що вказує на вірогідність порушення цілісності, достовірності інформації, прослідковується вразливість до кібератак. Результат тесту представлено на рис. 4.17.

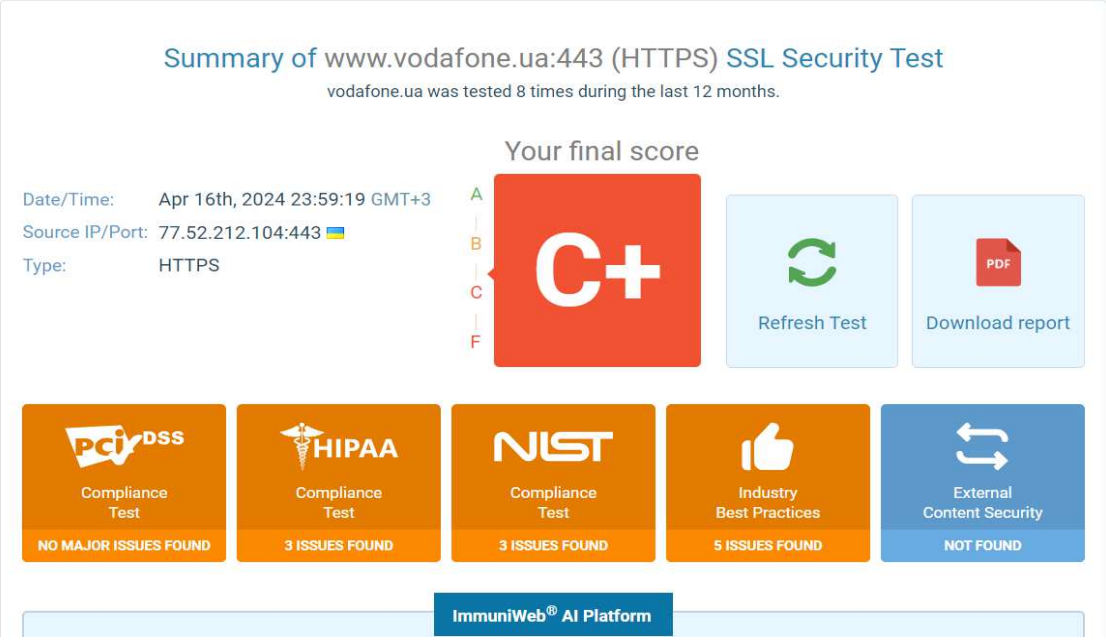


Рис. 4.17. Комплаєнс ризики (загрози) ПрАТ "ВФ Україна"

(сформовано за даними NIST)

У таблиці 4.14 представлені фінансово-економічні показники для розрахунку метрик безпеки (таблиця 4.15)

Таблиця 4.14

Фінансово-економічні показники ПрАТ "ВФ Україна", тис. грн

за 2018-2022 рр.

Показник	Код рядка	Рік				
		2018	2019	2020	2021	2022
Середньорічна вартість основних засобів	P. 1010	11664234	12302033	12356407	12418791	11726625
Активи	P.1300	25028061	24990035	37789650	36503968	40094776
Власний капітал	P. 1495	11845705	14385017	15586007	15912208	16909464
Чистий дохід від реалізації	P. 2000	12799024	15983419	18142407	20144755	18802655
Собівартість реалізації продукції	P.2050	7063774	8332113	9025372	9178029	7474429
Валовий прибуток(збиток)	P.2090	5735250	7651306	9025372	10966726	11328226
Операційний прибуток	P.2190	2775492	3621451	5027124	5920486	6569027
Чистий прибуток (збиток)	P.2350 (2355)	1747213	2539312	1201322	3831547	1065383
EBITDA:						
прибуток до оподаткування	P.2290	2206884	3228841	1596100	4787135	1363426
фінансові витрати	P.2250	744736	650282	1491450	1691167	1448569
витрати на амортизацію	P.2515	4087723	4703907	4800618	4989380	4040034
Витрати на оплату праці (вартість людського капіталу)	p.2505	886494	1335516	1394388	1868142	1751958
Загальна сума інвестованого капіталу	p.3260	6640385	3788312	4051469	3794922	3518237

(складено автором за даними [334;335])

Таблиця 4.15

Метрики визначення досягнення цільових результатів безпеки підприємства-постачальника електронних комунікаційних послуг ПрАТ “ВФ Україна”

Зацікавлені сторони	Показники (метрики)	Цільові результати безпеки підприємства	Роки						Ризики / загрози
			2018	2019	2020	2021	2022	Норма значення	
Кредитори Контрагенти Власники Керівники Регулятор	$K_{R\ послуг}$ Чистий прибуток/ Чистий дохід від реалізації	Прибутковість Платоспроможність Розвиток	0,16	0,14	0,066	0,190	0,056	>0,05	Ймовірність/Втрата здатності генерувати грошовий потік та втрати фінансової потужності
Інвестори, кредитори Власники Керівники, Регулятор, Споживачі	$K_{R\ прод,роб,посл}$ Валовий прибуток(збиток)/ Собівартість реалізації послуг	Прибутковість Конкурентоспроможність	0,81	0,92	0,989	1,19	1,371	> 0,3 (збільшення в динаміці)	Ймовірність зменшення/ зменшення прибутку, зростання цін, ризик зростання тарифів на послуги, ризик втрати користувачів послуг
Власники Інвестори Акціонери Регулятор	$K_{Rвк}$ Чистий прибуток(збиток)/ Власний капітал	Прибутковість Платоспроможність Розвиток Стійкість, Конкурентоспроможність	0,13	0,19	0,076	0,24	0,067	> 0,2 (збільшення в динаміці)	Ймовірність/ втрата генерації прибутку за рахунок власного капіталу, ймовірність/ зростання боргового навантаження
Менеджер,и кредитори, інвестори, конкуренти	$K_{R\ кап}$ Чистий прибуток(збиток)/ Баланс активів	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,07	0,1	0,03	0,103	0,014	> 0,1	Ймовірініть/ втрата генерації прибутку за рахунок активів підприємства
Інвестори, власники, Регулятор	$K_{R\ EBITDA}$ EBITDA/ Чистий дохід від реалізації	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,55	0,54	0,43	0,57	0,36	> 0, 46 (ереднє за конкурентами галузі)	Ймовірність втрати /втрата спроможності до самофінансування, визначення ефективності майбутніх інвестув. Ймовірність зниження/ зниження операційної ефективності компанії
Конкуренти, власники, Регулятор, споживачі	$K_{R\ валовий}$ Валовий прибуток/ Чистий дохід від реалізації	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,45	0,48	0,5	0,54	0,6	> 0,5 або ж (середнє за конкурентами в галузі)	Ймовірність/ зниження ефективності компанії в продукуванні нових товарів, послуг по відношенню до конкурентів
Інвестори, кредитори, керівники	$K_{R\ операційний}$ Операційний прибуток/ Чиста виручка	Прибутковість Платоспроможність Розвиток	0,22	0,23	0,28	0,29	0,35	0, 218 (середнє за конкурентами в галузі	Ймовірність/ нестійкість бізнесу через коливання, (чим більші коливання, тим більший ризик, нестійкість бізнесу)
Інвестори, власники, регулятор	$K_{R\ ROIC\ (інвестованого капіталу)}$ Чистий прибуток/ загальна сума інвестованого капіталу	Розвиток Прибутковість	0,26	0,67	0,3	1	0,3	> 0,14	Ймовірність/ втратf ефективності інвестицій, ймовірінсть/ гальмування розвитку
Власники, кредитори, керівники, регулятор	$K_{фондовіддачі\ ОЗ}$ Чистий дохід від реалізації/Середнь орічна вартість основних засобів	Розвиток Прибутковість	1,1	1,3	1,47	1,62	1,6	> 1,513 (середнє за конкурентами в галузі)	Ймовірність/ зниження забезпеченість основними засобами, ймовірність/ зниження використання основних засобів
Персонал, власники	$K_{ефект-ті\ інтелектуального капіталу}$ Валовий прибуток/Вартість людського капіталу	Прибутковість Розвиток Конкурентоспроможність	6,47	5,73	6,47	5,87	6,47	> 4,37 (середнє за конкурентами в галузі)	Ймовірність/ зниження продуктивності та мотивації персоналу

(розраховано автором)

В результаті розрахунків отримуємо, що ПрАТ “ВФ Україна” знаходиться на межі втрати здатності генерувати грошовий потік та втрати фінансової потужності, перебуваючи в зоні ризику. Загрози втрати генерації прибутку (за рахунок власного капіталу, а також активів) та зростання боргового навантаження відзначаються також відзнчаються у ПрАТ “ВФ Україна”.

Чутливість до ймовірної зміни обмінних курсів (що частка фінансових інструментів в іноземній валюті є постійною величиною на 31 грудня 2022 року і 31 грудня 2021 року) становить (таблиця 4.16)

Таблиця 4.16

Чутливість до ймовірної зміни обмінних курсів ПрАТ “ВФ Україна”

Зміна курсу валют	2018		2019		2020		2021		2022	
	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув
Зміна обмінного курсу долара США	+10,00%	(32780)	+10,00%	(35788)	+10,00%	(44350)	+10,00%	(41778)	+10,00%	(31245)
Зміна обмінного курсу євро	+10,00%	203517	+10,00%	134656	+10,00%	12230	+10,00%	21 121	+10,00%	3 112
Зміна обмінного курсу долара США	-1,00%	3762	-1,00%	3245	-1,00%	3540	-1,00%	3123	-1,00%	2789
Зміна обмінного курсу євро	-1,00%	(567)	-1,00%	(1223)	-1,00%	(1789)	-1,00%	(2 127)	-1,00%	(1277)

(складено автором за [335])

Компанія “Лайфселл”– мобільний оператор, розробник власних цифрових рішень, налічує близько 250 співробітників компанії. Належить турецькому телекомунікаційному холдингу Turkcell, постачальнику конвергентних послуг електронних комунікацій і технологічних послуг, акції якого котируються на Нью-Йоркській фондовій біржі (NYSE) та турецькій фондовій біржі Borsa Istanbul (BIST) [371]. ПрАТLifecell став першим мобільним оператором, який

разом із партнером IoT Ukraine розгорнув в Україні мережу інтернету речей стандарту LoRaWAN і почав тестувати технологію NB-IoT.

З 2019 року постачальник послуш ЕК реалізовує проєкти з “розумного обліку” ресурсів, “розумного освітлення”, моніторингу довкілля, покращення безпеки громадян і впроваджує інші IoT-рішення. Компанія підписала з міськими та обласними адміністраціями низку меморандумів і декларативних угод про співпрацю, які передбачають сприяння цифровізації українських міст і областей, а також упровадження рішень Smart City. Попри те, що компанія анонсує реалізовує проєкти з “розумного обліку” ресурсів, “розумного освітлення”, моніторингу довкілля, покращення безпеки громадян і впроваджує інші IoT-рішення, Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв’язку, (НКЕК) оштрафувала постачальника мобільного зв’язку “Лайфселл” на 10,5 млн грн. Динаміка основних фінансово-економічних показників постачальника електронних комунікацій ТОВ “Лайфселл” за 2018-2023 рр., тис. грн

Таблиця 4.17

Динаміка основних фінансово-економічних показників постачальника електронних комунікацій ТОВ “Лайфселл” за 2018-2023 рр., тис. грн

Показник	2018	2019	2020	2021	2022	2023
Активи	14 348 815	13 469 931	16 661 919	17 469 994	18 930 989	21 719 269
Гроші та їх еквіваленти	375 415	456 496	113 464	1 355 551	1 745 813	5 140 878
Довгострокові зобов’язання	2381137	2 159 287	3 514 718	4 321 576	3 024 513	2 321 082
Короткострокові зобов’язання	7329603	6 915 074	5 484 647	4 882 266	6,654,067	3 540 482
Чистий прибуток	609515	1 138 244	2 586 680	603 598	961,215	2 567 707

(складено автором за [340; 341;403; 404])

ТОВ “Лайфселл” використовує стандарти NIST і вважається стійкою до комплаєнс-ризиків, спроможна чинити опір кібератакам, що впливає позитивно на репутацію компанії, оцінка “A+”, рис. 4.18.

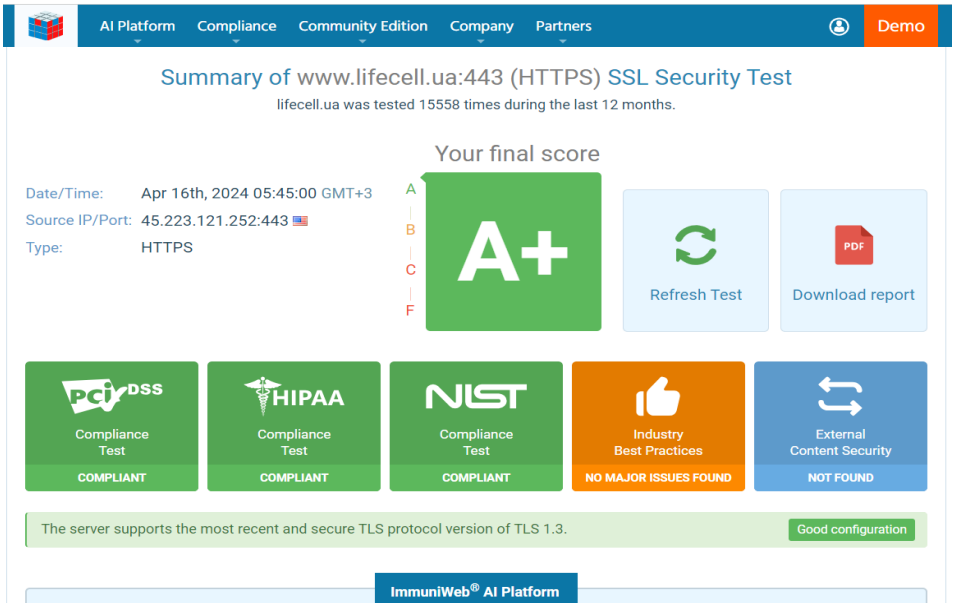


Рис. 4.18. Комплаєнс ризики (загрози) ТОВ “Лайфселл”

(складено за даними NIST)

Фінансово-економічні показники ПрАТ “Лайфселл”, представлено в табл. 4.18, які є вихідними даними, що використовуються для розрахунку метрик безпеки (табл. 4.19)

Таблиця 4.18

Фінансово-економічні показники ТОВ “Лайфселл”, тис. грн за 2018-2022 рр.

Показники	Код рядка	Рік				
		2018	2019	2020	2021	2022
Середньорічна вартість основних засобів	р.1010	5 307 856	5 092 513	5 088 756	6 464 461	6 373 403
Активи	Р.1300	14 352 265	13 476 855	16 669 389	17 485 162	18 930 989
Власний капітал	Р. 1495	4 642 230	4 403 818	7 672 784	8 283 639	9 255 908
Чистий дохід від реалізації	Р. 2000	5 268 521	5 983 804	6 835 816	8 482 687	9 411 748
Собівартість реалізації продукції	Р.2050	(4 326 296)	(4 648 675)	(5 076 862)	(5 749 336)	(6 287 636)
Валовий прибуток(збиток)	Р.2090/	942 225	1 335 129	1 758 954	2 733 351	3 124 112
Операційний прибуток	Р.2190	80 982	379 928	770 198	1 594 991	1 892 074
Чистий прибуток (збиток)	Р.2350 (2355)	(-608 416)	(-1 134 151)	2 588 662	610 855	972 269
EBITDA:						
прибуток до оподаткування	Р.2290	(-608 416)	(-1 134 151)	6 958	752 052	1 188 104
фінансові витрати	Р.2250	(1 192 993)	(1 498 742	(852 602)	(875 640)	(926 119)
витрати на амортизацію	Р.2515	2667842	2862980	2 860 691	3 156 246	3 554 437
Витрати на оплату праці (вартість людського капіталу)	р.2505	364060	421419	481 799	500 052	573 858
Загальна сума інвестованого капіталу	р.3260	4000227	1707393	(2 602 153)	(2 535 515)	(2 520 836)

(складено автором за [339; 340; 340; 341; 405; 406; 407])

Таблиця 4.19

Метрики визначення досягнення цільових результатів безпеки підприємства-постачальника електронних комунікаційних послуг ТОВ “Лайфселл”

Зацікавлені сторони	Показники (метрики)	Цільові результати безпеки підприємства	Роки					Нормативне значення	Ризики / загрози
			2018	2019	2020	2021	2022		
Кредитори Контрагенти Власники Керівники Регулятор	$K_{R\ послуг}$ Чистий прибуток/ Чистий дохід від реалізації	Прибутковість Платоспроможність Розвиток	-0,115	-0,199	0,379	0,072	0,103	>0,05	Ймовірність/Втрата здатності генерувати грошовий потік та втрати фінансової потужності
Інвестори, кредитори Власники Керівники, Регулятор, Споживачі	$K_{R\ прод.роб,\ посл}$ Валовий прибуток(збиток)/ Собівартість реалізації послуг	Прибутковість Конкурентоспроможність	0,218	0,287	0,347	0,475	0,497	> 0,3 (збільшення в динаміці)	Ймовірність зменшення/ зменшення прибутку, зростання цін, ризик зростання тарифів на послуги, ризик втрати користувачів послуг
Власники Інвестори Акціонери Регулятор	$K_{Rвк}$ Чистий прибуток(збиток)/ Власний капітал	Прибутковість Платоспроможність Розвиток Стійкість, Конкурентоспроможність	-0,135	-0,251	0,162	0,038	0,111	> 0,2 (збільшення в динаміці)	Ймовірність/ втрата генерації прибутку за рахунок власного капіталу, ймовірність/ зростання боргового навантаження
Менеджер, кредитори, інвестори, конкуренти	$K_{R\ кап}$ Чистий прибуток(збиток)/ Баланс активів	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	-0,044	-0,082	0,152	0,036	0,053	> 0,1	Ризик втрати генерації прибутку за рахунок активів підприємства
Інвестори, власники, Регулятор	$K_{R\ EBITDA}$ EBITDA/ Чистий дохід від реалізації	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,62	0,54	0,54	0,56	0,6	> 0, 46 (ереднє за конкурентами галузі)	Ймовірність втрати /втрата спроможності до самофінансування, визначення ефективності майбутніх інвестув.
Конкуренти, власники, Регулятор, споживачі	$K_{R\ валовий}$ Валовий прибуток)/ Чистий дохід від реалізації	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,18	0,22	0,26	0,32	0,33	> 0,5 або ж (середнє за конкурентами в галузі)	Ймовірність зниження/ зниження операційної ефективності компанії
Інвестори, кредитори, керівники	$K_{R\ операційний}$ Операційний прибуток/ Чиста виручка	Прибутковість Платоспроможність Розвиток	0,015	0,063	0,11	0,19	0,2	0, 218 (середнє за конкурентами в галузі	Ймовірність/ зниження ефективності компанії в продукуванні нових товарів, послуг по відношенню до конкурентів
Інвестори, власники, регулятор	$K_{R\ ROIC\ (інвестованого\ капіталу)}$ Чистий прибуток/ загальна сума інвестованого капіталу	Розвиток Прибутковість	-0,15	-0,66	0,99	0,24	0,39	> 0,14	Ймовірність/ втратf ефективності інвестицій, ймовірність/ гальмування розвитку
Власники, кредитори, керівники, регулятор	$K_{фондовіддачі\ ОЗ}$ Чистий дохід від реалізації/Середньорічна вартість основних засобів	Розвиток Прибутковість	0,99	1,18	1,34	1,31	1,48	> 1,513 (середнє за конкурентами в галузі)	Ймовірність/ зниження забезпеченістю основними засобами, ймовірність/ зниження використання основних засобів
Персонал, власники	$K_{ефект-ті\ інтелектуального\ капіталу}$ Валовий прибуток/Вартість людського капіталу	Прибутковість Розвиток Конкурентоспроможність	2,59	3,17	3,65	5,47	5,44	> 4,37 (середнє за конкурентами в галузі)	Ймовірнсть/ зниження продуктивності та мотивації персоналу

(розраховано автором)

У компанії “Лайфселл” відначаються загрози втрати генерації прибутку (за рахунок власного капіталу, а також активів) та зростання боргового

навантаження, загрози втрати конкурентоспроможності через зниження ефективності компанії в продукуванні нових товарів, послуг по відношенню до конкурентів, ризик нестійкості бізнесу.

Чутливість до ймовірної зміни обмінних курсів (що частка фінансових інструментів в іноземній валюті є постійною величиною на 31 грудня 2022 року і 31 грудня 2021 року), наведена у таблиці 4.20.

Таблиця 4.20

Чутливість до ймовірної зміни обмінних курсів “Лайфселл”

Зміна курсу валют	2018		2019		2020		2021		2022	
	Збільш/ (змен) у %	Збільш / (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув
Зміна обмінного курсу долара США	+10,00%	(5740)	+10,00%	(5478)	+10,00%	(4560)	+10,00%	(5145)	+10,00%	(5678)
Зміна обмінного курсу євро	+10,00%	(450)	+10,00%	(512)	+10,00%	451	+10,00%	7212	+10,00%	75644
Зміна обмінного курсу долара США	-1,00%	(481)	-1,00%	(561)	-1,00%	654	-1,00%	877	-1,00%	930
Зміна обмінного курсу євро	-1,00%	(177)	-1,00%	(187)	-1,00%	(930)	-1,00%	(1279)	-1,00%	(101)

(складено за данимии [339])

Наступним великим постачальником послуг зв’язку, найбільшим надавачем фіксованого зв’язку на ринку України є АТ “Укртелком”, база користувачів нараховує 1,0 млн осіб та 0,6 млн інтернет-користувачів. Компанія активно модернізує мережі, дотримується стандартів та вимог у сфері охорони праці, зафіксовано 49 декларацій, що засвідчують відповідність нормативно-правовим актам безпеки. Основні фінансово-економічні показники наведено у таблиці 4.21.

Таблиця 4.21

Динаміка основних фінансово-економічних показників постачальника електронних комунікацій АТ "Укртелеком" за 2018-2023 рр., тис. грн

Показники	2018	2019	2020	2021	2022	2023
Активи	11694334	11172424	14628828	16 194 671	12 930 434	12 797 454
Гроші та їх еквіваленти	340793	393184	739565	313861	796 675	482 370
Довгострокові зобов'язання	1724839	1712155	3180370	2 532604	2 162 996 000	1 837 444 000
Короткострокові зобов'язання	2968628	2143670	14778071	1748258	12 249	13 273 000 13 273
Чистий прибуток	127585	-	2091680	451987	-	58 128 000
Збиток	-	- 835989	-	-	-2 422 198 000	-

(складено автором за [337; 338])

Важливо, що компанія активно розбудовує мережу FTTH/P за технологією GPON, що сприяє пришвидшенню поширенню енергонезалежного інтернету та підвищує якість та стабільність надання послуги.

Впродовж минулого року прокладено близько 5,3 тисячі кілометрів волоконно-оптичного кабелю, що дозволило 2 млн домогосподарств користуватися послугами мережі, загальна кількість нових підключень збільшилася більш, ніж на 15%, а сукупний дохід від надання послуг на базі оптичної мережі зріс на 18% по відношенню до 2022 року.

Руйнівні наслідки російської агресії для Укртелекому сягають 2,8 млрд грн, що переважно зумовлено економічним знеціненням операційних активів. Внаслідок бойових дій було пошкоджено близько 260 будівель компанії, а близько 50 — повністю зруйновано. На відновлення інфраструктури було витрачено 20 млн грн, що дозволило відновити майже 430 км оптичних ліній та 16 км мідних ліній зв'язку, функціонування 10 регіональних вузлів зв'язку.

Фінансово-економічні показники ПрАТ "Укртелеком" представлені у табл. 4.22 та слугують вихідними даними для розрахунку метрик безпеки (табл. 4.23)

Таблиця 4.22

Фінансово-економічні показники ПрАТ “Укртелеком”, тис. грн за 2018-2022 рр.

Показники	Код рядка	Рік				
		2018	2019	2020	2021	2022
Середньорічна вартість основних засобів	р.1010	8551670	5216103	10495100	11196366	7537403
Активи	Р.1300	11314951	11003092	14630236	16033786	12930434
Власний капітал	Р. 1495	6634856	7007238	10135494	11824551	8831810
Чистий дохід від реалізації	Р. 2000	5936564	5771328	5449056	4394064	5279923
Собівартість реалізації продукції	Р.2050	3840909	3883627	3668503	4197256	3827299
Валовий прибуток(збиток)	Р.2090/	2095655	1887701	1791845	1082667	566765
Операційний прибуток	Р.2190	896520	746702	1080961	718990	-1994174
Чистий прибуток (збиток)	Р.2350 (2355)	127585	-835989	2031675	451987	-2422198
EBITDA:						
прибуток до оподаткування	Р.2290	576175	-533097	2428201	512226	-2852167
фінансові витрати	Р.2250	353580	345263	589983	534075	611141
витрати на амортизацію	Р.2515	712208	759569	668673	1161984	1238712
Витрати на оплату праці (вартість людського капіталу)	р.2505	1933129	1949496	1947996	1939203	1546714
Загальна сума інвестованого капіталу	р.3260	671935	735121	660852	998423	556777

(складено автором за [337; 338]

Таблиця 4.23

Метрики визначення досягнення цільових результатів безпеки підприємства-постачальника електронних комунікаційних послуг ПАТ “Укртелеком”

Зацікавлені сторони	Показники (метрики)	Цільові результати безпеки підприємства	Роки					Нормативне значення	Ризики / загрози
			2018	2019	2020	2021	2022		
Кредитори Контрагенти Власники Керівники Регулятор	$K_{R\ послуг}$ Чистий прибуток/ Чистий дохід від реалізації	Прибутковість Платоспроможність Розвиток	0, 02	-0,14	0,37	0,1	-0,45	>0,05	Ймовірність/Втрата здатності генерувати грошовий потік та втрати фінансової потужності
Інвестори, кредитори Власники Керівники, Регулятор, Споживачі	$K_{R\ прод,роб,посл}$ Валовий прибуток(збиток)/ Собівартість реалізації послуг	Прибутковість Конкурентоспроможність	0,54	0,48	0,49	0,26	0,15	> 0,3 (збільшення в динаміці)	Ймовірність зменшення/ зменшення прибутку, зростання цін, ризик зростання тарифів на послуги, ризик втрати користувачів послуг
Власники Інвестори Акціонери Регулятор	$K_{Rвк}$ Чистий прибуток(збиток)/ Власний капітал	Прибутковість Платоспроможність Розвиток Стійкість, Конкурентоспроможність	0,019	-0,12	0,2	0,038	-0.27	> 0,2 (збільшення в динаміці)	Ймовірність/ втрата генерації прибутку за рахунок власного капіталу, ймовірність/ зростання боргового навантаження
Менеджер, кредитори, інвестори, конкуренти	$K_{R\ кап}$ Чистий прибуток(збиток)/ Баланс активів	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	-0,011	-0,076	0,14	0,028	-0,19	> 0,1	Ймовіріність/ втрата генерації прибутку за рахунок активів підприємства

продовження таблиці 4.23

Інвестори, власники, Регулятор	$K_{REBITDA}$ EBITDA/ Чистий дохід від реалізації	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,603	0,634	0,678	0,676	0,575	> 0, 46 (середнє за конкурентами галузі)	Ймовірність втрати /втрата спроможності до самофінансування, визначення ефективності майбутніх інвестув. Ймовірність зниження/ зниження операційної ефективності компанії
Конкуренти, власники, Регулятор, споживачі	$K_{R\ валовий}$ Валовий прибуток/ Чистий дохід від реалізації	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,96	0,97	0,66	0,97	0,58	> 0,5 або ж (середнє за конкурентами в галузі)	Ймовірність/ зниження ефективності компанії в продукуванні нових товарів, послуг по відношенню до конкурентів
Інвестори, кредитори, керівники	$K_{R\ операційний}$ Операційний прибуток/ Чиста виручка	Прибутковість Платоспроможність Розвиток	0,42	0,48	0,52	0,51	0,41	>0, 218 (середнє за конкурентами в галузі	Ймовірінсть/ нестійкість бізнесу через коливання, (чим більші коливання, тим більший ризик, нестійкість бізнесу)
Інвестори, власники, регулятор	$K_{R\ ROIC\ (інвестованого\ капіталу)}$ Чистий прибуток/ загальна сума інвестованого капіталу	Розвиток Прибутковість	0,94	2,36	2,09	2,21	1,56	> 0,14	Ймовірність/ втратf ефективності інвестицій, ймовірінсть/ гальмування розвитку
Власники, кредитори, керівники, регулятор	$K_{фондовіддачі\ ОЗ}$ Чистий дохід від реалізації/Середньорічна вартість основних засобів	Розвиток Прибутковість	2,34	1,84	1,8	1,75	1,6	> 1,513 (середнє за конкурентами в галузі)	Ймовірність/ зниження забезпеченістю основними засобами, ймовірність/ зниження використання основних засобів
Персонал, власники	$K_{ефект-ті\ інтелектуального\ капіталу}$ Валовий прибуток/Вартість людського капіталу	Прибутковість Розвиток Конкурентоспроможність	9,74	10,23	9,67	9,28	6,35	> 4,37 (середнє за конкурентами в галузі)	Ймовірінсть/ зниження продуктивності та мотивації персоналу

(розраховано автором)

У результаті розрахунку метрик з'ясовано, що ПАТ "Укртелеком" знаходиться на межі втрати здатності генерувати грошовий потік та втрати фінансової потужності, перебуваєь в зоні загроз, подолавши критичну точку біфуркації, існує загрози втрати генерації прибутку (за рахунок власного капіталу, а також активів) та зростання боргового навантаження відзначаються, загроза втрати спроможності до самофінансування, інвестиційної привабливості, зниження операційної ефективності наявна у компанії "Укртелеком"; загрози втрати конкурентоспроможності через зниження ефективності компанії в продукуванні нових товарів, послуг по відношенню до конкурентів відзначаються у компанії "Укртелеком", загроза нестійкості бізнесу, загроза

втрати ефективності інвестицій та ризик гальмування розвитку в “Укртелеком”, загроза зниження продуктивності та мотивації персоналу.

Чутливість до ймовірної зміни обмінних курсів (що частка фінансових інструментів в іноземній валюті є постійною величиною на 31 грудня 2022 року і 31 грудня 2021 року) представлена в таблиці 4.24.

Таблиця 4.24

Чутливість до ймовірної зміни обмінних курсів АТ “Укртелеком”

Зміна курсу валют	2018		2019		2020		2021		2022	
	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув
Зміна обмінного курсу долара США	+10,00%	(122)	+10,00%	(177)	+10,00%	(350)	+10,00%	(481)	+10,00%	(1585)
Зміна обмінного курсу євро	+10,00%	27 52	+10,00%	3098	+10,00%	4120	+10,00%	4234	+10,00%	(2760)
Зміна обмінного курсу долара США	-1,00%	455	-1,00%	4562	-1,00%	4110	-1,00%	4 168	-1,00%	(2140)
Зміна обмінного курсу євро	-1,00%	(455)	-1,00%	(767)	-1,00%	(1095)	-1,00%	(5671)	-1,00%	(1112)

(складено автором за [337; 338]

Не зважаючи на довіру з боку держави, комплаєнс ризики (загрози) АТ “Укртелеком” є високими, рис. 4.19, підприємство не впроваджує стандарти безпеки.

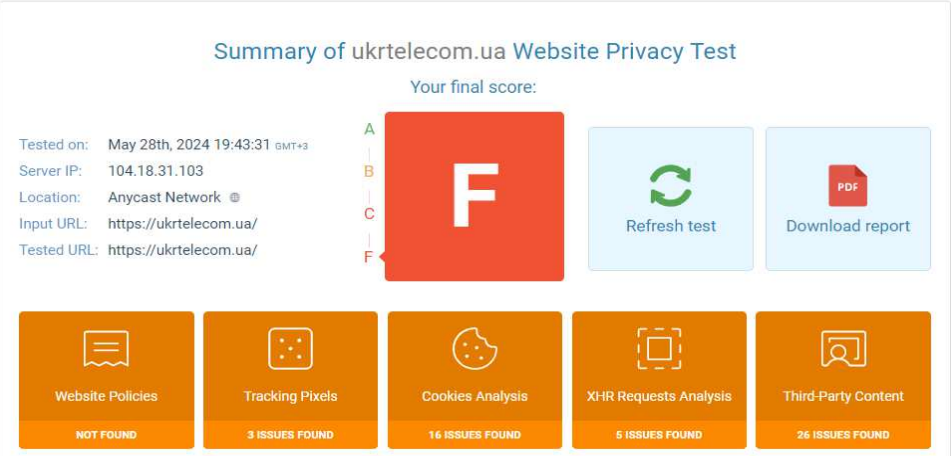


Рис. 4.19. Комплаєнс ризики (загрози) АТ “Укртелеком”

(складено з даними NIST)

АТ “Укртелеком” має високий комплаєнс ризик, не дотримується стандартів NIST і вважається нестійкою до комплаєнс ризиків, спроможна чинити опір кібератакам, що впливає негативно на репутацію компанії, має найнижчу за шкалою оцінку – “F”.

ПрАТ “Датагруп” – український постачальник послуг електронних комунікацій для суб’єктів підприємництва та домашнього користування. Надає спектр послуг: передачі даних і доступу в глобальної мережі, телефонії, відеоконференцій і відеоспостереження, супутникового зв’язку і хмарних сервісів [368]. Рішення компанії забезпечують надійний зв’язок для сегментів корпоративного, домашнього та постачальників електронних комункацій. Користуються довірою державного та обронного секторів, для яких розробляються та впроваджуються інновації. Забезпечує електронними комунікаційними послугами клієнтів у більш, ніж у 90 населених пунктах України.

Фінансово-економічні показники ПрАТ “Датагруп” (табл. 4.25), які використовуються для розрахунку метрик безпеки (табл. 4.26)

Таблиця 4.25

Фінансово-економічні показники ПрАТ “Датагруп”, тис. грн

за 2018-2022 рр.

Показники	Код рядка	Рік				
		2018	2019	2020	2021	2022
Середньорічна вартість основних засобів	р.1010	763753	791509	80893500	96530200	99580300
Активи	Р.1300	1456969	1461908	159014900	3 103 12300	3 727 76300
Власний капітал	Р. 1495	416133	555430	740 87600	707 70500	1 025 92800
Чистий дохід від реалізації	Р. 2000	1161813	1320850	1 285 31700	1 374 01500	1 204 75200
Собівартість реалізації продукції	Р.2050	761451	751709	650 64500	749 20700	757 25600
Валовий прибуток(збиток)	Р.2090/	400362	569141	634 67200	624 80800	447 49600
Операційний прибуток	Р.2190	31159	275249	342 24600	321 01600	184 38100
Чистий прибуток (збиток)	Р.2350 (2355)	20339	141764	187 51700	164 94100	-102 95100

продовження таблиці 4.25

EBITDA:						
прибуток до оподаткування	Р.2290	29541	175811	232 87900	204 58600	-147 29100
фінансові витрати	Р.2250	85227	114065	88 73400	120 40700	414 63700
витрати на амортизацію	Р.2515	137047	138495	157 38800	180 43100	194 69800
Витрати на оплату праці (вартість людського капіталу)	р.2505	253034	287640	329 61600	336 54200	323 15000
Загальна сума інвестованого капіталу	р.3260	204198	220435	229 07400	284 38300	440 95800

(складено автором за [401])

Таблиця 4.26

Метрики визначення досягнення цільових результатів безпеки підприємства-постачальника електронних комунікаційних послуг ПрАТ “Датагруп”

Зацікавлені сторони	Показники (метрики)	Цільові результати безпеки підприємства	Роки					Норматив. значення	Ризики / загрози
			2018	2019	2020	2021	2022		
Кредитори Контрагенти Власники Керівники Регулятор	$K_{R\ послуг}$ Чистий прибуток/ Чистий дохід від реалізації	Прибутковість Платоспроможність Розвиток	0,02	0,11	0,15	0,12	-0,09	>0,05	Ймовірність/Втрата здатності генерувати грошовий потік та втрати фінансової потужності
Інвестори, кредитори Власники Керівники, Регулятор, Споживачі	$K_{R\ прод,роб,посл}$ Валовий прибуток(збиток)/ Собівартість реалізації послуг	Прибутковість Конкурентоспроможність	0,53	0,76	0,49	0,83	0,59	> 0,3 (збільшення в динаміці)	Ймовірність зменшення/ зменшення прибутку, зростання цін, ризик зростання тарифів на послуги, ризик втрати користувачів послуг
Власники Інвестори Акціонери Регулятор	$K_{Rвк}$ Чистий прибуток(збиток)/ Власний капітал	Прибутковість Платоспроможність Розвиток Стійкість, Конкурентоспроможність	0,05	0,26	0,25	0,23	-0,1	> 0,2 (збільшення в динаміці)	Ймовірність/ втрата генерації прибутку за рахунок власного капіталу, ймовірність/ зростання боргового навантаження
Менеджер, кредитори, інвестори, конкуренти	$K_{R\ кап}$ Чистий прибуток(збиток)/ Баланс активів	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,01	0,1	0,12	0,05	-0,28	> 0, 46 (ереднє за конкурентами галузі)	Ймовіріність/ втрата генерації прибутку за рахунок активів підприємства
Інвестори, власники, Регулятор	$K_{R\ EBITDA}$ EBITDA/ Чистий дохід від реалізації	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,22	0,32	0,37	0,37	0,38	> 0,5 або ж (середнє за конкурентами в галузі)	Ймовірність втрати /втрата спроможності до самофінансування, визначення ефективності майбутніх інвестув. Ймовірність зниження/ зниження операційної ефективності компанії
Конкуренти, власники, Регулятор, споживачі	$K_{R\ валовий}$ Валовий прибуток/ Чистий дохід від реалізації	Прибутковість Конкурентоспроможність Платоспроможність Розвиток	0,34	0,43	0,49	0,45	0,37	0, 218 (середнє за конкурентами в галузі	Ймовірність/ зниження ефективності компанії в продукуванні нових товарів, послуг по відношенню до конкурентів
Інвестори, кредитори, керівники	$K_{R\ операційний}$ Операційний прибуток/ Чиста виручка	Прибутковість Платоспроможність Розвиток	0,03	0,21	0,27	0,23	0,15	> 0,14	Ймовірінсть/ нестійкість бізнесу через коливання, (чим більші коливання, тим більший ризик, нестійкість бізнесу)

продовження таблиці 4.26

Інвестори, власники, регулятор	K R ROIC (інвестованого капіталу) Чистий прибуток/ загальна сума інвестованого капіталу	Розвиток Прибутковість	0,1	0,64	0,82	0,58	-0,23	> 1,513 (середнє за конкурентами в галузі)	Ймовірність/ втрат ефективності інвестицій, ймовірність/ гальмування розвитку
Власники, кредитори, керівники, регулятор	$K_{фондовіддачі ОЗ}$ Чистий дохід від реалізації/Середньорічна вартість основних засобів	Розвиток Прибутковість	1,52	1,67	1,59	1,42	1,21	> 0, 46 (ереднє за конкурентами галузі)	Ймовірність/ зниження забезпеченість основними засобами, ймовірність/ зниження використання основних засобів
Персонал, власники	K ефект-ті інтелектуального капіталу Валовий прибуток/Вартість людського капіталу	Прибутковість Розвиток Конкурентоспроможність	1,58	1,98	1,93	1,86	1,38	> 4,37 (середнє за конкурентами в галузі)	Ймовірність/ зниження продуктивності та мотивації персоналу

(розраховано автором)

З'ясовано, що ПрАТ "Датагруп" знаходиться на межі втрати здатності генерувати грошовий потік та втрати фінансової потужності, "Датагруп" перебуваючи в зоні загроз, подолавши критичну точку біфуркації, відзначається загроза втрати генерації прибутку (за рахунок власного капіталу, а також активів) та зростання боргового навантаження; загроза втрати конкурентоспроможності через зниження ефективності компанії в продукуванні нових товарів, послуг по відношенню до конкурентів відзначаються у компанії, ризик нестійкості бізнесу, загроза втрати ефективності інвестицій та ризик гальмування розвитку; ризик зниження продуктивності та мотивації персоналу прослідковується в ПрАТ "Датагруп".

Чутливість до ймовірної зміни обмінних курсів (що частка фінансових інструментів в іноземній валюті є постійною величиною на 31 грудня 2022 року і 31 грудня 2021 року) представлена у таблиці 4.27.

Таблиця 4.27

Чутливість до ймовірної зміни обмінних курсів ПрАТ "Датагруп"

Зміна курсу валют	2018		2019		2020		2021		2022	
	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув	Збільш/ (змен) у %	Збільш/ (змен) прибутку до оподаткув
Зміна обмінного курсу долара США	+10,00%	114	+10,00%	(388)	+10,00%	(445)	+10,00%	3513	+10,00%	(4788)
Зміна обмінного курсу євро	+10,00%	7522	+10,00%	1360	+10,00%	2564	+10,00%	4563	+10,00%	(3122)

продовження таблиці 4.27

Зміна обмінного курсу долара США	-1,00%	780	-1,00%	950	-1,00%	670	-1,00%	5 80	-1,00%	(780)
Зміна обмінного курсу євро	-1,00%	(675)	-1,00%	(2740)	-1,00%	(4564)	-1,00%	(3140)	-1,00%	(980)

(складено автором за [401]

Комплаєнс ризик у ПрАТ "Датагруп" – низький, стандарти NIST використовуються, стійкість до комплаєнс-ризиків номальна, спроможна чинити опір кібератакам, оцінка "А –" (рис. 4.20).

За аналізований період всі досліджувані підприємства понесли втрати через валютні коливання, коваріативний шок панував в Україні в 2022 році із початком повномаштбного вторгнення на її територію, рівень інфляції зріс майже на 28%, що суттєво позначилося на результатах діяльності постачальників електронних комунікаційних послуг. Врахування комплаєнс-ризиків важливе у контексті євроінтеграційних процесів та гармонізації регулятивних документів щодо управління підприємствами (управління ризиками) в Україні у відповідності до вимог ЄС.

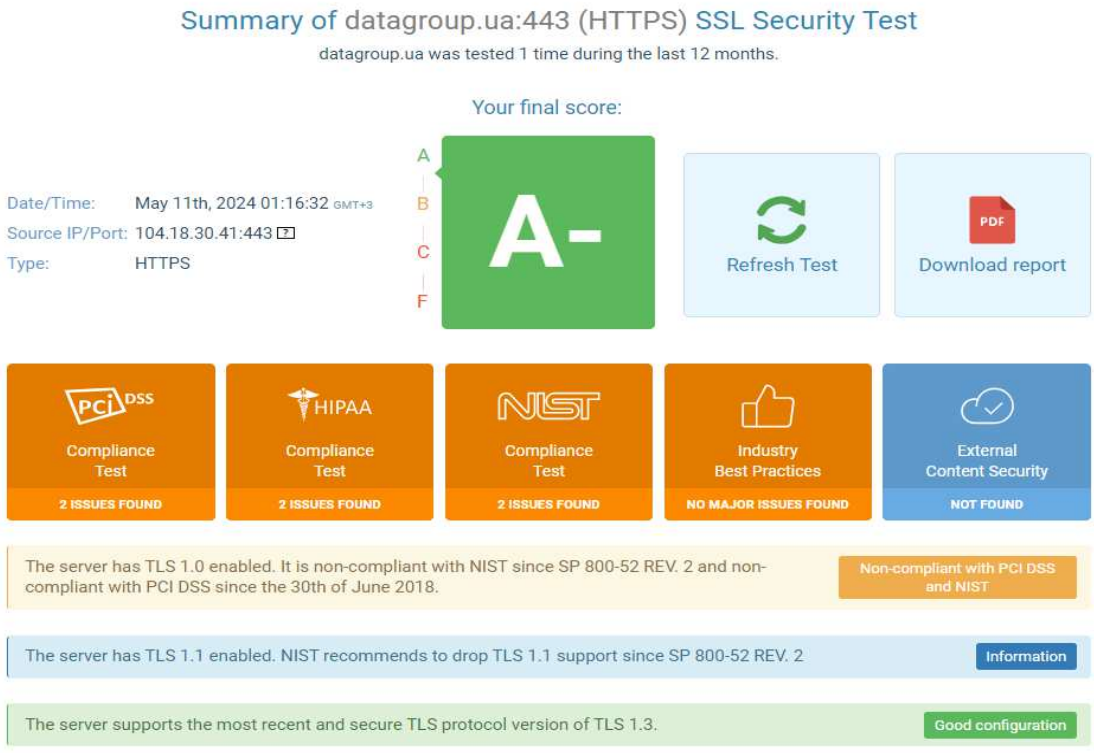


Рис. 4.20. Комплаєнс ризики (загрози) ПрАТ "Датагруп "

(складено за даними NIST)

Із метою узагальнення результатів моніторингу безпекової площини функціонування українських підприємств-постачальників електронних комунікаційних послуг, доцільно визначити інтегральний показник безпеки підприємства ($I_{БП}$). Вагові коефіцієнти для кожної метрики безпеки підприємства диференціюються за ступенем гармонізації інтересів стейкхолдерів (відповідно до узгодженості із цільовими безпековими орієнтирами) і визначатимуться за наступним алгоритмом:

1) аналіз метрик безпеки та визначення ступеня гармонізації розрахованих показників із інтересами стейкхолдерів;
2) визначення вертикалей взаємоузгодженості інтересів стейкхолдерів із цільовими результатами безпеки;
3) визначення вагових коефіцієнтів відповідно до результатів гармонізації інтересів (вертикалей) із отриманими результатами метрик безпеки.

Ступінь гармонізації інтересів стейкхолдерів щодо цілей безпеки, як результату досягнення цільових безпекових орієнтирів (що вимірюються метриками безпеки) з визначеними ваговими коефіцієнтами для кожного результату безпеки (пропорційно рівню угодженості інтересів стейкходерів) представлено у табл. 4.28.

Таблиця 4.28

Вертикалі узгодженості інтересів стейкхолдерів підприємства ПЕКМП із цільовими результатами безпеки

Стейкхолдери	Рівень узгодженості інтересів	Метрики (показники безпеки)	Ваговий коефіцієнт	Цільові результати безпеки підприємства
Вертикаль:	Високий (>75%)			
Власники Інвестори Акціонери Регулятор	95%	Коефіцієнт рентабельності власного капіталу	0.20	Прибутковість Платоспроможність Розвиток Стійкість Конкурентоспроможність
Менеджер, кредитори, інвестори, конкуренти	86%	Коефіцієнт рентабельності капіталу	0.15	Прибутковість Конкурентоспроможність Платоспроможність Розвиток

продовження таблиці 4.28

Інвестори, власники, Регулятор	84%	Коефіцієнт рентабельності EBITDA	0.15	Прибутковість Конкурентоспроможність Платоспроможність Розвиток
Вертикаль:	Нормальний (60-75%)			
Кредитори Контрагенти Власники Керівники Регулятор	67%	Коефіцієнт рентабельності надання послуг	0.12	Прибутковість Платоспроможність Розвиток
Вертикаль:	Середній (40-60%)			
Інвестори, кредитори Власники Керівники, Регулятор, Споживачі	52%	Коефіцієнт рентабельності робіт, послуг	0.10	Прибутковість Конкурентоспроможність
Конкуренти, власники, Регулятор, споживачі	46%	Коефіцієнт рентабельності валовий	0.10	Прибутковість Конкурентоспроможність Платоспроможність Розвиток
Інвестори, кредитори, керівники	51%	Коефіцієнт рентабельності операційний	0.10	Прибутковість Платоспроможність Розвиток
Вертикаль:	Низький (25-40%)			
Інвестори, власники, регулятор	38%	Коефіцієнт рентабельності інвестованого капіталу	0.05	Розвиток Прибутковість
Вертикаль:	Недостатній (до 25%)			
Власники, кредитори, керівники, регулятор	24%	Коефіцієнт ефективності використання основних засобів	0.015	Розвиток Прибутковість
Персонал, власники	23%	Коефіцієнт ефективності інтелектуального капіталу	0.015	Прибутковість Розвиток Конкурентоспроможність

(розраховано та складено автором)

Зважаючи на запропонований методологічний підхід до оцінки відповідності інтересам стейкхолдерів, отримуємо наступні вагові коефіцієнти: коефіцієнт рентабельності надання послуг – 0.12; коефіцієнт рентабельності робіт, послуг – 0.10; коефіцієнт рентабельності власного капіталу – 0.20; коефіцієнт рентабельності капіталу – 0.15; коефіцієнт рентабельності EBITDA – 0.15; коефіцієнт рентабельності валовий – 0.10; коефіцієнт рентабельності операційний – 0.10; коефіцієнт рентабельності інвестованого капіталу – 0.05;

коефіцієнт ефективності використання основних засобів – 0.015; коефіцієнт ефективності інтелектуального капіталу – 0.015.

Встановлені вагові коефіцієнти враховують вплив кожного показника на загальну економічну безпеку підприємства, зокрема їх роль у фінансовій стійкості, прибутковості та здатності до розвитку. Розрахунок інтегрального показника економічної безпеки підприємства з урахуванням вагових коефіцієнтів (формула 4.3):

$$I_{БП} = \sum_{i=1}^{10} \omega_i * x_i, \quad (4.3)$$

де - ω_i - ваговий коефіцієнт для і-го показника (метрики) безпеки;

x_i – значення і-го показника (метрики) безпеки.

Вагові коефіцієнти відображають відносну важливість кожного показника з точки зору економічної безпеки та стійкості підприємства за умов невизначеності. Формула для інтегрального показника безпеки (4.3) підприємств матиме наступний вигляд (формула 4.4):

$$I_{БП} = 0.2 * K_{Rвк} + 0.15 * K_{R\ кап} + 0.15 * K_{R\ EBITDA} + 0.12 * K_{R\ послуг} + 0.1 * K_{R\ прод,\ роб,\ посл} + 0.1 * K_{R\ валовий} + 0.1 * K_{R\ операційний} + 0.05 * K_{ефект-ті\ інвестованого\ капіталу} + 0.015 * K_{фондовіддачі\ ОЗ} + 0.015 * K_{ефект-ті\ інтелектуального\ капіталу} \quad (4.4)$$

Даний підхід дозволяє комплексно оцінити економічну безпеку підприємства з урахуванням впливу кожного цільового безпекового орієнтира на загальну стійкість та адаптивність підприємства до умов невизначеності.

Результати розрахунків інтегральних індексів безпеки підприємств: ПЕКМП ПрАТ “Київстар”, ПрАТ “ВФ Україна”, ТОВ “Лайфселл”, АТ “Укртелеком”, ПрАТ “Датагруп” представлено відповідно у таблицях (табл. 4.29, табл. 4.30, табл. 4.31, табл. 4.32., табл. 4.33).

Таблиця 4.29

Інтегральний індекс безпеки підприємства ПЕКМП ПрАТ “Київстар”

Метрики ЦРБ (x_i)	Роки					*Вагові коеф (ω_i)*
	2018	2019	2020	2021	2022	
$K_{R\ надання\ послуг}$	0,36	0,4	0,41	0,39	0,31	*0,12*
$K_{R\ прод,\ роб,\ посл}$	1,48	1,88	1,95	1,91	1,36	*0,1*
$K_{Rвк}$	0,45	0,15	0,21	0,65	0,55	*0,2*
$K_{R\ кап}$	0,28	0,09	0,1	0,32	0,27	*0,15*
$K_{R\ EBITDA}$	0,603	0,634	0,678	0,676	0,575	*0,15*
$K_{R\ валовий}$	0,96	0,97	0,66	0,97	0,58	*0,1*
$K_{R\ операційний}$	0,42	0,48	0,52	0,51	0,41	*0,1*
$K_{R\ ROIC\ (інвестованого\ капіталу}$	0,94	2,36	2,09	2,21	1,56	*0,05*
$K_{фондовіддачі\ ОЗ}$	2,34	1,84	1,8	1,75	1,6	*0,015*
$K_{ефект\text{-}ті\ інтелектуального\ капіталу}$	9,74	10,23	9,67	9,28	6,35	*0,015*
$I_{БП}$	0,77985	0,81865	0,79745	0,94115	0,7062	*1*

(розраховано та складено автором)

Таблиця 4.30

Інтегральний індекс безпеки підприємства ПЕКМП ПрАТ “ВФ Україна”

Метрики ЦРБ (x_i)	Роки					*Вагові коеф. (ω_i)*
	2018	2019	2020	2021	2022	
$K_{R\ надання\ послуг}$	0,16	0,14	0,066	0,19	0,056	*0,12*
$K_{R\ прод,\ роб,\ посл}$	0,81	0,92	0,989	1,19	1,371	*0,1*
$K_{Rвк}$	0,13	0,19	0,076	0,24	0,067	*0,2*
$K_{R\ кап}$	0,07	0,1	0,03	0,103	0,014	*0,15*
$K_{R\ EBITDA}$	0,55	0,54	0,43	0,57	0,36	*0,15*
$K_{R\ валовий}$	0,45	0,48	0,5	0,54	0,6	*0,1*
$K_{R\ операційний}$	0,22	0,23	0,28	0,29	0,35	*0,1*
$K_{R\ ROIC\ (інвестованого\ капіталу}$	0,26	0,67	0,3	1	0,3	*0,05*
$K_{фондовіддачі\ ОЗ}$	1,1	1,3	1,47	1,62	1,6	*0,015*
$K_{ефект\text{-}ті\ інтелектуального\ капіталу}$	6,47	5,73	6,47	5,87	6,47	*0,015*
$I_{БП}$	0,41275	0,45275	0,40312	0,5361	0,44437	*1*

(розраховано та складено автором)

Таблиця 4.31

Інтегральний індекс безпеки підприємства ПЕКМП ТОВ “Лайфселл”

Метрики ЦРБ (x_i)	Роки					*Вагові коеф.(ω_i)*
	2018	2019	2020	2021	2022	
$K_{R\ надання\ послуг}$	-0,115	-0,199	0,379	0,072	0,103	*0,12*
$K_{R\ прод,\ роб,\ посл}$	0,218	0,287	0,347	0,475	0,497	*0,1*
$K_{Rвк}$	-0,135	-0,251	0,162	0,038	0,111	*0,2*
$K_{R\ кап}$	-0,044	-0,082	0,152	0,036	0,053	*0,15*
$K_{R\ EBITDA}$	0,62	0,54	0,54	0,56	0,6	*0,15*
$K_{R\ валовий}$	0,18	0,22	0,26	0,32	0,33	*0,1*
$K_{R\ операційний}$	0,015	0,063	0,11	0,19	0,2	*0,1*
$K_{R\ ROIC\ (інвестованого\ капіталу}$	-0,15	-0,66	0,99	0,24	0,39	*0,05*
$K_{фондовіддачі\ ОЗ}$	0,99	1,18	1,34	1,31	1,48	*0,015*
$K_{ефект\text{-}ті\ інтелектуального\ капіталу}$	2,59	3,17	3,65	5,47	5,44	*0,015*
$I_{БП}$	0,1331	0,08387	0,37773	0,31784	0,35851	*1*

(розраховано та складено автором)

Таблиця 4.32

Інтегральний індекс безпеки підприємства ПЕКМП АТ “Укртелеком”

Метрики ЦРБ	Роки					*Вагові коеф. (ω_i)*
	2018	2019	2020	2021	2022	
$K_{R\ надання\ послуг}$	0,02	-0,14	0,37	0,1	-0,45	*0,12*
$K_{R\ прод,\ роб,\ посл}$	0,54	0,48	0,49	0,26	0,15	*0,1*
$K_{Rвк}$	0,019	-0,12	0,2	0,038	-0,27	*0,2*
$K_{R\ кап}$	-0,011	-0,076	0,14	0,028	-0,19	*0,15*
$K_{R\ EBITDA}$	0,603	0,634	0,678	0,676	0,575	*0,15*
$K_{R\ валовий}$	0,96	0,97	0,66	0,97	0,58	*0,1*
$K_{R\ операційний}$	0,42	0,48	0,52	0,51	0,41	*0,1*
$K_{R\ ROIC\ (інвестованого\ капіталу}$	0,94	2,36	2,09	2,21	1,56	*0,05*
$K_{фондовіддачі\ ОЗ}$	2,34	1,84	1,8	1,75	1,6	*0,015*
$K_{ефект\text{-}ті\ інтелектуального\ капіталу}$	9,74	10,23	9,67	9,28	6,35	*0,015*
$I_{БП}$	0,5152	0,53495	0,65065	0,57515	0,261	*1*

(розраховано та складено автором)

Таблиця 4.33

Інтегральний індекс безпеки підприємства ПЕКМП ПрАТ “Датагруп”

Метрики ЦРБ	Роки					*Вагові коеф. (ω_i)*
	2018	2019	2020	2021	2022	
$K_{R\ надання\ послуг}$	0,02	0,11	0,15	0,12	-0,09	*0,12*
$K_{R\ прод,\ роб,\ посл}$	0,53	0,76	0,49	0,83	0,59	*0,1*
$K_{Rвк}$	0,05	0,26	0,25	0,23	-0,1	*0,2*
$K_{R\ кап}$	0,01	0,1	0,12	0,05	-0,28	*0,15*
$K_{R\ EBITDA}$	0,22	0,32	0,37	0,37	0,38	*0,15*
$K_{R\ валовий}$	0,34	0,43	0,49	0,45	0,37	*0,1*
$K_{R\ операційний}$	0,03	0,21	0,27	0,23	0,15	*0,1*
$K_{R\ ROIC\ (інвестованого\ капіталу}$	0,1	0,64	0,82	0,58	-0,23	*0,05*
$K_{фондовіддачі\ ОЗ}$	1,52	1,67	1,59	1,42	1,21	*0,015*
$K_{ефект-ті\ інтелект.\ капіталу}$	1,58	1,98	1,93	1,86	1,38	*0,015*
$I_{БП}$	0,1884	0,35495	0,3603	0,3526	0,12255	*1*

(розраховано та складено автором)

За результати розрахунку загальний інтегральний показник безпеки дозволить відобразити стани безпеки підприємства. Для того, щоб застосувати запропоновану у роботі методологію визначення безпекової площини, потрібно вирахувати порогове значення безпеки, використовуючи нормативи за метриками безпеки, як базові, що формуватимуть порогове нижнє значення і перший стан безпеки – відносний стан безпеки (табл. 4.34).

Таблиця 4.34

Інтегральний індекс безпеки підприємств ПЕКМП

Метрики ЦРБ	Нормативне значення метрик	*Вагові коеф.(ω_i)*
$K_{R\ надання\ послуг}$	0,05	*0,12*
$K_{R\ прод,\ роб,\ посл}$	0,3	*0,1*
$K_{Rвк}$	0,2	*0,2*
$K_{R\ кап}$	0,1	*0,15*
$K_{R\ EBITDA}$	0,46	*0,15*
$K_{R\ валовий}$	0,5	*0,1*
$K_{R\ операційний}$	0,218	*0,1*
$K_{R\ ROIC\ (інвестованого\ капіталу}$	0,14	*0,05*
$K_{фондовіддачі\ ОЗ}$	1,513	*0,015*
$K_{ефект-ті\ інтелектуального\ капіталу}$	4,37	*0,015*
$I_{БП0}$	0,327	*1*

(розраховано та складено автором)

З метою визначення станів безпеки, що запропоновані у роботі (відносний, нормальний, стабільний, досконалий - стани безпеки; незначний, передкризовий, кризовий, критичний – стани небезпеки), вважаємо за доцільне встановити базисне порогове нижнє значення $I_{БП0,}$ за яким визначатиметься перший стан безпеки – відносний стан безпеки.

Стани безпеки, визначатимуться за медіанними значеннями щодо відхилень показників від нормативу метрик безпеки у наступних співвідношеннях (табл. 4.35):

Таблиця 4.35

Диференція станів безпеки підприємства за відхиленнями інтегрального індексу безпеки

Відхиленя інтегрального індексу безпеки $I_{БП0,}$	Стан безпеки/небезпеки
до 1%	Нормальний стан безпеки
від 1% до 3%	Відносний стан небезпеки
від 4% до 7%	Незначний стан небезпеки
від 8% до 11%	Передкризовий стан небезпеки
від 12% до 21%	Кризовий стан небезпеки
більше 22%	Критичний стан небезпеки

(розраховано та складено автором)

Дані відхилення будуть враховуватись при моделюванні безпекових площин досліджуваних підприємств, визначенні їх стійкості за цільовими результами безпеки відхилення від критеріальних точок (репелер та біфукації).

Отже, за запропонованою результатми розрахунків метрих цільових результатів безпеки підприємтсва та загроз, з’ясовано, що ПрАТ “ВФ Україна” знаходиться на межі втрати здатності генерувати грошовий потік та втрати фінансової потужності, ПАТ “Укртелеком” та “Датагруп” перебувають в зоні загроз, подолавши критичну точку біфуркації, в зоні ризику перебуває ПрАТ “ВФ Україна”. Загрози втрати генерації прибутку (за рахунок власного капіталу, а також активів) та зростання боргового навантаження відзначаються у ПрАТ

“ВФ Україна”, ТОВ “Лайфселл”, АТ “Укртелеком”, ПрАТ “Датагруп”. Загроза втрати спроможності до самофінансування, інвестиційної привабливості, зниження операційної ефективності наявна у компанії АТ “Укртелеком”; загрози втрати конкурентоспроможності через зниження ефективності компанії в продукуванні нових товарів, послуг по відношенню до конкурентів відзначаються у компанії ТОВ “Лайфселл”, АТ “Укртелеком”, ПрАТ “Датагруп”; ризик нестійкості бізнесу характерний для ТОВ “Лайфселл” та ПрАТ “Датагруп”, під загрозою АТ “Укртелеком”; загроза втрати ефективності інвестицій та ризик гальмування розвитку в АТ “Укртелеком” та ПрАТ “Датагруп”; ризик зниження продуктивності та мотивації персоналу прослідковується в ПрАТ “Датагруп”, загроза в АТ “Укртелеком”. Відзначено потребу у відображенні безпекової площини функціонування підприємств для формування резистентності кожного окремого підприємства в динаміці для пошуку підходу до прийняття ризиків або підходу до управління безпекою підприємства у разі його високої чутливості до умов функціонування. Модель Ляпунова найкраще відобразить стани безпеки, що ідентифікуються точками атрактора, біфуркації та репелерними, за результатами якої буде прийматися рішення щодо управління підприємством та поверненню його у безпекову площину, у разі відхилень від нормативів цільових безпекових орієнтирів.

4.3. Моделювання управління безпекою підприємств-постачальників електронних комунікаційних послуг

Безпека підприємства визначена нами як стан, характеризується динамічністю, переходом від рівноважного (за відсутності зовнішніх впливів) до нестійкого стану (під дією внутрішніх та зовнішніх впливів). У залежності від умов господарювання поведінка підприємств різниться та змінюється у часі, може принципово змінитися, а може повернутися до початкової, дані можливості описують спроможінсть стійкості функціонування підприємства. У

безпековій площині стійкість відіграє особливу роль, оскільки вказує на спроможність підприємства повертатися до стану, за якого забезпечуватимуться цільові безпекові результати-орієнтири. Розмежування ризиків та загроз спонукає до визначення точок репелер та біфуркації у безпековій площині, через відхилення від нормативних значень, що призводить до зміни станів безпеки. Характер стійкості особливих точок, можна описати диференціальним рівнянням (формула 4.5):

$$\frac{dx_i}{dt} = f_i(t, x_1, x_2, \dots\dots, x_n), \text{ i = 1, 2, ……., n,} \quad (4.5)$$

де $f_i(t, x_1, x_2, \dots\dots, x_n)$ – функція Ляпунова, яка обирається без попереднього знаходження рішень системи [360].

Метод функцій Ляпунова полягає у безпосередньому дослідженні стійкості, знаходження точки перебування підприємства у стані рівноваги. Точками спокою є наступні значення x: $x_1 = 0, i = 1, 2, \dots, n$.

Функція $V(x_1, x_2, \dots\dots, x_n)$ є знаковизначеною й вказуватиме на перехід від стану безпеки до небезпеки, відповідно позитивно-визначеною та негативно-визначеною, якщо вона належить області (формула 4.6):

$$|x_i| \leq h, i = 1, 2, \dots, n, \quad (4.6)$$

де h – достатньо мале позитивне число, що може прийняти значення лише одного визначеного знаку та перетворюється у 0 лише за $x_1 = \cdots = x_n = 0$, у такому разі n = 3 функції:

$$V = x_1^2 + x_2^2 + x_3^2) \text{ та } V = x_1^2 + 2x_1 * x_2 + 2x_2^2 + x_3^2)$$

$h > 0$ приймають визначено-позитивні різновеликі значення.

Функція $V(x_1, x_2, \dots\dots, x_n)$ називається знакопостійною (позитивною або від'ємною), якщо вона в області $|x_i| \leq h, \ i = 1, 2, \dots, n$ може приймати

значення тільки одного визначеного стану, але може приймати лише один визначений знак та може приймати значення 0 при:

$$V(x_1, x_2, x_3) = x_1^2 + x_2^2 + 2x_1x_2 + x_3^2)$$

$$x_1^2 + x_2^2 + \cdots + x_n^2 \neq 0$$

буде визначено-позитивною, знакопостійною. Функцію можна записати наступним чиною:

$$V(x_1, x_2, x_3) = x_1^2 + x_2^2 + 2x_1x_2 + x_3^2)$$

$V(x_1, x_2, x_3) = (x_1 + x_2)^2 + x_3^2$, звідки випливає, що функція перетворюється в 0 також при $x_1^2 + x_2^2 + x_3^2 \neq 0$, а саме при $x_3 = 0$ та будь яких x_1 та x_2, таких що $x_1 = -x_2$.

При $V(x_1, x_2, x_3)$ є диференційована функція власних аргументів і x_1, x_2, x_3 , які є деякими функціями часу, котрі задовольняють системі диференціальних рівнянь:

$$\frac{dx_i}{dt} = f_i(t, x_1, x_2, \dots\dots, x_n) \text{ i = 1, 2, ……., n,}$$

тоді для загальної похідної функції V по часу матимемо (формула 4.7):

$$\frac{dV}{dt} = \sum_{i=1}^{n} \frac{dV}{dx_i} * \frac{dx_i}{dt} = \sum_{i=1}^{n} \frac{dV}{dx_i} f(x_1, x_2, \dots\dots, x_n) \quad (4.7)$$

Величина $\frac{dV}{dt}$ визначається за формулою , яка називається повною похідною функції V по часу, яка складається за рівняннями $\frac{dx_i}{dt} = f_i(t, x_1, x_2, \dots\dots, x_n)$, i = 1, 2, ……., n.

Якщо для системи диференціальних рівнянь положення рівноваги підприємства, $\frac{dx_i}{dt} = f_i(x_1, x_2, \dots\dots, x_n)$, i = 1, 2, ……., n існує знаковизначна функція $V(x_1, x_2, \dots\dots, x_n)$, тоді повна похідна функції $\frac{dV}{dt}$, котра за часом складена в силу рівноваги підприємства $\frac{dx_i}{dt} = f_i(x_1, x_2, \dots\dots, x_n)$ існує

знакопостійна функція знака протилежного з V або тотожно рівна нулю, тоді точка спокою $x_i = 0, i = 1, 2, \dots, n$, визначає стан безпеки підприємства стійким.

Якщо ж для системи дифиренціальних рівнянь положення рівноваги підприємства, $\frac{dx_i}{dt} = f_i(x_1, x_2, \dots\dots, x_n)$, i = 1, 2, ……., n існує знаковизначна функція $V(x_1, x_2, \dots\dots, x_n)$, повна похідна якої $\frac{dV}{dt}$, складена за часом в силу рівноваги підприємства $\frac{dx_i}{dt} = f_i(x_1, x_2, \dots\dots, x_n)$, тоді існує знаковизначаюча функція знака протилежного з V, за якої точка спокою $x_i = 0$, рівноваги підприємства визначає стан безпеки підприємства асимптоматично стійким.

Для системи диференціальних рівнянь $\frac{dx_i}{dt} = f_i(x_1, x_2, \dots\dots, x_n)$ існує диференційна в області рівноваги функція $V(x_1, x_2, \dots\dots, x_n)$, така, що $V(0, 0, \dots\dots, 0) = 0$. Якщо її повна похідна $\frac{dV}{dt}$, яка складена за $\frac{dx_i}{dt} = f_i(x_1, x_2, \dots\dots, x_n)$, є визначено-позитивна функція, за якої $V(x_1, x_2, \dots\dots, x_n)$ приймає позитивне значення, тоді точка спокою $x_i = 0, i = 1, 2, \dots, n$ визначає стан безпеки підприємства нестійким.

Модель стійкості підприємств за цільовими результатами безпеки апробовано на досліджуваних підприємствах: ПрАТ “Київстар”; ПрАТ “ВФ Водафон”, ТОВ “Лайфселл”, АТ “Укртелеком”, ПрАТ “Датагруп”, результати моделювання представлено графічно відповідно на рис. 4.21, рис.4. 22, рис. 4.23, рис. 4.24, рис. 4.25.

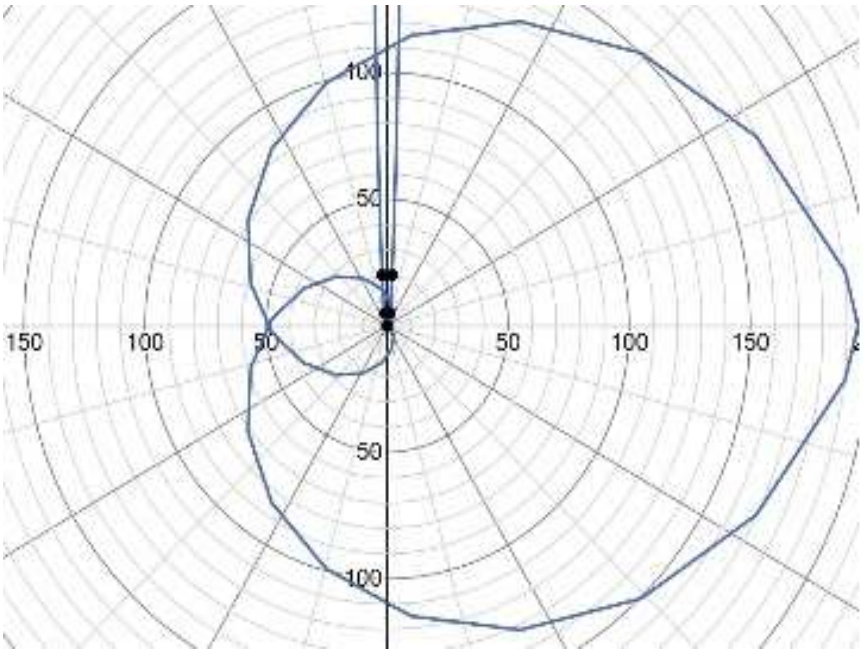


Рис. 4.21. Стійкість підприємства ПрАТ “Київстар” за цільовими результатами безпеки *(авторська розробка)*

Компанія “Київстар” вважається стійкою, оскільки за цільовими результатами безпеки відхилення від критеріальних точок не відбулося. Стан безпеки – стабільний.

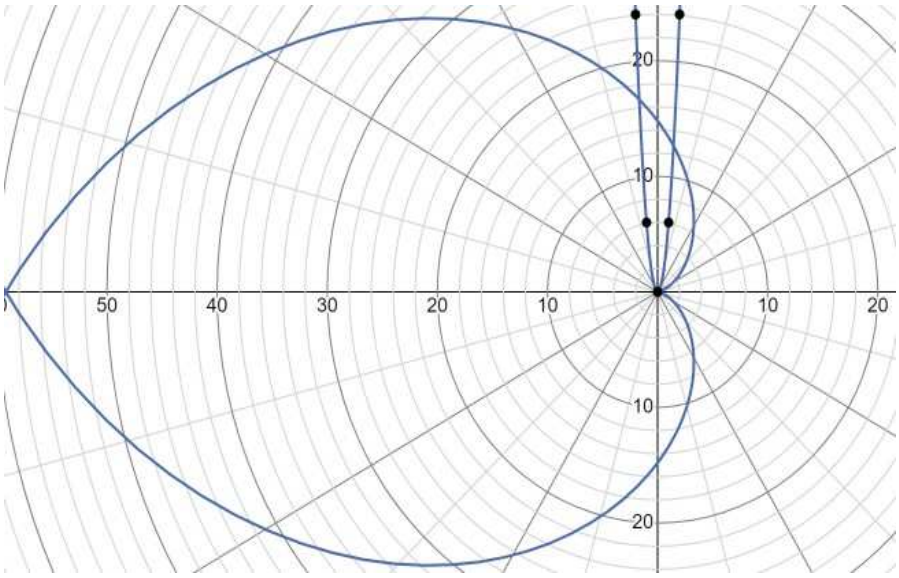


Рис. 4.22. Стійкість підприємства ПрАТ “ВФ Україна” за цільовими результатами безпеки
(авторська розробка)

Компанія “ВФ Україна” за цільовими результатами знаходиться за межами стійкості, відхилення становить до 5%, тому стан відзначається як відносний стан безпеки.

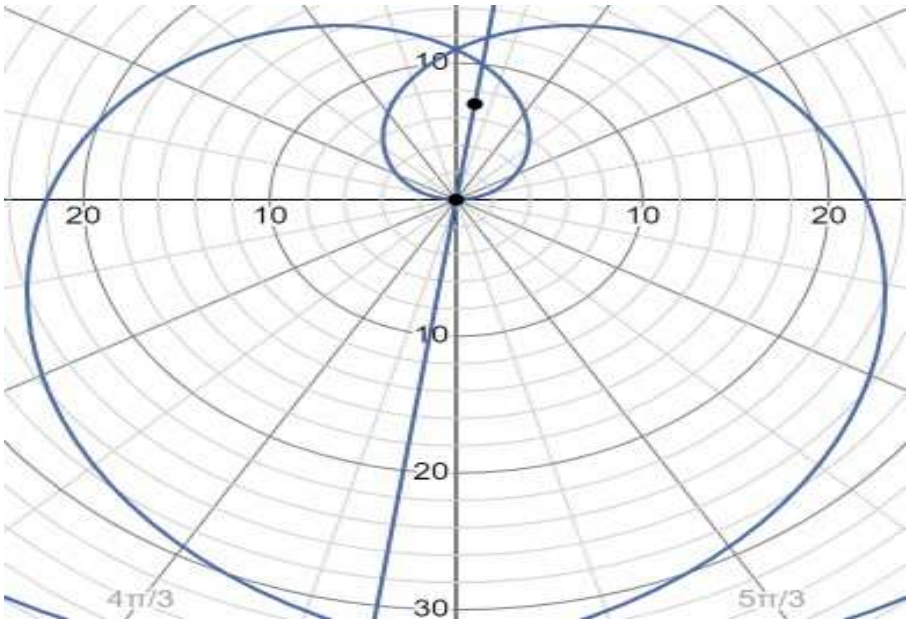


Рис. 4.23. Стійкість підприємства ТОВ “Лайфселл” за цільовими результатами безпеки *(авторська розробка)*

ТОВ “Лайфселл” перебуває у діапазоні відхилень цільових безпекових результатів у межах 14%, стан визначається, як кризовий.

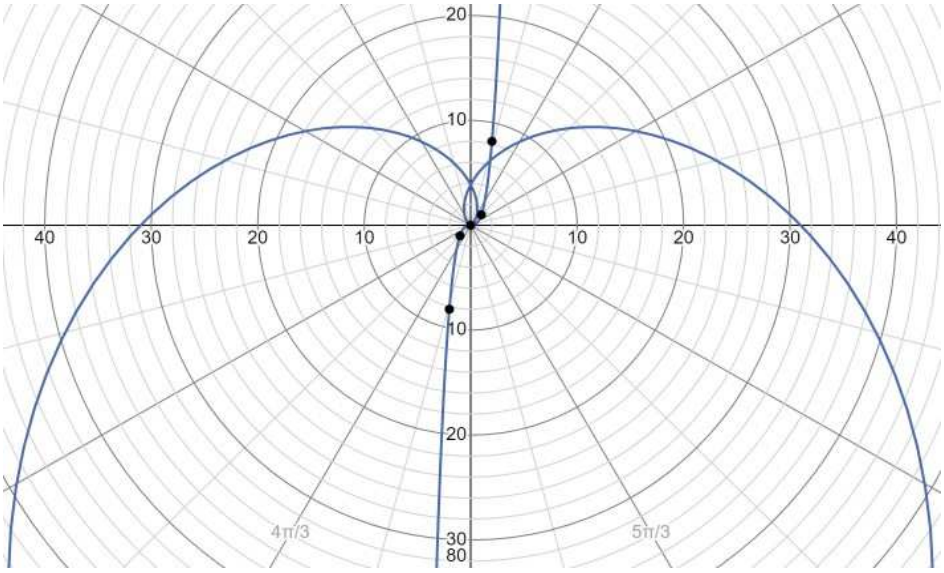


Рис. 4.24. Стійкість підприємства АТ “Укртелеком” за цільовими результатами безпеки *(авторська розробка)*

АТ “Укртелеком” демонструє нестійкість за цільовими результатами безпеки, відхилення становлять більше 19%, стан визначається як критичний.

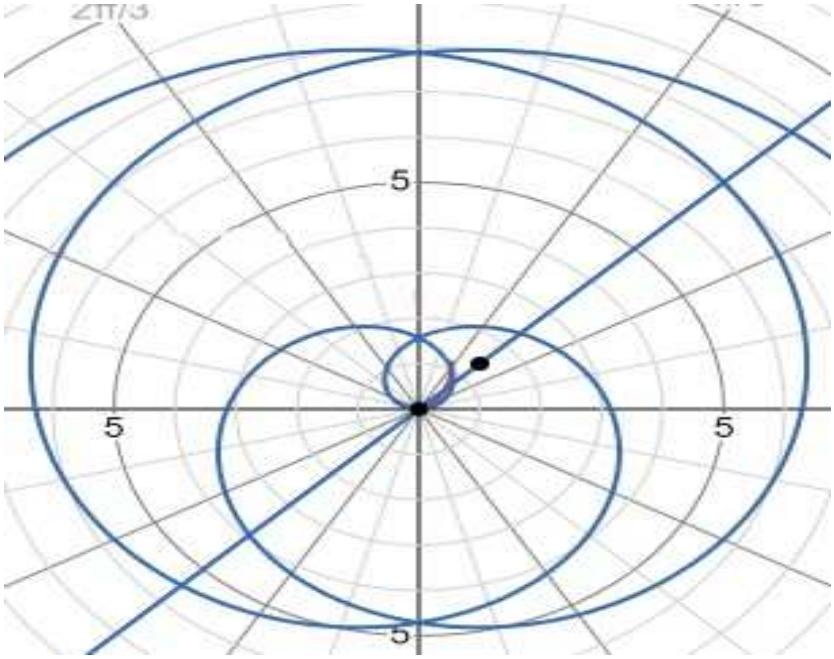


Рис. 4.25. Стійкість підприємства ПрАТ “Датагруп” за цільовими результатами безпеки *(авторська розробка)*

Стан безпеки ПрАТ “Датагруп” визначається як передкризовий, відхилення цільових безпекових результатів становить близько 8 %.

Припустимо, що подія А наступає лише за умови появи однієї із несумічних випадкових подій (гіпотез) H_1 H_2 H_i, що утворюють повну групу випадкових подій. Припустимо, що подія А вже відбулась, і необхідно визначити ймовірність того, що подія А відбулась саме завдяки реалізації гіпотези H_i . Дане питання вирішується за теоремою гіпотез або критерія Байєса, тому теорему гіпотез можна вважати наслідком теореми множення ймовірностей та формули повної ймовірності. Ймовірність $P\,(H_i|A)$, яка визначається як ймовірність гіпотези H_i за умови, що подія А відбулася, називається апостеріорною ймовірністю (на відміну від апріорної ймовірності $P\,(H_i)$, яка відома ще до

початку обчислень та моніторингу випробувань. Апостеріорна ймовірність обчислюється за формулою Байєса:

$$P\ (H_i|A) =\ P\ (H_i) * P\ (H_i|A)/P\ (A), \quad (4.8)$$

З метою зменшення ризиків або ж їх уникнення для досліджуваних підприємство розглядається 10 вірогідних випадків щодо прийняття рішення стейкхолдерами щодо інвестування в безпеку (табл. 4.36), яка враховуватиме ймовірність настання ризикових та загрозливих подій від різних варіацій вкладень у розвиток, капітальні [322]. При чому повна йовірність розраховується як:

$$P_{\text{інв}} =\ P_{\text{розв}} +\ P_{\text{ОЗ}} +\ P_{\text{захист}}, \quad (4.9),$$

де: $P_{\text{розв}}$ – інвестування з метою залучення клієнтів та розширення клієнтської бази;

$P_{\text{ОЗ}}$ – закупівля нового обладнання та устаткування;

$P_{\text{захист}}$ – витрати на програмне забезпечення та захист.

Таблиця 4.36

Варіанти прийняття стейкхолдерами рішень щодо інвестування

Рішення	Інвестування розвитку (задля збільшення кількості клієнтів, покращення якості послуг)	Споживання (ОЗ)	Інвестиції в безпеку
1	1,0	0,1	0
2	0,99	0	0,01
3	0,8	0,1	0,1
4	0,7	0,1	0,2
5	0,6	0,2	0,4
6	0,5	0,3	0,2
7	0,4	0,1	0,5
8	0,2	0,6	0,2
9	0,1	0,5	0,4
10	0	0,1	0,9
	Повна ймовірність подій = 1		

(розраховано автором)

Остаточне рішення щодо інвестування приймаються за критерієм Байєса, враховуючи наслідки від прийняття рішень.

Критерій Байєса слугує індикатором визначення оптимального рішення (максимальних вигід) за найменших витрат підприємства при інвестуванні в безпеку.

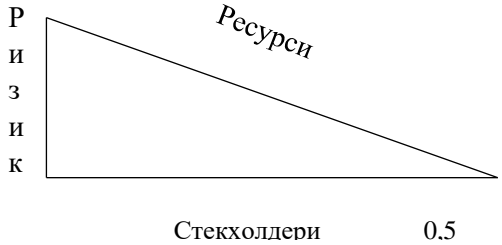
$$P = \frac{P\,(H) * P\,(A/H)}{P\,(A)}, \tag{4.10}$$

Розраховуємо вірогідність події за прийняття рішень, починаючи першим, закінчуючи останнім варіантом, які пропонуються стейкхолдерами.

Вірогідність настання події, тобто прийняття рішення:

$$P_1 = \frac{1 * 0}{0} = 0$$

Стійкість підприємств до ризиків, вірогідності ризиків для кожного із варіантів предствлено відповідно на рис. 4.26, рис. 4.27, рис. 4.28, рис. 4.29, рис. 4.30, рис. 4.31, рис. 4.32, рис. 4.33, рис.4.34, рис. 4.35.



$P_{\text{ризик}} = 1 - P_{\text{захист}}$

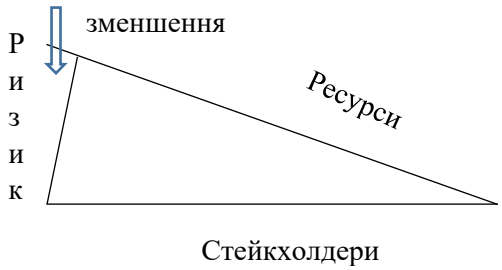
$P^1_{\text{ризик}} = 1 - 0 = 1\ (100\%)$

$P^1_{\text{захист}} = 0$ (не існує)

Рис. 4.26. Стійкість підприємства до ризиків у відповідності прийняття рішення стейкхолдерами за варіантом 1 *(авторська розробка)*

Вірогідність прийняття рішення за варіантом 2:

$$P_2 = \frac{0{,}99 * 0}{0,1} = 0$$



$P_{ризик} = 1 - P_{захист}$

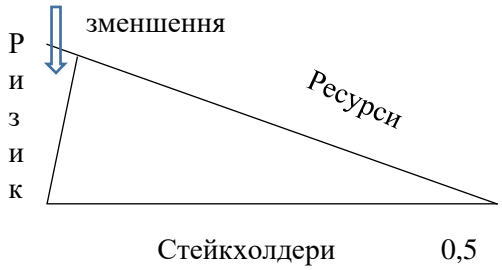
$P^2_{ризик} = 1 - 0,01 = 0,99$ (99% ризик)

$P^2_{захист} = 0,01$ (1%).

Рис. 4.27. Стійкість підприємства до ризиків у відповідності прийняття рішення стейкхолдерами за варіантом 2 *(авторська розробка)*

Вірогідність прийняття рішення за варіантом 3:

$$P_3 = \frac{0,8 * 0,1}{0,1} = 0,8$$



$P_{ризик} = 1 - P_{захист}$

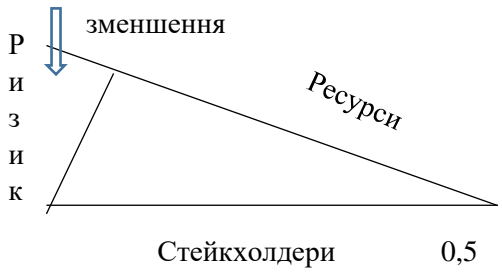
$P^3_{ризик} = 1 - 0,01 = 0,9$ (90 % ризик)

$P^3_{захист} = 0,1$ (10%).

Рис. 4.28. Стійкість підприємства до ризиків у відповідності прийняття рішення стейкхолдерами за варіантом 3 *(авторська розробка)*

Вірогідність прийняття рішення за варіантом 4:

$$P_4 = \frac{0,7 * 0,1}{0,2} = 0,35$$



$P_{ризик} = 1 - P_{захист}$

$P^4_{ризик} = 1 - 0,2 = 0,8$ (80 % ризик)

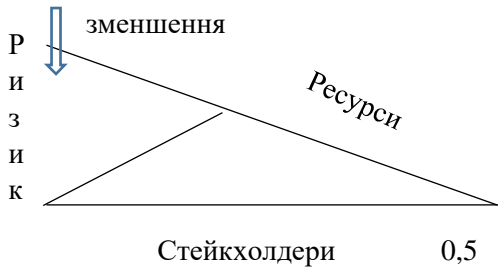
$P^4_{захист} = 0,2$ (20%).

Рис. 4.29. Стійкість підприємства до ризиків у відповідності прийняття рішення стейкхолдерами за варіантом 4

(авторська розробка)

Вірогідність прийняття рішення за варіантом 5:

$$P_5 = \frac{0{,}6 * 0{,}2}{0{,}4} = 0,3$$



$P_{\text{ризик}} = 1 - P_{\text{захист}}$

$P^5_{\text{ризик}} = 1 - 0,4 = 0,6$ (80 % ризик)

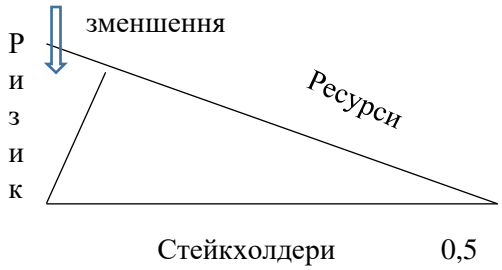
$P^5_{\text{захист}} = 0,4$ (40%).

Рис. 4.30. Стійкість підприємства до ризиків у відповідності прийняття рішення стейкхолдерами за варіантом 5

(авторська розробка)

Вірогідність прийняття рішення за варіантом 6:

$$P_6 = \frac{0{,}5 * 0{,}3}{0{,}2} = 0,75$$



$P_{\text{ризик}} = 1 - P_{\text{захист}}$

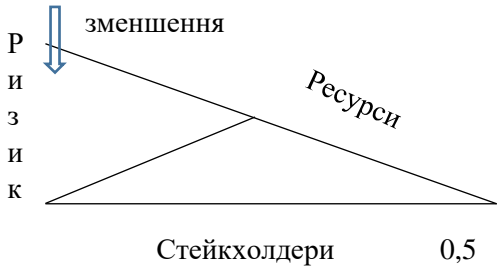
$P^6_{\text{ризик}} = 1 - 0,2 = 0,8$ (80 % ризик)

$P^6_{\text{захист}} = 0,2$ (20%).

Рис. 4.31. Стійкість підприємства до ризиків у відповідності прийняття рішення стейкхолдерами за варіантом 6

(авторська розробка)

Вірогідність прийняття рішення за варіантом 7:



$$P_{\text{ризик}} = 1 - P_{\text{захист}}$$

$$P^{7}_{\text{ризик}} = 1 - 0,5 = 0,5 \ (50\ \% \text{ ризик})$$

$$P^{7}_{\text{захист}} = 0,5 \ (50\%).$$

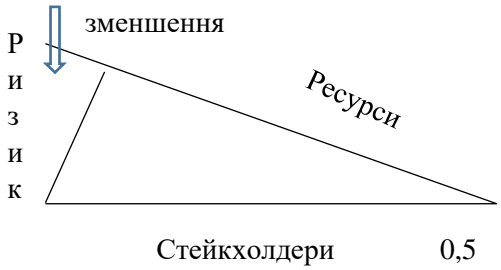
Рис. 4.32. Стійкість підприємства до ризиків у відповідності прийняття рішення стейкхолдерами за варіантом 7

(авторська розробка)

$$P_7 = \frac{0,4 * 0,1}{0,5} = 0,08$$

Вірогідність прийняття рішення за варіантом 8:

$$P_8 = \frac{0,2 * 0,6}{0,2} = 0,6$$



$$P_{\text{ризик}} = 1 - P_{\text{захист}}$$

$$P^{8}_{\text{ризик}} = 1 - 0,2 = 0,8 \ (80\ \% \text{ ризик})$$

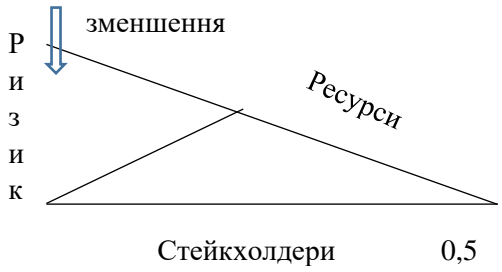
$$P^{8}_{\text{захист}} = 0,2 \ (20\%).$$

Рис. 4.33. Стійкість підприємства до ризиків у відповідності прийняття рішення стейкхолдерами за варіантом 8

(авторська розробка)

Вірогідність прийняття рішення за варіантом 9:

$$P_9 = \frac{0,1 * 0,5}{0,4} = 0,125$$



$$P_{\text{ризик}} = 1 - P_{\text{захист}}$$

$$P^{9}_{\text{ризик}} = 1 - 0,4 = 0,6 \quad (60\ \%\ \text{ризик})$$

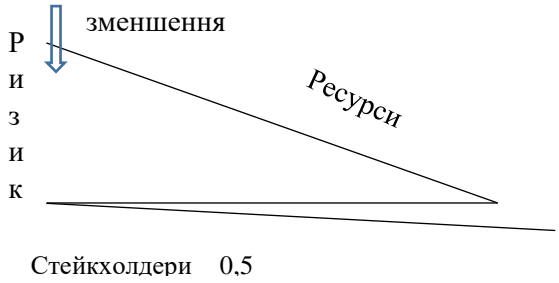
$$P^{9}_{\text{захист}} = 0,4\ (40\%).$$

Рис. 4.34. Стійкість підприємства до ризиків у відповідності прийняття рішення стейкхолдерами за варіантом 9

(авторська розробка)

Вірогідність прийняття рішення за варіантом 10:

$$P_{10} = \frac{0 * 0,1}{0,9} = 0$$



$$P_{\text{ризик}} = 1 - P_{\text{захист}}$$

$$P^{10}_{\text{ризик}} = 1 - 0,9 = 0,1 \quad (10\ \%\ \text{ризик})$$

$$P^{10}_{\text{захист}} = 0,9\ (90\%).$$

Рис. 4.35. Стійкість підприємства до ризиків у відповідності прийняття рішення стейкхолдерами за варіантом 10

(авторська розробка)

Варіація ризиків та стійкості підприємства в залежності від прийняття рішень стейкхолдерами щодо інвестування із відображенням ризиків та переходу їх у ділянку загроз за окремих ухвалень рішень наведена на рис. 4.36.

Як порогове заначення допустимого ризику δ прийнято на рівні 50% (оскільки рішення приймаються у такому співвідношенні стейкхолдерами), тоді, порівнюючи послідовно вірогідності прийняття рішень стейкхолдерами із : $P \geq$

$0{,}5 = \delta$ та шукаємо максимум (За $P^{8}_{\text{ризик}} = P^{6}_{\text{ризик}} = P^{3}_{\text{ризик}}$) та підставляючи у $\begin{cases} P_3 \\ P_6 \\ P_8 \end{cases} => \max$, отримуємо, що оптимальний результат досягається за P_3, що свідчить про доцільність рівномірного розподілу на обладнання та захист, за якого досягається найбільший ефект:

$$\begin{cases} 0{,}8 \\ 0{,}75 \\ 0{,}6 \end{cases} => P_3 \max = opt$$

За отриманими результатами, визначеним оптимальним значенням щодо вірогідності прийняття рішення є 3-й варіант прийняття рішення стейкхолдерами у співвідношенні: 0,8 – 0,1 – 0,1, тобто рівномірний розподіл вкладень коштів у обладнання та програмне забезпечення і захист забезпечить найвищий ефект захисту та гарантуватиме стійкість підприємства, а отже і безпеку.

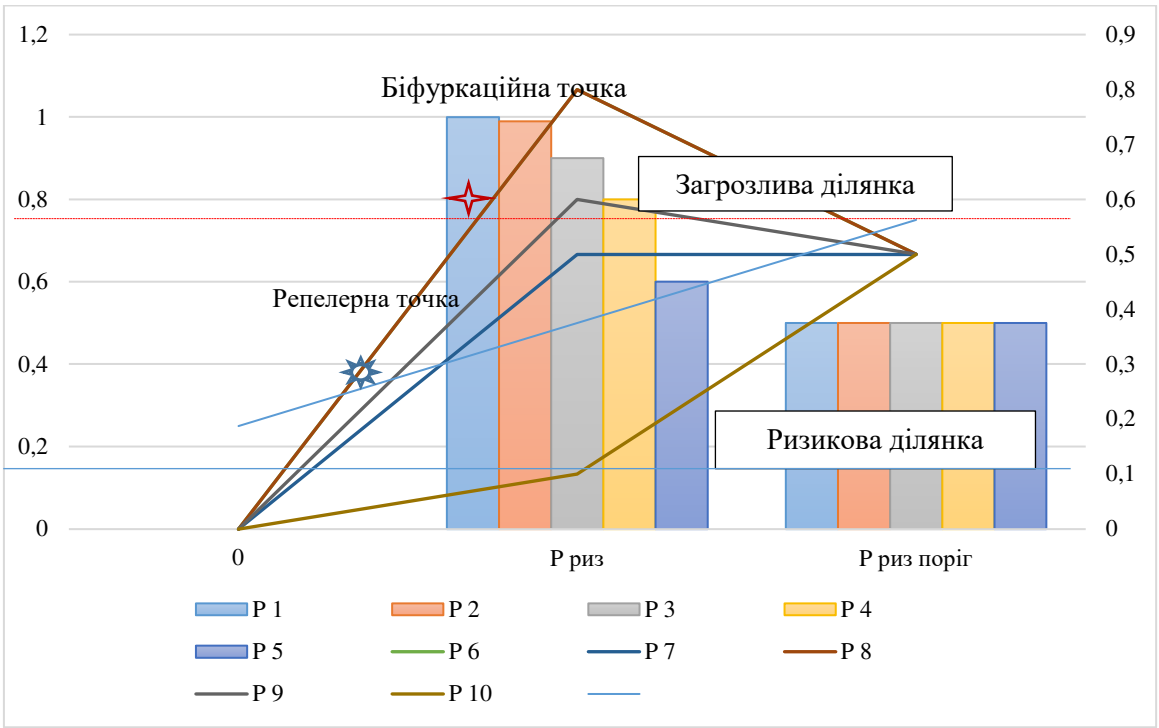


Рис. 4.36. Варіація ризиків та стійкості підприємства в залежності від прийняття рішень стейкхолдерами щодо інвестування

(авторська розробка)

Прийняття рішення за критерієм Байєса надає можливість гарантувати дієвість та ефективність інвестування, варіанти максимума та мінімума наведені на рис. 4.37.

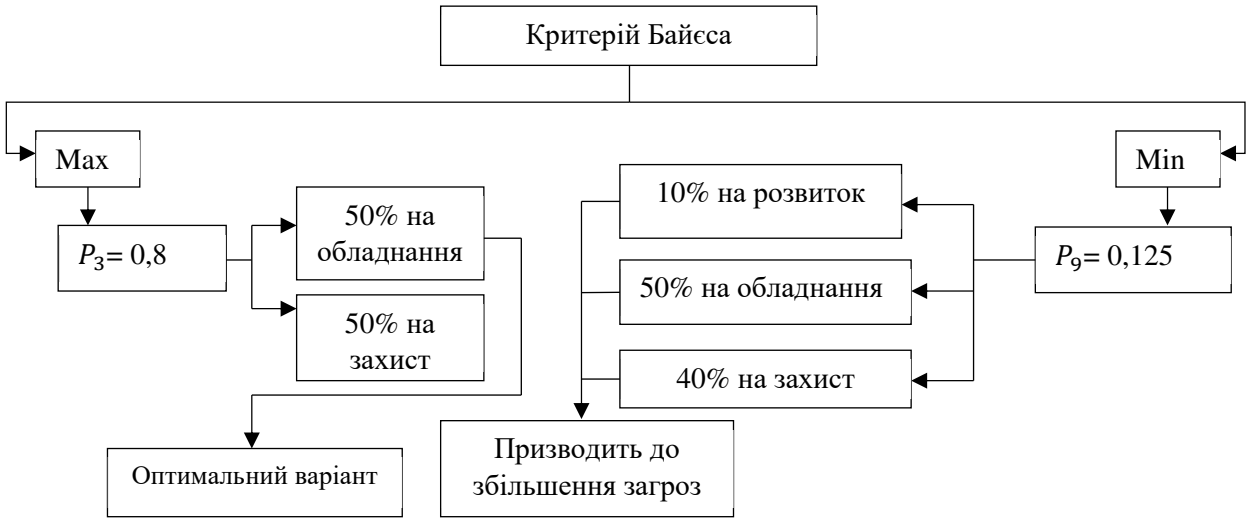


Рис. 4.37. Прийняття рішення стейкхолдерами щодо інвестування в безпеку підприємства за критерієм Байєса

(авторська розробка)

Мінімальне значення *P* досягається у 9-му із можливих варіантів прийняття рішень щодо розподілу вкладень на розвиток, основні засоби, програмне забезпечення та захист, що пояснюється тим, що інвестиції в захист старого обладнання або ж програмного забезпечення підприємств зв'язку не будуть ефективними, через низьку продуктивність, а також неспроможність задоволення потреб у якісному зв'язку, підтримання нових технологій та послуг електронних комунікацій. За даного варіанту збільшуються ризики для розширення бізнесу, виробничих потужностей, послуг та фінансові ризики, що свідчить про неефективність капіталовкладень в захист за такого варіанту (рис. 4.38).

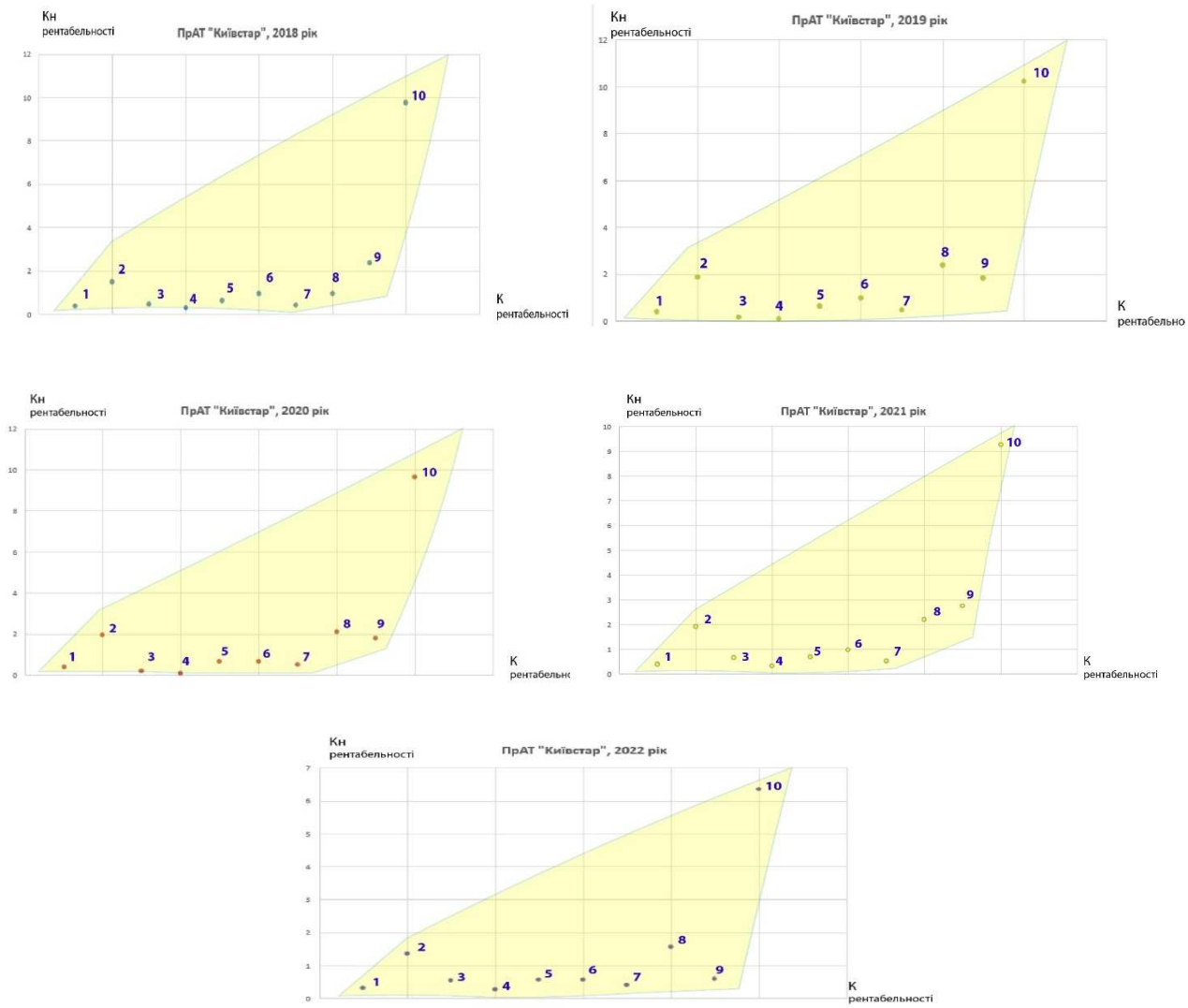


Рис. 4.38. Зональність ризиків та загроз ПрАТ “Київстар” за цільовими безпековими орієнтирами в динаміці (2018-2022 рр.)

(авторська розробка)

За результатами розрахунків та співставленням відхилень від критеріальних (критичне нижне та верхнє порогове), отримуємо, що ПрАТ “Київстар” відзначається стійкістю цільових результатів безпеки, стан визначається як безпечний. Зональність ризиків та загроз ПрАТ “ВФ Україна” в динаміці за цільовими безпековими орієнтирами за 2018-2022 рр. представлено на рис. 4.39

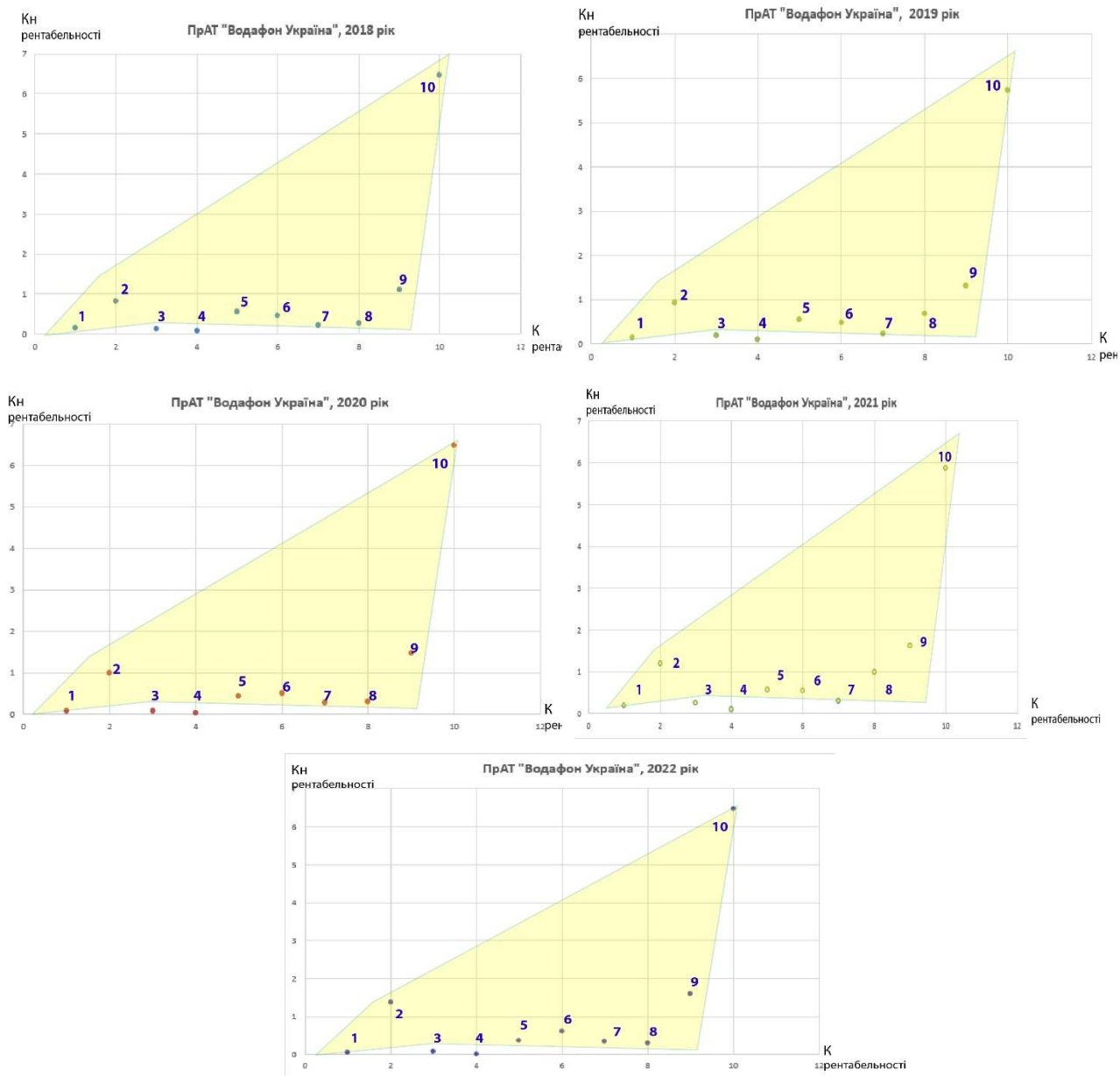


Рис. 4.39. Зональність ризиків та загроз ПрАТ “ВФ Україна” в динаміці за цільовими безпековими орієнтирами (2018-2022 рр.)

(авторська розробка)

Цільові безпекові орієнтири ПрАТ “ВФ Україна” за відхиленнями знаходяться у зоні ризиків, оскільки з’являються дві репелер-точки, які відображаються на зниженні спроможності генерації прибутку за рахунок власного капіталу та ризик втарти спроможності до самофінансування, ризик операційної ефективності компанії. Стан безпеки відзначається, як відносний (порівняно) стан безпеки. Зональність ризиків та загроз ТОВ “Лайфселл” в

динаміці за цільовими безпековими орієнтирами за 2018-2022 рр. проедставлено на рис. 4.40.

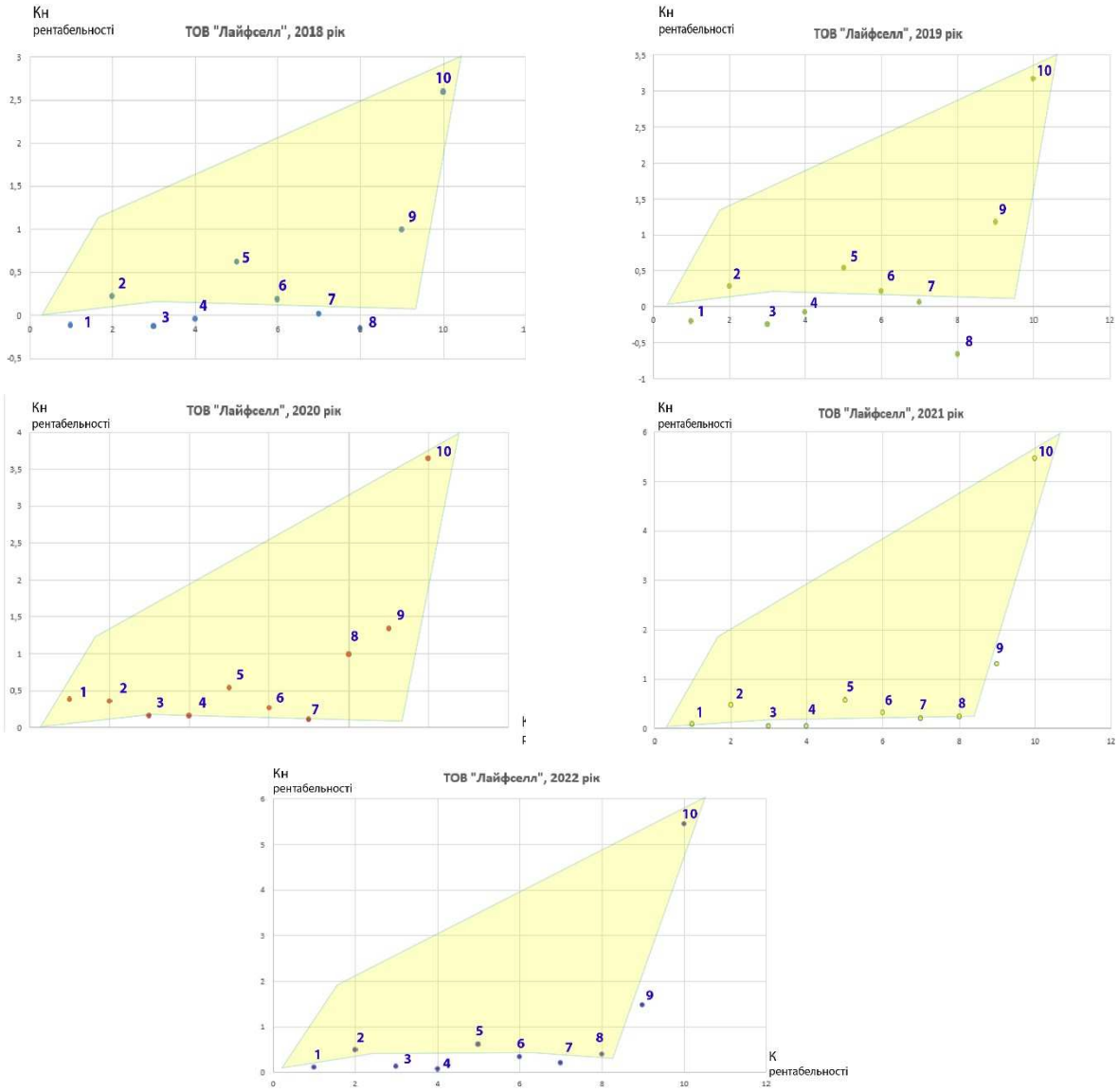


Рис. 4.40. Зональність ризиків та загроз ТОВ “Лайфселл” в динаміці за цільовими безпековими орієнтирами (2018-2022 рр.)

(авторська розробка)

Результати оцінки зон безпеки та небезпеки для ТОВ “Лайфселл” вказує на появу біфуркаційної точки: загроза втрати спроможності генерувати прибуток за рахунок власного капіталу та зростання боргового навантаження, а також на діагностування репелер точкок: ризик втрати генерації прибутку за рахунок активів; ризик зниження ефективності компанії в продукуванні нових послуг по відношенню до конкурентів; ризик нестійкості бізнесу через коливання; зниження

забезпеченості основними засобами та їх використання. Стан безпеки підприємства-постачальника послуг електронних комунікацій визначається, як кризовий стан безпеки. Зональність ризиків та загроз АТ “Укртелеком” в динаміці за цільовими безпековими орієнтирами (2018-2022 рр.) представлено на рис. 4.41.

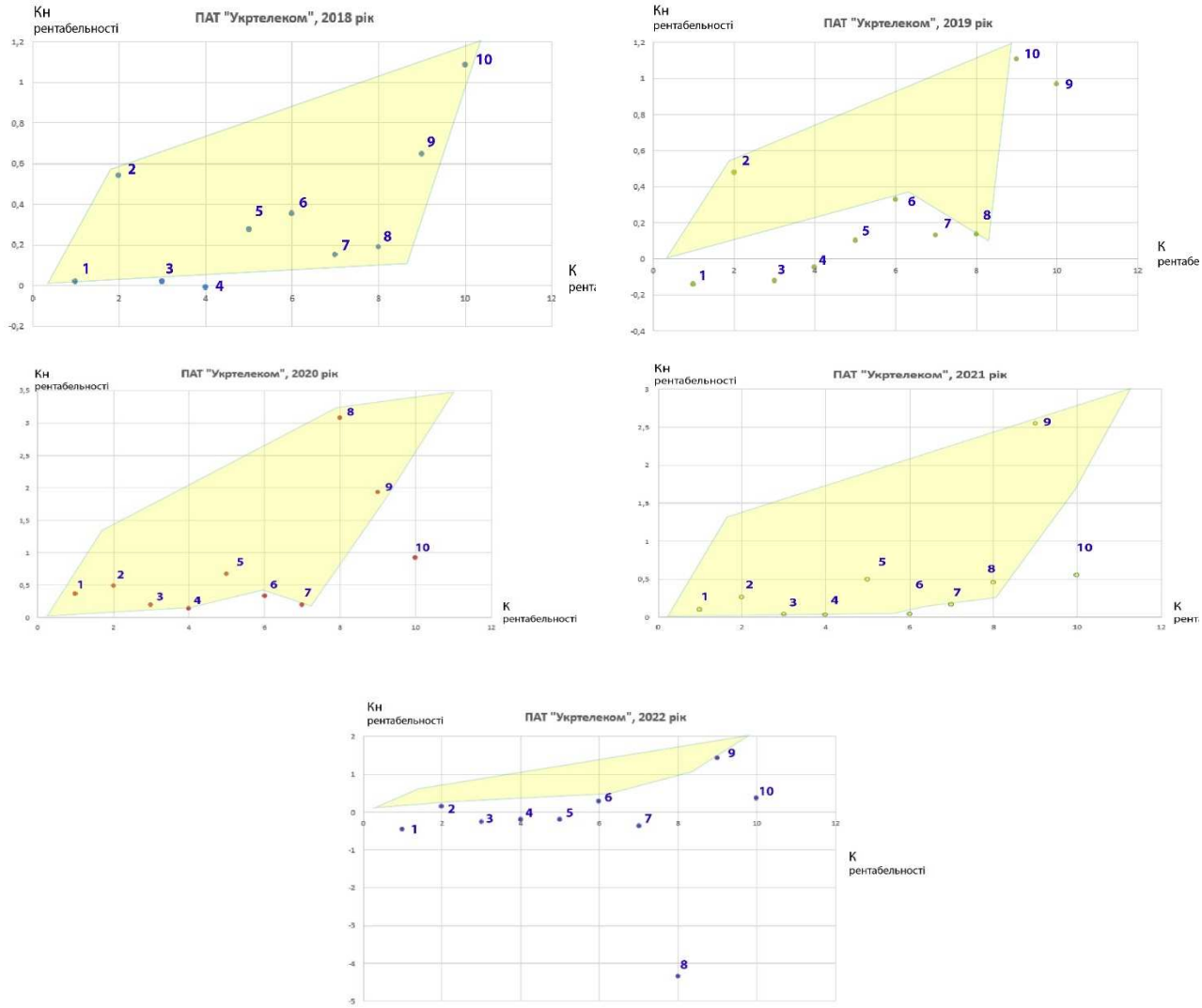


Рис. 4.41. Зональність ризиків та загроз АТ “Укртелеком” в динаміці за цільовими безпековими орієнтирами (2018-2022 рр.)

(авторська розробка)

Моніторинг ризиків та загроз АТ “Укртелеком” вказує на перебування підприємства за цільовими безпековими орієнтирами у зоні небезпеки: біфуркаційні точки: загроза втрати генерації грошовими потоками та втрати фінансової потужності; загроза зниження прибутку, зростання тарифів на послуги, відтік споживачів; загроза втрати генерації прибутку за рахунок

власного капіталу, зростання боргового навантаження; загроза втрати генерації прибутку за рахунок активів; загроза втрати спроможності до самофінансування; загроза зниження спроможності компанії в продукуванні нових товарів та послуг по відношенню до конкурентів; загроза нестійкості; загроза залучення інвестицій та гальмування ровитку; загроза зниження продуктивності інтелектуального капіталу. Також ідентифікується репелер-точка – ризик втрати залучення інвестицій та гальмування розвитку. За відхиленнями та кількістю біфуркаційних точкок підприємство перебуває в зоні критичного стану небезпеки. Зональність ризиків та загроз ПрАТ “Датагруп” в динаміці за цільовими безпековими орієнтирами за досліджуваний період представлено на рис. 4.42.

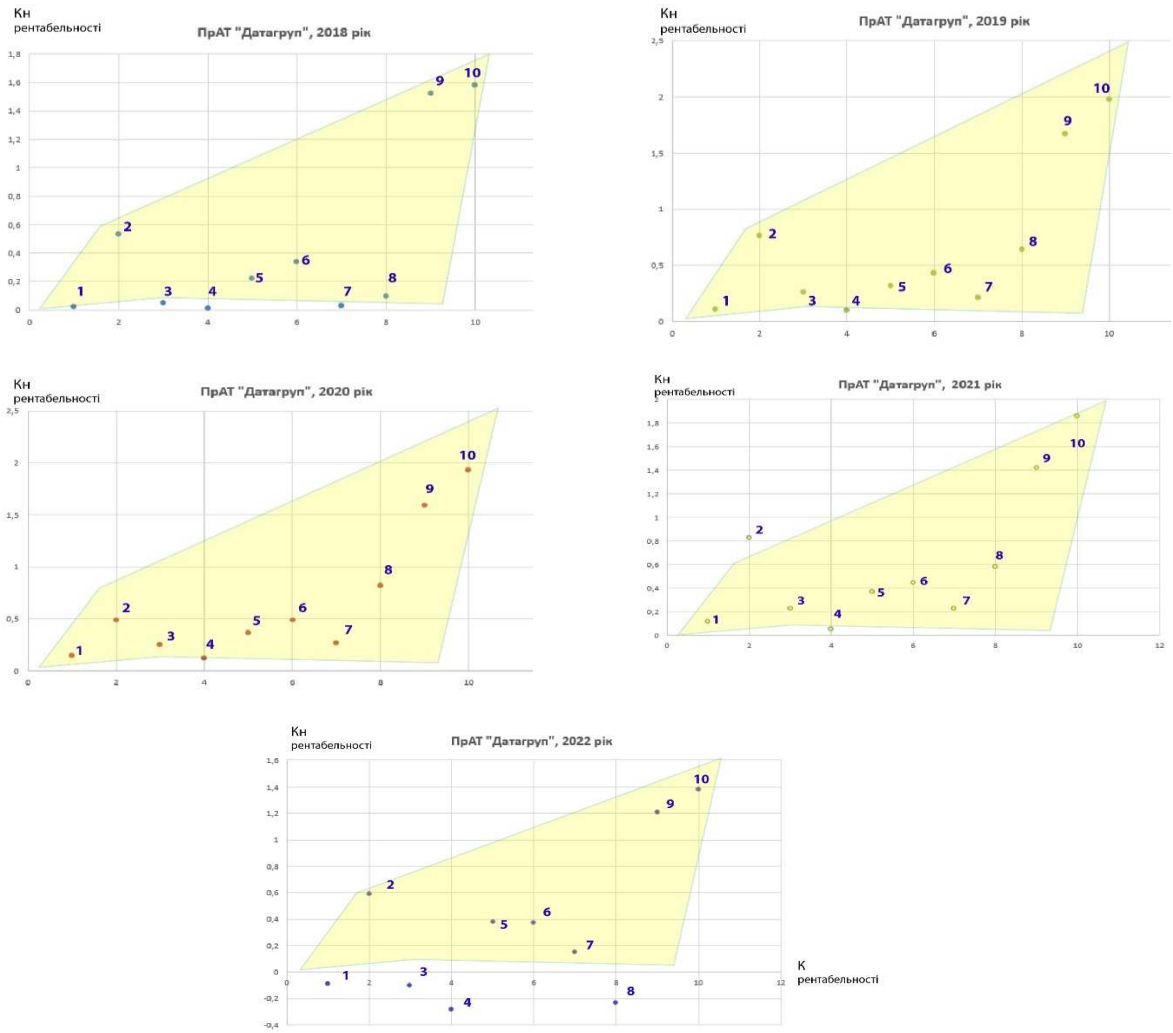


Рис. 4.42. Зональність ризиків та загроз ПрАТ “Датагруп” в динаміці за цільовими безпековими орієнтирами (2018-2022 рр.)

(авторська розробка)

За результатами оцінки цільових безпекових орієнтирів та їх відхилень у ПрАТ "Датагруп" виявлені репелер точоки – ризики втрати генерування прибутку за рахунок власного капіталу; ризик зростання боргового навантаження; ризик втрати генерації прибутку за рахунок активів; ризик зниження ефективності компанії в продукуванні нових товарів та послуг по відношенню до конкурентів; ризик нестійкості (проте тільки у 2022 році), ризик низької забезпеченості основними засобами; ризик зниження продуктивності та мотивованості інтелектуального капіталу. За отриманими даними підприємство перебуває у зоні передкризового стану небезпеки. Узагальнюючи результати оцінки цільових безпекових орієнтирів: прибутковість, платоспроможність, стійкість, конкурентоспроможність, розвиток, отримуємо безпекові точки, за якими ідентифікується стан безпеки або небезпеки підприємства. Ідентифікація безпекової площини (стан безпеки/небезпеки) українських підприємств-постачальників електронних комунікацій за цільовими безпековими орієнтирами представлено у табл. 4.37.

Таблиця 4.37

Ідентифікація безпекової площини (стан безпеки/небезпеки) українських підприємств-постачальників електронних комунікацій за цільовими безпековими орієнтирами

Підприємство-постачальник електронних комунікаційних послуг	Цільові безпекові орієнтири					Рівень ризику/ загрози	Стан безпеки/ небезпеки
	Прибуткovість	Платоспроможність	Стійкість	Конкурентоспроможність	Розвиток		
	Точки безпеки (атрактор)/ небезпеки (репелер, біфуркація)						
ПрАТ "Київстар"	атрактор	атрактор	атрактор	атрактор	атрактор	мінімальний	Безпека (надійний)
ПрАТ "ВФ Україна"	репелер	репелер	атрактор	атрактор	атрактор	незначний	Відносний (порівняно) стан безпеки
ТОВ "Лайфсел"	біфуркація	репелер	репелер	репелер	репелер	середній	Кризовий стан небезпеки
АТ "Укртелеком"	біфуркація	біфуркація	репелер	біфуркація	біфуркація	високий	Критичний стан небезпеки
ПрАТ "Датагруп"	репелер	репелер	атрактор	атрактор	репелер	низький	Передкризовий стан небезпеки

(авторська розробка)

Визначення стану безпеки та небезпеки та ідентифіковані репелер та біфуркаційні точки дозволять сконструювати управління за запропонованим резистентно-ситуаційним підходом до управління безпекою, який схематично предсавлений на рис. 4.43.

Обрання підходу до управління безпекою залежить від результатів оцінки відхилень цільових безпекових орієнтирів від нормативних значень, їх коливання навколо критичних порогових значень дозволило визначити точки небезпек – ризиків та загроз і ідентифікувати площину безпеки та небезпеки, що описує безпековий стан. Так, для компанії ПрАТ "Київстар" доцільним є активний підхід до управління, для компнії ПрАТ "ВФ Україна" – адаптивний підхід, для ТОВ "Лайфселл" – антикризове, для компанії – антикризове із залученням зовнішнього антикризового менеджера-експерта, котрий отримує винагороду, пропорційну приросту прибутку компанії. Пропозиція щодо варіації підходів до управління безпекою у залежності від стійкості підприємства та площини перебування підприємства у межах репелер та біфуркаційних точок, якими ідентифікується стан безпеки, забезпечуватиме рух підприємства у безпекову площину.

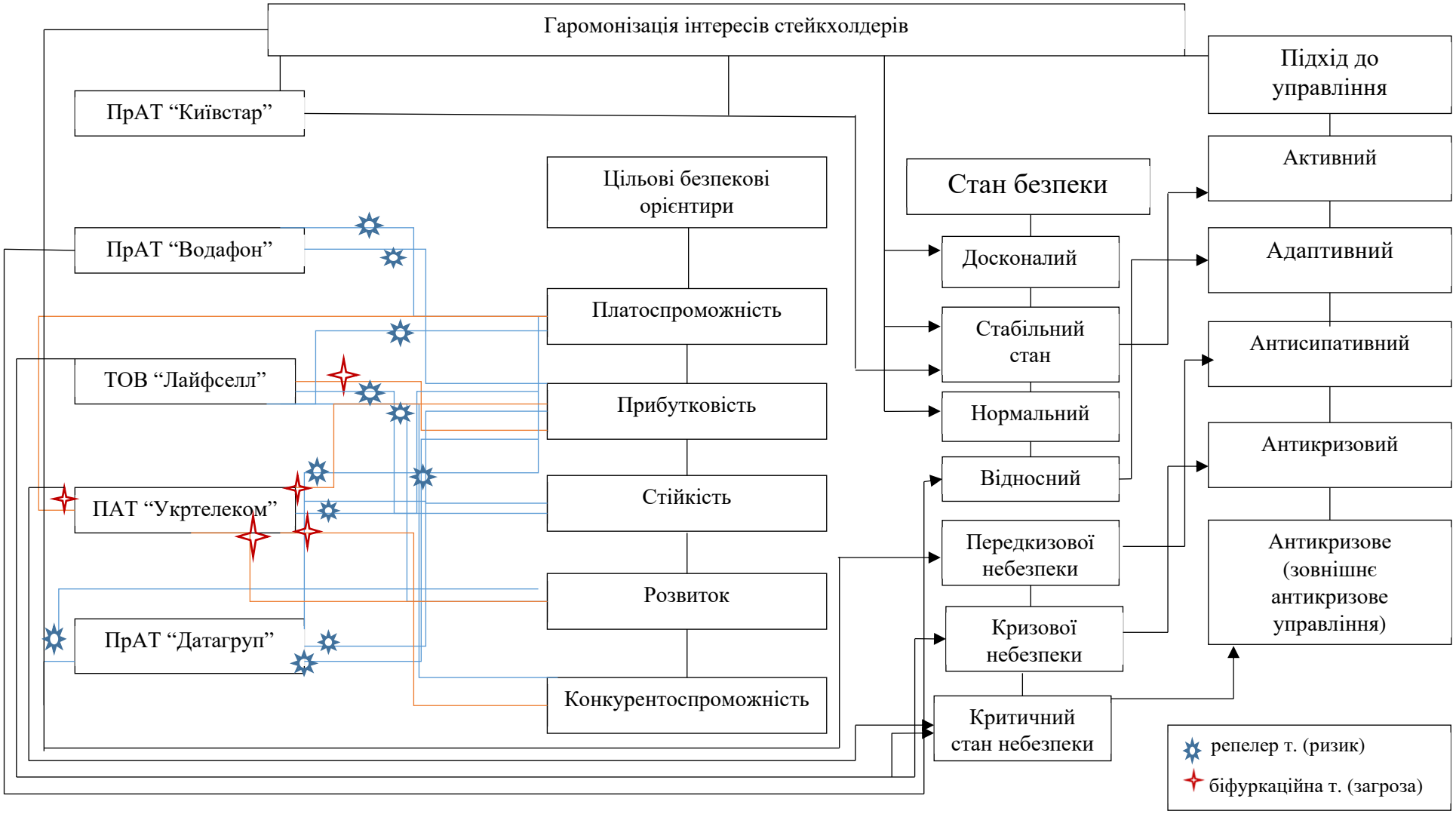


Рис. 4.43. Управління безпекою підприємств-постачальників електронних комунікацій за результатами оцінки цільових безпекових орієнтирів *(авторська розробка)*

Висновки до четвертого розділу

В результаті аналізу стану ринку постачання електронних комунікаційних мереж та послуг визначено затребуваність послуг зв'язку через активну цифровізацію держави надання електронних послуг підприємствам (надання публічних е-послуг, е-ідентифікації, е-декларування через створений портал державних послуг "Дія"). Відзначається потреба у гармонізації стандартів, нормативно-правових актів із країнами Євросоюзу, впродовж останнього десятиріччя активно напрацьовує базис щодо відповідності до законодавчих актів та регуляторних положень у сфері ЕК, проаналізовано основні інституційні зміни щодо впровадження цифрових інновацій та розширення переліку надання е-послуг. Відмічено, що наразі буквені коди видів діяльності в сефрі ЕК гармонізуються із міжнародними. Зросла кількість суб'єктів господарювання з надання електронних комунікаційних мереж та послуг, майже у 2 рази у 2023 році по відношенню до 2022 року, що вказує на сприятливі умови функціонування, що надані державою та вказує на конкуренцію на ринку.

У результаті аналізу динаміки доходів зв'язку, з'ясовано їх приріс по відношенню до 2022 року, темп росту доходів від надання електронних комунікаційних послуг за 2023 рік по відношенню до попереднього року становив 116,95%, найбільша частка доходів припадає на мобільний зв'язок.

Відзначено, що існує потреба у використанні технології PON для забезпечення безперебійного надання послуг та безпечного функціонування підприємств та організацій в умовах воєнного стану, розглянуто існуючі технології з подальшим аналізом їх використання постачальниками послуг Інтернет в Україні (у структура фіксованого доступу до Інтернет у розрізі частка підключень становила за технологіями FTTx (46,8%) та xPON (41,3%)).

Виявлено, що за даними світового рейтингу тестування швидкості Інтернет Speed Test Global Index Україна посідає 88 місце за швидкістю мобільного Інтернету та відповідно 76 за фіксованим широкосмуговим

доступом до глобальної мережі, що вказує на потребу удосконалення технологій надання послуги.

Аналізуючи частки постачальників послуг на ринку виокремлюється трійка: ПрАТ “Київстар” ПрАТ “ВФ Україна”, ТОВ “Лайфселл”, долі яких складають 34%, 21% та 12% відповідно, а разом на них припадає 67% обсягів доходів у секторі електронних комунікацій, крім того послуга 4 та 4,5G (LTE Advanced) цими ж надається трьома постачальниками послуг зв’язку

За розрахованими метриками безпеки підприємств, підсумовано, що ПрАТ “ВФ Україна” знаходиться на межі втрати здатності генерувати грошовий потік та втрати фінансової потужності, АТ “Укртелеком” та ПрАТ “Датагруп” перебувають в зоні загроз, подолавши критичну точку біфуркації, в зоні ризику перебуває ПрАТ “ВФ Україна”. Загрози втрати генерації прибутку (за рахунок власного капіталу, а також активів) та зростання боргового навантаження відзначаються у ПрАТ “ВФ Україна”, ТОВ “Лайфселл”, АТ “Укртелеком”, ПрАТ “Датагруп”. Загроза втрати спроможності до самофінансування, інвестиційної привабливості, зниження операційної ефективності наявна у компанії АТ “Укртелеком”; загрози втрати конкурентоспроможності через зниження ефективності компанії в продукуванні нових товарів, послуг по відношенню до конкурентів відзначаються у компанії ТОВ “Лайфселл”, ТОВ “Укртелеком”, ПрАТ “Датагруп”; ризик нестійкості бізнесу характерний для ТОВ “Лайфселл” та ПрАТ “Датагруп”, під загрозою АТ “Укртелеком”; загроза втрати ефективності інвестицій та ризик гальмування розвитку в АТ “Укртелеком” та ПрАТ “Датагруп”; ризик зниження продуктивності та мотивації персоналу прослідковується в ПрАТ “Датагруп”, загроза в АТ “Укртелеком”.

Відзначено потребу у відображенні безпекової площини функціонування підприємств для формування резистентності кожного окремого підприємства в динаміці для пошуку підходу до прийняття ризиків або підходу до управління безпекою підприємства у разі його високої чутливості до умов функціонування

Аргументовано доцільність побудови безпекових площин із формуванням

станів безпеки підприємства, для визначення станів безпеки (небезпеки), зважаючи на здатність повернення підприємства у висхідний стан безпеки, або ж навпаки його віддалення та зміни через відхилення від точки (атрактора) нормативних значень за межі допустимих (критичного нижнього). Побудовано модель управління безпекою підприємств-постачальників електронних комунікаційних послуг з визначенням безпекових відхилень у безпеко-небезпечній площині дотичності репелерних точок впливу ризиків і біфуркаційних точок дії загроз та вибором відповідного підходу до управління безпекою підприємства для досяжності цільових показників діяльності.

Доведено, що змодельовані відхилення площин безпеки дозволяють диференціювати підходи до управління безпекою підприємства з урахуванням втрат (відхилень) від цільових метрик безпеки (результатів).

Основні ідеї та наукові положення, презентовані у даному розділі, викладені у піблікаціях та працях [232; 259; 322; 324; 327; 328; 329; 344; 358; 366; 367; 368; 371]

РОЗДІЛ 5
УПРАВЛІННЯ БЕЗПЕКОЮ ПІДПРИЄМСТВА ЗА УМОВ НЕВИЗНАЧЕНОСТІ

5.1. Виклики управління безпекою підприємства за невизначених умов

Виклики сьогочасності загально охоплюють функціонуючі економічні одиниці в країні, окрім того зачіпають питання базових безпекових потреб суспільства через руйнування країною-агресором критично важливої інфрастуктури, тим самим ускладнюючи доступ до суспільних благ та установ.

Безпечне функціонування господарюючих суб'єктів в умовах невизначеності, що нині склалися, забезпечення стабільної роботи критично важливої інфраструктури (з можливістю підтримки об'єктів, робота яких від неї залежить), до якої відноситься сфера електронних комунікацій, досягатиметься за адаптації підприємств до викликів та дієвого управління безпекою

З причин невизначеності умов (починаючи із часів пандемії) безпека у інформаційно-комунікаційному просторі набуває особливої значимості, світовими організаціями проводяться дослідження та наводяться статистичні дані безпечності роботи у глобальній мережі. Світовий банк проводив аналіз у розрізі країн світу щодо безпечності інтернет-серверів, за результатами якого найбільш безпечними вважаються сервери Сполучених Штатів Америки – 46678110 серверів на 1 млн осіб, потім Німеччини – 8109646 серверів на 1 млн осіб, далі Великої Британії – 2445275 серверів на 1 млн осіб. Щодо України показник відчутно нижчий – 395092 сервери на 1 млн осіб (*The World Bank*, 2020) [347].

Зрозуміло, що розвиток та поширення технологій, інфокомунікацій, мережі Інтернет, використання техніки у досліджуваних високорозвинених країнах відбувалися швидшими темпами, ніж у країнах, що розвиваються. Крім того, з активним використанням глобальної мережі та інтернет-технологій у

досліджуваних країнах (що займають лідируючи позиції щодо захисту серверів) з'являлися нові послуги ЕК, тому й питання захисту та безпеки в інфокомунікаційному просторі ставилися раніше, одночасно із початком наданням таких послуг. Саме тому рівень захисту та безпеки в цих країнах у цифровому просторі значно вищий.

Останнім часом увага держави, суспільства, підприємств концентрується на безпеці, її гарантуванні у всіх сферах. Розглядається низка питань стосовно упередження загроз, усунення ризиків задля безпечного функціонування господарюючих суб'єктів на мікро- та макрорівні. Наразі набирає обертів геополітична напруга, загострюються конфлікти, виникає дедалі більше інцидентів порушення цілісності даних в інформаційному полі, дестабілізується робота об'єктів критичної інфраструктури. Тому наріжним питанням є вчасне виявлення загроз, оцінка ризиків, які загрожують безпеці, планування заходів щодо упередження та усунення наслідків загроз в умовах невизначеності, а інколи в агресивному зовнішньому оточенні, що заплановано та активно дестабілізує функціонування господарюючих суб'єктів.

Гарантування економічної безпеки залишається актуальним питанням для підприємств впродовж їх життєвого циклу. Низка викликів сучасності продукує зростання вартості матеріально-технічних ресурсів, дефіциту робочої сили, енергетичних та виробничих проблем, які потребують виваженого та стратегічного підходу до управління ризиками на підприємствах [359]. Учений Охріменко І.В., вважає, що розв'язання проблем має ґрунтуватися на: запровадженні ефективних заходів, таких як: диверсифікація постачальників, використання фінансових інструментів для захисту від коливань валютного курсу та активне вивчення податкового законодавства, як ключових елементах стратегії [345].

Впродовж останніх чотирьох років відбувся активний перехід до віддаленої роботи, розширення технологічних меж з активним використанням хмарних технологій та обчислень, налагодження комунікації через соціальні мережі та канали, використання цифрових додатків. Бізнес перейшов у нову

площину – цифрову, причому кожний окремий етап взаємодії із клієнтом або партнером для її ефективності вимагає різних цифрових інструментів [365].

Зрозуміло, що перехід у цифровий простір породжує для господарюючого суб'єкта низку нових, до цього невідомих викликів. Підлягають ризику бази даних, інформація щодо клієнтів, конференційна інформація, результати та розробки, інформація щодо винаходів, інтелектуальної власності компаній у новій та складній, динамічній мережі комунікації із зовнішнім оточенням. Крім того, виникають нові типи атак, які важко ідентифікувати, через що підприємства стають до них більш вразливими, тож виникає потреба розширити перелік загроз із подальшим моніторингом їх впливу та наслідків, пошуку шляхів їх нейтралізації.

За результатами опитування респондентів, яке проводилося Міжнародним економічним форумом (World Economic Forum), важливість питання захисту цілісності даних та інформаційного простору організацій підтверджується (табл. 5.1).

Таблиця 5.1

Критичні загрози для світу в найближчі 10 років

0–2 роки		2–5 років		5–10 років	
Критичні загрози	*% опитуваних*	Критичні загрози	*% опитуваних*	Критичні загрози	*% опитуваних*
Екстремальні погодні умови	31,1	Невдачі у боротьбі зі зміною клімату	35,7	Невдачі у боротьбі зі зміною клімату	42,1
Криза джерел до існування	30,4	Екстремальні погодні умови	34,6	Екстремальні погодні умови	32,4
Невдачі у боротьбі зі зміною клімату	27,5	Руйнування соціальної згуртованості	23,0	Зменшення біорізноманіття	27,0
Руйнування соціальної згуртованості	27,5	Криза джерел до існування	20,1	Кризи природних ресурсів	23,0
Інфекційні захворювання	26,4	Боргові кризи	19,0	Екологічна шкода, завдана людиною довкіллю	21,7

продовження табл. 5.1

Погіршення психічного здоров'я	26,1	Екологічна шкода, завдана людиною довкіллю	164	Руйнування соціальної згуртованості	191
Порушення кібербезпеки	195	Геоекономічні конфлікти	14,8	Вимушена міграція	15,0
Боргові кризи	19,3	Порушення кібербезпеки	14,6	Негативний технологічний прогрес	14,9
Цифровий розрив	18,2	Зменшення біорізноманіття	13,5	Геоекономічні конфлікти	14,1
Крах “бульбашкових” активів	14,2	Крах “бульбашкових” активів	12,7	Геополітична боротьба за ресурси	13,5

(складено автором за [346])

Більшість із згаданих вище ризиків – глобальні, виникли у результаті діяльності суспільства та пов’язані з екологічними змінами, тобто вважаються для господарюючих суб’єктів екзогенними, на які підприємство впливає лише частково. Серед згаданих ризиків є такі, що виникли в результаті невизначеностей, на які підприємство вплинути не спроможне, а лише може адаптуватися до змін внаслідок їх дії. Так, зрушення, що пов’язані із діджиталізацією та інформатизацією світу, призвели до проблеми з інформаційною безпекою та потреби включення кібербезпеки до складових, що мають враховуватися при забезпеченні безпеки діяльності економічних одиниць, підприємств, суспільства, організацій, державних об’єктів упродовж наступних п’яти років. Зростання зовнішнього та внутрішнього боргу країн спонукає до проведення аналізу безпекової ситуації щодо боргового навантаженя при обранні джерел залучення додаткових фінансових ресурсів [362].

За даними глобального дослідження “Future risk report 2022”, що проводиться щороку компанією AXA спільно з науково-дослідним інститутом IPSOS та за консультування Eurasia Group (напрям дослідження – геополітичний аналіз), в якому прийняли участь 4,5 тис. експертів з понад 50 країн, а також близько 20 тис. респондентів, обраних серед населення, можна

відзначити ризики, що загрожують світу [346]. Серед найбільших викликів, що загрожуватимуть безпеці впродовж наступного десятиліття, відзначаються: зміни клімату, геополітична напруженість, ризики кібербезпеки, а також енергетичні ризики.

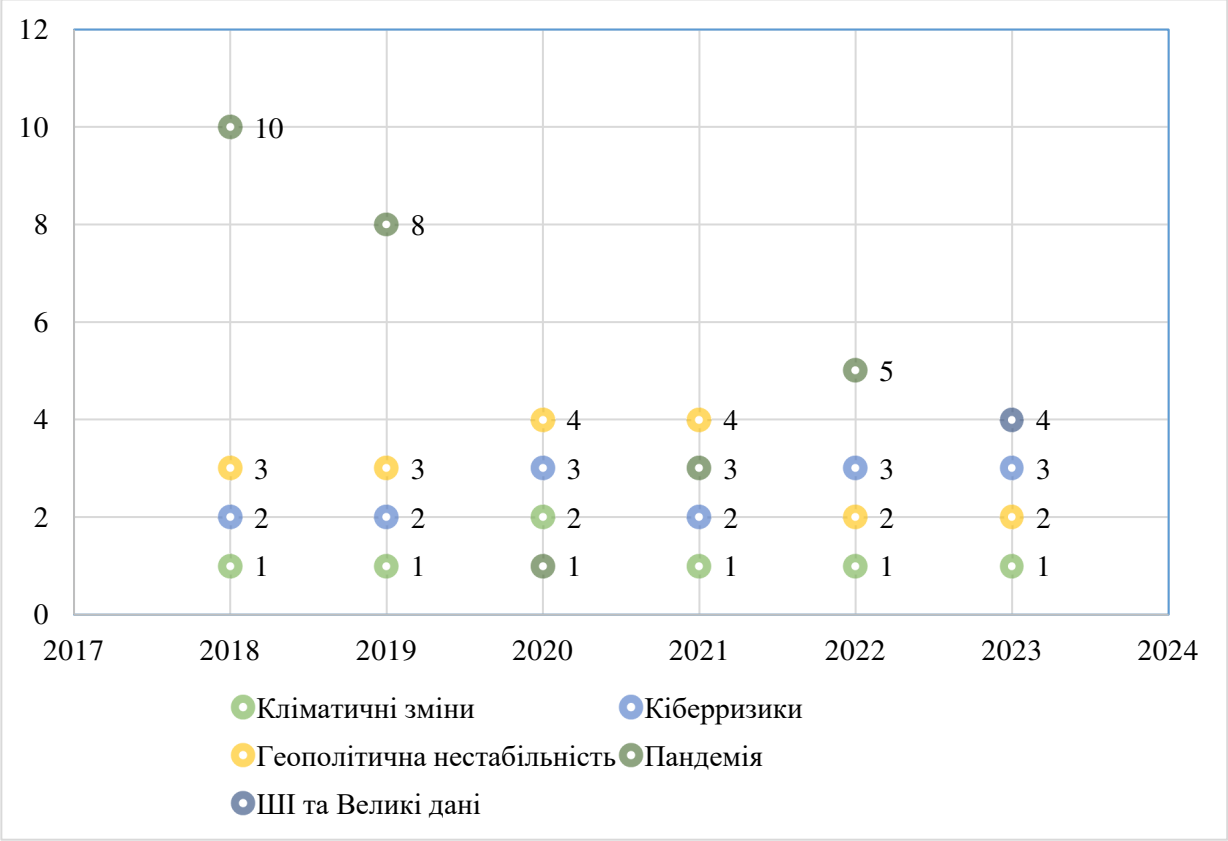


Рис. 5.1. Ранги глобальних викликів впродовж 2017-2023 рр.

(складено автором з [346])

Слід зазначити, що за даними AXA впродовж 2023 року екстремальні погодні явища, посухи, пожежі, втрата біорізноманіття, процеси руйнації екології від зміни клімату підкреслили вагу проблеми та вважаються найвищим ризиком для населення при чому у всіх регіонах дослідження.

Кіберризики залишаються у трійці загроз, починаючи із 2018 року. Цифрові трансформації та їх вплив на наш спосіб життя сприяє використанню інформації проти населення, держав, уряду, окрім того, тісно переплітається з геополітичними риками, посідаючи третє місце.

Відзначається стрімким зростанням ризик від використання штучного інтелекту (ШІ) та великих даних, вони одразу перейшли з 14 місця на 4 місце у 2023 році Вони підскочили з 14-го на 4-е місце в рейтингу експертів – це не дивно. Проте генеративний ШІ та ChatGPT за думкою громадськості не є ризиковими, у першу чергу у Європі, що можна сприйняти як вектор-виклик прогресу.

Неурядова організація Інститут кібермиру (Cyber Peace Institute) слідкує за кіберстаном у світі, за їх даними також підтверджуються прогнози аналітиків, експертів і громадськості, щодо посилення загроз у інформаційному просторі, відзначається стрімке зростання кібератак із початку війни в Україні. Окрім урядових організацій, підвищений інтерес кібернападників становлять підприємства сфери ЕК, так у грудні 2022 року відбулася атака проти серверів української компанії, яка тривала три дні. За даними звітів Інституту про безпекову ситуацію в Україні, відзначається активність у фінансовій сфері, торгівлі, енергетиці, медіа, виробництві, ІКТ [349; 350]

За перший квартал 2023 року відбулося 10 інцидентів націлених на сектор інформаційно-комунікаційних технологій. Продовжувалися атаки на фінансовий сектор (приріст на 46%), державне управління (рис. 5.2).

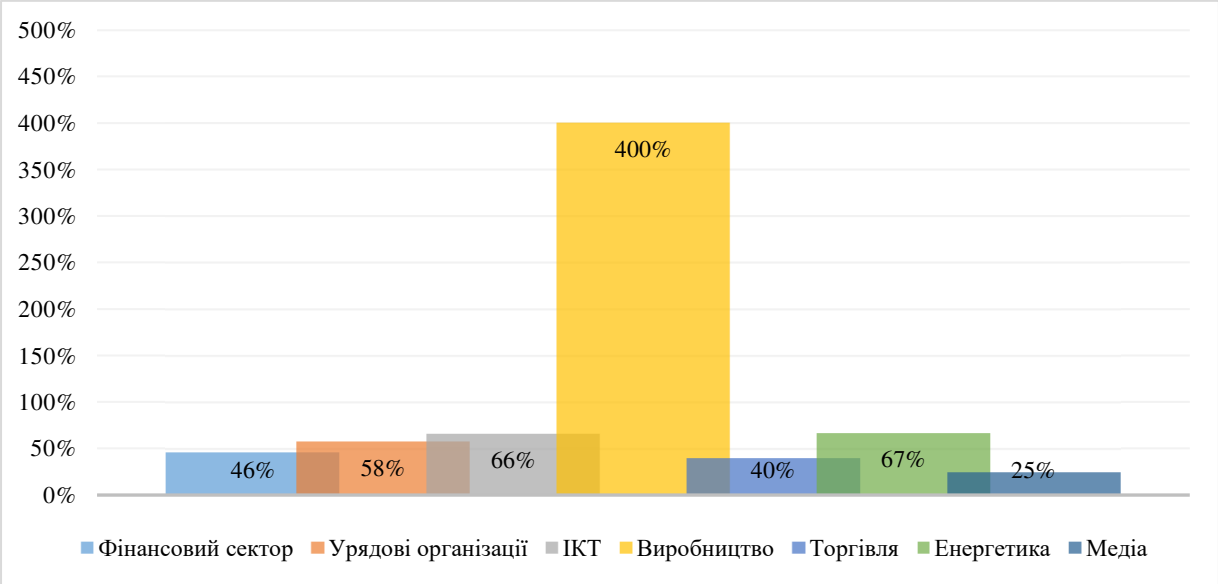


Рис. 5.2. Приріст кіберінцидентів за секторами (I кв. 2023 р.)

(складено автором за [350])

Цьогоріч світ перебуває у багатоспектральній кризі, що проєцюється наслідками війни в різних країнах світу, які відчувають вплив на економіку, політику, торгівлю та інтеграційні процеси. Окрім того посилюється цифрова трансформація, глобальне потепління та геополітична напруга, тому розуміння безпеки та її роль безпеки посилюється та отримує нову парадигму її сприйняття. Геополітиці, кліматичним змінам, пандемії властивий зовнішній характер, дані виклики не піддаються управлінню з боку господарюючих суб'єктів, їх варто враховувати, стартегічно планувати їх упередження. Кібербезпека, штучний інтелект, великі дані спродуковані науково-технічним прогресом, цифровізацією, тісно пов'язані із сферою електронних комунікацій та підприємствами зв'язку, є внутрішніми та регульованими.

Спостерігається зростанням кібератак, проаналізувавши кількість атак за даними Significant Cyber Incidents упродовж 2021 та 2022 рр., отримано, що по всьому світу атаки посилюються, крім того, кіберінциденти поширювались навіть на урядові, оборонні, високотехнологічні компаній країн із високим ступенем кіберзахисту (табл. 5.2).

Таблиця 5.2

Кіберінциденти на урядові, оборонні, високотехнологічні компанії (із збитками понад 1 млрд дол) у 2021-2022 рр.

Рік	Країна походження кіберінциденту / Країна, у якій відбувався кіберінцидент	Підприємства та організації, що зазнавали атак, опис інциденту
2021	Іран / Нідерланди	У лютому 2021 року злом амстердамських серверів, що використовувалися як командно-контрольний центр для подальших атак на політичних опонентів у Нідерландах, Німеччині, Швеції, Індії.
	РФ / Україна	Поширення шкідливих документів, які могли б встановити на комп'ютери шкідливе програмне забезпечення. Атака націлена на знищення інформаційних ресурсів системи електронної взаємодії органів виконавчої влади.
	Китай / Індія	Кампанія кібершпигунства (фішинг, використання відомих вразливостей в загальнодоступних програмах як початковий режим входу для компрометації корпоративної мережі) проти індійського транспортного сектору (IRCTC, Tata Motors, Національне управління автомобільних доріг Індії, RITES, Dedicated Freight Corridor Corporation of India, Center for Railway Information Systems (CRIS) і Roads & Building Dept, Андхра-Прадеш)

продовження таблиці 5.2

	РФ → Польща	Нетривале захоплення веб-сайтів Національного агентства з атомної енергії та Міністерства охорони здоров'я Польщі, щоб поширити неправдиві повідомлення про неіснуючу радіоактивну загрозу.
	Китай → Афганістан	Фішингові листи з метою отримання доступу до облікового запису електронної пошти одного із чиновників для надсилання представникам національної безпеки підробного електронниго листа із інструкцією дій щодо майбутньої прес-конференції.
	Північна Корея → Південна Корея	Кібератака на південнокорейський державний Науково-дослідний інститут атомної енергії (KAERI) сталася через вразливість у VPN постачальника (тринадцять несанкціонованих IP-адрес отримали доступ до внутрішньої мережі KAERI).
	РФ → Австралія	Атака на австралійську комунальну компанію CS Energy з використанням програмного забезпечення з вимогою викупу.
	Іран → США	Атаковано акаунти у Facebook через надсилання зараженого шкідливого програмного забезпечення, файлів або обманом змушували жертв (американських військовослужбовців) вводити конфіденційні облікові дані на фішингових сайтах.
	США → Китай	Численні кібератаки на Північно-Західний політехнічний університет Китаю з боку Агентства національної безпеки, викрадання даних користувачів і проникнення в цифрові комунікаційні мережі.
2022	Китай → Фінляндія	DDoS-атака на парламент Фінляндії, яка зробила веб-сайт парламенту недоступним.
	Індійські → Пакистан	Атака на ВПС Пакистану (PAF) у кампанії підводного полювання з метою розгортання шкідливого програмного забезпечення та отримання конфіденційних файлів.
	Російські хакери → Норвегія	Атака на державні установи Норвегії за допомогою DDoS-атак, порушуючи роботу державних веб-сайтів.
	Китайські → Німеччина	Китайська хакерська група зламала кілька німецьких фармацевтичних і технологічних компаній (спроба викрадення інтелектуальної власності).
	Іран → Ізраїль	Хакери атакували муніципальні системи оповіщення в Єрусалимі та Еліаті, увімкнувши сирени повітряної тривоги в обох містах. Ізраїльська компанія з промислової кібербезпеки приписала атаку Ірану.

(складено автором за [354; 356; 392])

Аналізуючи дані по кіберінцидентам, приходимо до висновку, що атаки були націлені насамперед на підприємства та організації, які відносять або до критично важливих, або урядових. Найбільше нападів чинилася із боку сусіда країни-агресора, Ірану, Китаю, нанесені збитки вимірювалися в млн та млрд дол. США. Зважаючи на рівень організацій (урядові, оборонні та високотехнологічні), на які були спрямовані атаки, їх можливості щодо захисту від кіберзагроз, постає питання щодо посилення захисту інформаційного середовища усіма підприємствами задля уникнення фінансових втрат та

уникнення репутаційних ризиків щодо діяльності та надійності підприємства. Лише стійкі до зовнішніх впливів підприємства, які працюють на упередження здатні функціонувати в умовах невизначеності, відбивати атаки, в тому числі кібератаки, тим самим посилюючи довіру з боку клієнтів та збільшуючи вартість компанії, що позитивно сприймається стейкхолдерами [395].

У бізнес-середовищі спостерігається стабільна тенденція до переходу роботи підприємств у режим віддаленого доступу, у цілях безпеки підприємства тяжіють до забезпечення належних умов і приділяють увагу захисту персоналу та підприємств від ризиків, що виникають у процесі виконання своєї операційної діяльності. Проте, через воєнні дії ускладнюється пряма комунікація (фізична), збільшуються ланцюги постачання послуг, так як намагаються якнайшвидше та безпечніше передавати інформацію, використовувати її з максимальною можливою швидкістю по перевіреним каналам. Із метою пришвидшення комунікації та територіального охоплення споживачів, постачальників, посередників підприємства використовують хмари та хмарні сервіси. Таким чином уможливлюється відкриття інтернет-магазинів, спільне використання баз даних, управління підприємством, використання поштових серверів. Хмара слугує віртуальною IT-інфраструктурою підприємства, в якій можна розгорнути будь-які системи та програми.

Ogрунтовано висвітлена проблема потреби у використанні хмарних сервісів науковцями І. Шевчук та Б. Депутат, відзначено, що питання гостро постало для підприємницьких структур, починаючи з 2014 року через анексію територій Донбасу та Криму. Підприємці були вимушені рятувати власний бізнес та переїжджати на більш безпечні території, ними використовувалися хмарні сервіси для продовження роботи, тому що створення власних було занадто витратним [351].

К. Нікітенко, А. Осадчий підкреслили переваги використання хмар, такі як: безперешкодний доступ до даних з будь-якої точки за наявності Інтернету; зменшення витрат на утримання (відсутність потреби у купівлі обладнання,

програмного забезпечення, а також обслуговування); можливість використання не залежно від місця розташування підприємства; високотехнологічність. Однак, одночасно із перевагами вказані недоліки, що у першу чергу, пов'язані із безпекою даних, збереженістю даних, які забезпечуються надавачем хмарних послуг [352].

Вчені С. Михайловина, О. Матрос, О. Поліщук розглядають позитивні сторони від використання SaaS (Software as a Service): фіксована абонплата; реалізація потреб у віддаленому доступі та виконанні завдань; низька потреба у технічних засобах та пристроях; ліцензоване програмне забезпечення; постійне оновлення та техпітримка на безоплатній основі. Водночас наголошено і на потребах, які здебільшого стосуються безпеки даних – побудова власної приватної хмари у разі засекречених даних; резервне копіювання даних з метою збереження цілісності даних та уникнення їх втрати [353].

Наковці М. Дауд, Ш. Ту, Ч. Сяо, Х. Аласмарі, М. Вакас, С. Ур Рехман вважають, що у світі хмарних обчислень безпека даних і ресурсів є головним пріоритетом, хмарна безпека непокоїть організації, бізнес, науково-дослідницький сектор, але доволі часто виникає супротив та протиріччя щодо розміщення та повного використання хмарних обчислень із міркувань безпеки даних [354].

На думку С. Чоудхурі, Н. Рей, С. Дана, Д. Марвана, зловмисники можуть атакувати постачальників онлайн-сховищ, оскільки захищені норми реєстрації дозволяють хакерам залишатися анонімними, що ускладнює їх виявлення. Можливості управління та забезпечення конфіденційності є затратними в хмарі, підприємства готові нести ці витрати задля безпеки даних, проте все одно існує високий ризик відслідковування та викрадення даних через неналежну безпечність інтернет-середовища [418]. Тому питання безпеки даних у хмарному середовищі та аналізу загроз підприємства залишаються відкритими, потребують подальших досліджень за невизначених умов функціонування господарюючих суб'єктів.

Із активним переходом підприємств з часів пандемії у віртуальну ІТ-інфраструктуру, одночасно зростають загрози цілісності даних та з’являється потреба у додаткових засобах їх захисту, тобто, із переходом у хмарне середовище, використанням хмарних сервісів, посилюються кібератаки на масиви даних у хмарах.

Питання безпеки хмарних послуг окреслено у Законі України “Про хмарні послуги”, в якому чітко визначено потребу у дотриманні заходів щодо безпеки, які “…мають забезпечувати рівень безпеки електронної комунікаційної мережі, електронної комунікаційної послуги та інформаційних систем, які використовуються для надання хмарних послуг, що відповідає ризику, який виник, та враховувати такі елементи: безпеку систем та устаткування; врегулювання інцидентів; управління безперервністю бізнесу; моніторинг, аудит та випробування; відповідність міжнародним стандартам” [355].

Критична інфраструктура залишається у полі зору кібернападників, в тому числі й підприємства ПЕКМП, які забезпечують комунікацію, зв’язок, включаючи компанії-розробники програмного забезпечення, серверів. Відзначається інтенсивність атак впродовж 2023 року, при чому їх посилення відбулося, починаючи із літа. Здійснена низка DDoS-атак на сайти українських компаній-постачальників послуг ЕК, сервери, розробників веб-платформ (рис. 5.3).

За даними спеціалізованого структурного підрозділу CERT-UA (Computer Emergency Response Team of Ukraine) Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, починаючи з травня по вересень 2023 року зафіксовано втручання в роботу 11 українських постачальників електронних комунікацій, а саме в інформаційно-комунікаційні системи, що призвело до збоїв надання послуг.

Використовуючи раніше скомпрометовані системи, зловмисник зміг сканувати мережі на наявність відкритих портів і отримати доступ до дистанційного керування.

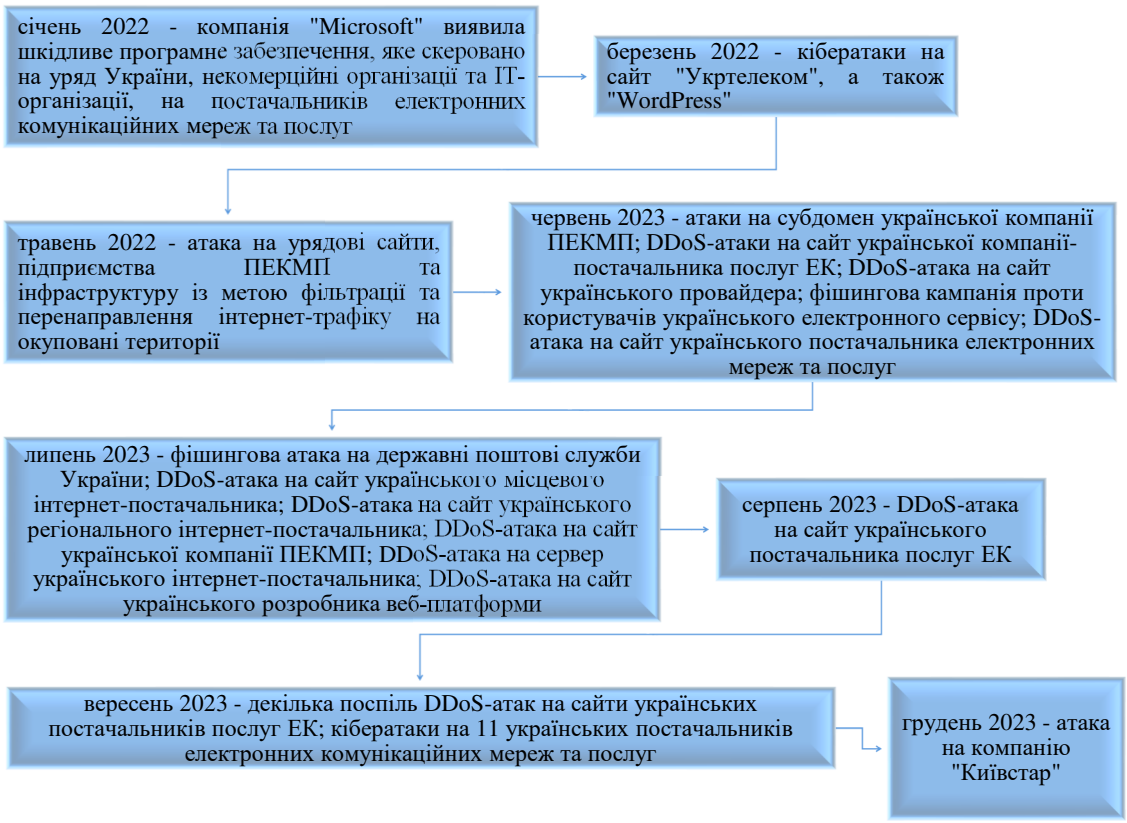


Рис. 5.3. Масовані кібератаки на українські підприємства та організації ІТ-сфери впродовж 2022-2023 рр.

(складено автором за [374; 375; 376])

Потрапивши всередину, зловмисник зміг отримати віддалений доступ та втручатися в роботу інформаційно-комунікаційних систем 11 постачальників послуг ЕК України, вивівши з ладу активне мережеве та серверне обладнання, а також системи зберігання даних, що призвело до перебоїв у наданні послуг споживачам.

Тож, підсумовуючи, за результатами аналізу загроз підприємству отримано, що експерти з різних країн світу (94 %) вважають, що найближчим часом геополітична напруга зростатиме, крім того, всі дійшли згоди щодо взаємопосилення: зміни клімату, геополітичної нестабільності та енергетичних ризиків, які стали відчутними через вторгнення сусіда-агресора в Україну. Крім того, відзначено, що роль високотехнологічних компаній зросла, користь від їх рішень щодо інформаційної та кібербезпеки більша, ніж від урядових (компанія Microsoft відслідкувала російську кіберактивність на початку війни, технології

Starlink уможливили забезпечення зв’язку на території нашої країни, а головне – на територіях, де велися активні бойові дії). Підкреслюється важливість питань безпеки підприємств у хмарному середовищі та посилення кіберзагроз за функціонування їх в умовах невизначеності.

Кіберризики впродовж п’яти років залишаються в полі зору аналітиків та експертів, оскільки технології використовуються усюди, нагальним є питання життєво важливих сфер: медицина, оборона, фінанси, електронні комунікації, енергетика, освіта.

Наріжним залишається питанням захисту критичної інфраструктури та послуг, які надаються підприємствами, що до неї належать (вважає 51% експертів), кіберризики зростають й стабільно утримуються у трійці найбільш загрозливих не лише для організацій, підприємств, а й для людства.

В результаті проведеного аналізу загроз, які пов’язані з активізацією використання хмарних технологій та сервісів за невизначених умов, підтверджено, що виникає серйозна проблема, оскільки дані стають більш вразливими до загроз, виникають порушення інформаційної та кібернетичної безпеки організацій.

Викликом для України був фінансовий стрес, який країна пережила на початку повномасштабного вторгнення, індекс становив 0,8, проте станом на кінець травня стабілізувався до рівня 0,1535, що засвідчує спроможність залучати інвесторів для розвитку сфери електронних мереж та комунікацій, рідаочастотного спектру та поштового зв’язку.

Індекс фінансового стресу (ІФС) визначається Національним банком України, є індикатором, що відображає рівень напруги у фінансовому секторі України (становить від 0 (відсутність стресу) до 1 (найвищий рівень стресу)) [376]. Через суттєві коливання валютних курсів, інфляційні процеси, зростання боргового навантаження та економічної нестабільності для вирівнювання фінансового стресу, аналізуючи спроможності та потенціал до залучення коштів державою та управління державним боргом [373].

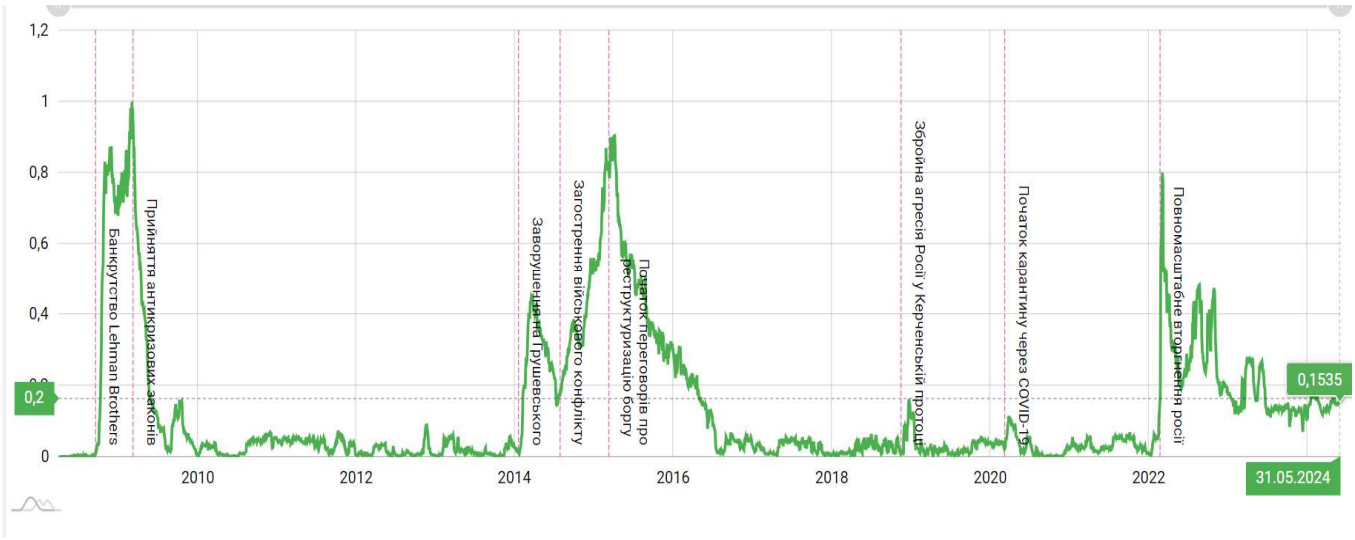


Рис. 5.4. Динаміка індексу фінансового стресу в Україні впродовж 2010-2024 рр.

(сформовано автором за [376])

Отже, за нинішніх невизначених умов для забезпечення нормального функціонування підприємства, кібербезпека є тим компонентом безпеки, який впливає на функціонування підприємств, репутацію, ставлення стейкхолдерів та ланцюги постачання. У надскладних умовах функціонування, що нині склалися в країні, питання безпеки залишається невирішеним. Для підприємств та організацій – безпека інформації та забезпечення безпеки даних і сервісів при використанні хмарних технологій залишається актуальною та потребує подальших досліджень для побудови стійкої бізнес-екосистеми [360].

Наслідки викликів через війну в Україні є важкопрогнозованими, передбачення їх впливу ускладнюється низькою поінформованістю щодо розв'язання збройного конфлікту, тому, оцінювання проводитиметься якісно з побудовою вірогідних сценаріїв розвитку підприємств сфери електронних комунікацій. Аналіз безпекового середовища підприємства доцільно провести матричним методом, з використанням інструментів VUCA та BANI для виявлення дестабілізуючих характеристик, а також SPOD для узагальнень отриманих результатів та побудови вірогідних сенаріїв щодо подальших умов функціонування підприємств.

Матриця сильних сторін, проблем, можливостей та невизначеностей (SPOD) – це стратегічний інструмент, який використовується для аналізу та розуміння ендогенного та екзогенного середовища організації.

Даний матричний аналіз дозволить окреслити загальні риси викликів, які постали перед сектором електронних комунікацій та викликів для України в умовах війни, що використовуватимуться як підгрунтя для визначення ключових факторів та формуванню стратегічних міркувань та узагальнень щодо упраління безпекою підприємства.

Таблиця 5.3

Матриця сильних сторін, проблем, можливостей та невизначеностей (SPOD)

Показник	Ендогенні можливості	Ендогенні проблеми	Екзогенні можливості	Екзогенні небезпеки
Сильні сторони	Розгалужена інфраструктура та покриття мережею, переміщення частини обладнання та устаткування у більш безпечні регіони Стійка клієнтська база. Кваліфікований персонал. Стратегічне партнерство та тісні взаємозв'язки із постачальниками послуг зв'язку в країнах ЄС, єдиний роумінг.	Зруйнована та пошкоджена інфраструктура на територіях бойових дій. Зростання операційних витрат через відбудову пошкодженої інфраструктури. Витрати на заходи безпеки. Підвищений ризик для безпеки робочих місць.	Гранти та допомога від іноземних партнерів. Зростання попиту на послуги зв'язку у роумінгу, збільшення обсягів передачі даних. Модернізація та використання нових технологій.	Невизначеність умов функціонування через втрату прогностичності тривалості воєнного стану. Економічна нестабільність. Регуляторна невизначеність. Зниження інвестиційної привабливості.
Проблеми	Високі витрати на технічне обслуговування. Ускладний доступ до обладнання до мереж електронних комунікацій в бойових дій. Висока вірогідність відмови в наданні послуг через втрати надійності працездатності мережі. Зниження пропускної здатності через перевантаження мережі.	Перебої в наданні послуг в результаті відключення енергосоптачання. Зниження платоспроможності . Споживачів. Загрози інформаційній та кібербезпеці через гібридну війну, яка ведеться агресором впродовж 10 років Відтік висококваліфікованих фахівців.	Сприяння та стимулювання державою відновленню інфраструктури. Ринки, що розвиваються в сільській місцевості. Програми розвитку цифрової інфраструктури та трансформаційні процеси, що покликані на розбудову цифрової держави.	Геополітичні ризики. Ринкова конкуренція. Порушення ланцюгів постачання.
Можливості	Потенціал для інновацій та відновлення сучасної інфраструктури. Експансія на нові, недостатньо охоплені ринки. Співпраця зі світовими технологічними компаніями	Повільні темпи реконструкції. Невизначеність інвестиційного клімату. Складне регуляторне середовище.	Розгортання технології 5G. Розширені цифрові послуги для віддаленої роботи та освіти. Розвиток е-комерції, е-послуг, е-гривні, фінтех.	Затягування тривалості конфлікту, що націлене на виснаження економіки, гальмування розвитку третинного сектору. Фрагментація ринку через регіональні особливості, відмінності. Перегляд споживачами кошику потреб через скорочення доходів.

продовження таблиці 5.3

Небезпеки	Наявний знаннєвий та інтелектуальний потенціал для швидкого відновлення та стабілізації ринку. Витривалість та стійкість перед обличчям несприятливих обставин. Державна підтримка розвитку сектору ІКТ	Знищення інфраструктури Економічний спад, що впливає на доходи. Посилення конкуренції з боку глобальних гравців.	Міжнародна співпраця з питань відновлення сектору ІКТ. Зацікавленість в освіті сфери ІКТ. Потенційне зростання попиту на послуги зв'язку для забезпечення освітнього процесу та роботи у віддаленому режимі	Тривала регуляторна невизначеність. Ескалація конфлікту. Потенційна націоналізація або суворий державний контроль.

(складено автором)

За результатами побудови матриці та аналізу інфраструктура підприємств-постачальників електронних комунікаційних мереж та послуг відзначається стабільністю та збереженням функціонування в регіонах, які знаходяться територіально віддалено від зони бойових дій, що дозволяє продовжувати надавати послуги та обслуговувати клієнтів. Клієнтська база є стійкою через лояльність до клієнтів та тривалим користуванням полсугами конкретного оператора, крім того якісний зв'язок забезпечується трьома основними постачальниками послуг електронних комунікацій, що стримує перехід до інших постачальників електронних комунікаційних послуг, тим самим забезпечує компаніям надходження оплат та приросту доходів від послуг.

Інтелектуальний капітал значиться, як висококваліфікований, здатний працювати в сфері інноваційних та цифровізаційних змін. Слід відмітити посилення стратегічного партнерства з міжнародними організаціями та телекоммунікаційними групами, що сприяє пришвидшенню інтеграції та відкриває доступ до технологій та ресурсів.

Серед екзогенних проблем значаться наступні: зростання витрат на утримання інфраструктури, особливо у зонах бойових дій; ускладнення доступу до мереж та їх обслуговування у районах на територіях, що постраждали від конфлікту та були деокуповані. Складність забезпечення надійної роботи мережі через наближеність окремих територій до зон активних бойових дій.

Екзогенними можливостями виступають: виявлення ініціативи до інвестування сектору ІКТ з метою його відновлення та укріплення з боку міжнародних країн-партнерів та організацій; зростання потреби перебування на зв'язку для моніторингу подій та спілкування, онлайн роботи та навчання [357]; потенціал до впровадження нових технологій з метою модернізації та розширення спектру послуг; сприяння на інституційному рівні інноваційній розбудові та відновленню інфраструкутри з розвитку сфер ІКТ.

Серед екзогенних небезпек виокремлюються: триваліть конфлікту, зростання рівня інфляції, валютні коливання та економічна нестабільність, як наслідок зниженя купівельної спроможності споживачів послуг; невизначеність державного та регуляторного середовища, що суттєво впливає на інвестування та побудову стратегічних планів; висока геополітична напруга та перепони для фінансування з боку країн-прибічників країни агресора; невизначеність стратегічних міркувань щодо розбудови сектору ІКТ на найближчу перспективу.

Аналіз сильних сторін, що нині характерні для підприємств-постачальників електронних комунікаційних мереж, дозволяє визначити перспективи вирішення вищезазаначених проблем наступним чином:

- посилення стратегічного партнерства задля пришвидшення модернізації та розбудови сектору ІКТ;
- залучення висококваліфікованих фахівців з впровадження новітніх інноваційних рішень з метою забезпечення надійності та операційної ефективності мережі;
- співпраця з міжнародними гуманітарними організаціями та інвесторами, фандрайзинговими платформами для забезпечення фінансування відновлювальних робіт;
- моніторинг потенціалу виходу на нові ринки в регіонах з недостатньо розвиненою мережею зв'язку;
- інвестувати в 5G і цифрові послуги, щоб задовольнити зростаючий попит на високошвидкісний інтернет і цифровий зв'язок;

- розробка перспективних та прогностичних планів на випадок надзвичайних ситуацій т
- інвестування з захист інформаційних активів, в кібербезпеку, щоб захиститися від зростання кількості кіберзагроз;
- гнучкість планів та стратегій розвитку, щоб адаптуватися до невизначених умов, мінливого регуляторного середовища з причин інтегрування в європейський простір [359];
- активна співпраця з державними та міжнародними організаціями, установами для вирішення економічних та регуляторних проблем;
- систематично та перманентно аналізувати фактори впливу на функціонування підприємств-постачальників електронних комунікаційних мереж та послуг для подолання поточної невизначеності та побудови гнучких стратегій розвитку, а також швидкого відновлення та зростання.

З урахуванням низької прогностичності та постійного мінливого середовища функціонування підприємств-постачальників електронних комунікаційних мереж та послуг, проведено аналіз викликів, які постали перед сектором електронних комунікацій в умовах війни. Запропоновано науково-методичний підхід до оцінки викликів за невизначених умов функціонування підприємств, який ґрунтується на матричному аналізі сильних сторін, проблем, можливостей, невизначеностей (матриця SPOD) та комбінації VUCA, BANI-аналізу для виявлення дестабілізуючих факторів в умовах високої ентропії, на основі якого побудовано чотири вірогідні сценарії розвитку підприємств сфери електронних комунікацій (рис. 5):

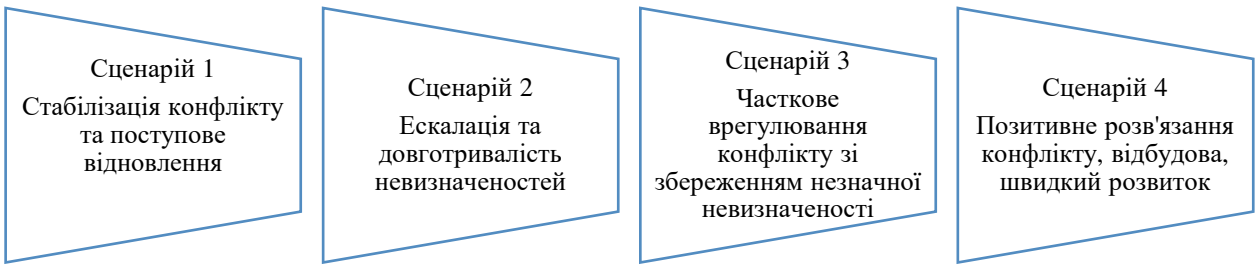


Рис. 5.5. Вірогідні сценарії щодо подальших умов функціонування підприємств *(авторська розробка)*

– стабілізація конфлікту та поступове відновлення;
– ескалація та довготривалість невизначеностей;
– часткове врегулювання зі збереженням незначної невизначеності;
– позитивне розв'язання конфлікту, відбудова, швидкий розвиток.

З причин відсутності інформації щодо подальшого розгортання подій, дані сценарії важко оцінити кількісно, тому оптимальним у даному випадку є якісний аналіз, при чому на основі VUCA та BANI-аналізу, які розглядалися більш детально у попередніх розділах роботи, а також є прийнятними за невизначених умов функціонування підприємств.

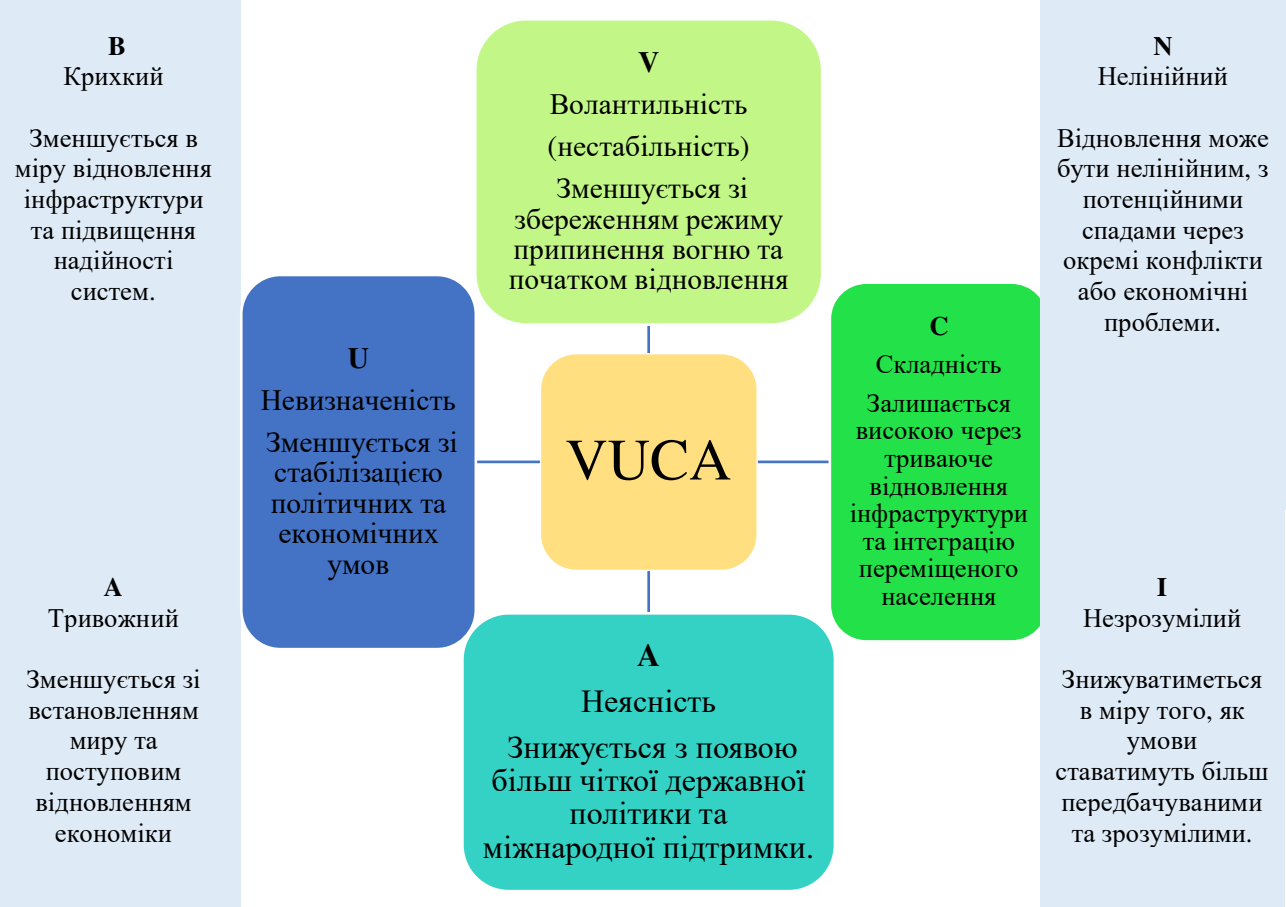


Рис. 5.6. Аналіз VUCA та BANI для сценарію 1 – стабілізація конфлікту та поступове відновлення

(авторська розробка)

Для сценарію 2 – ескалація та довготривалість невизначеностей, вбачатиметься невизначеність окреслена характеристиками, що наведені на рис. 5.7

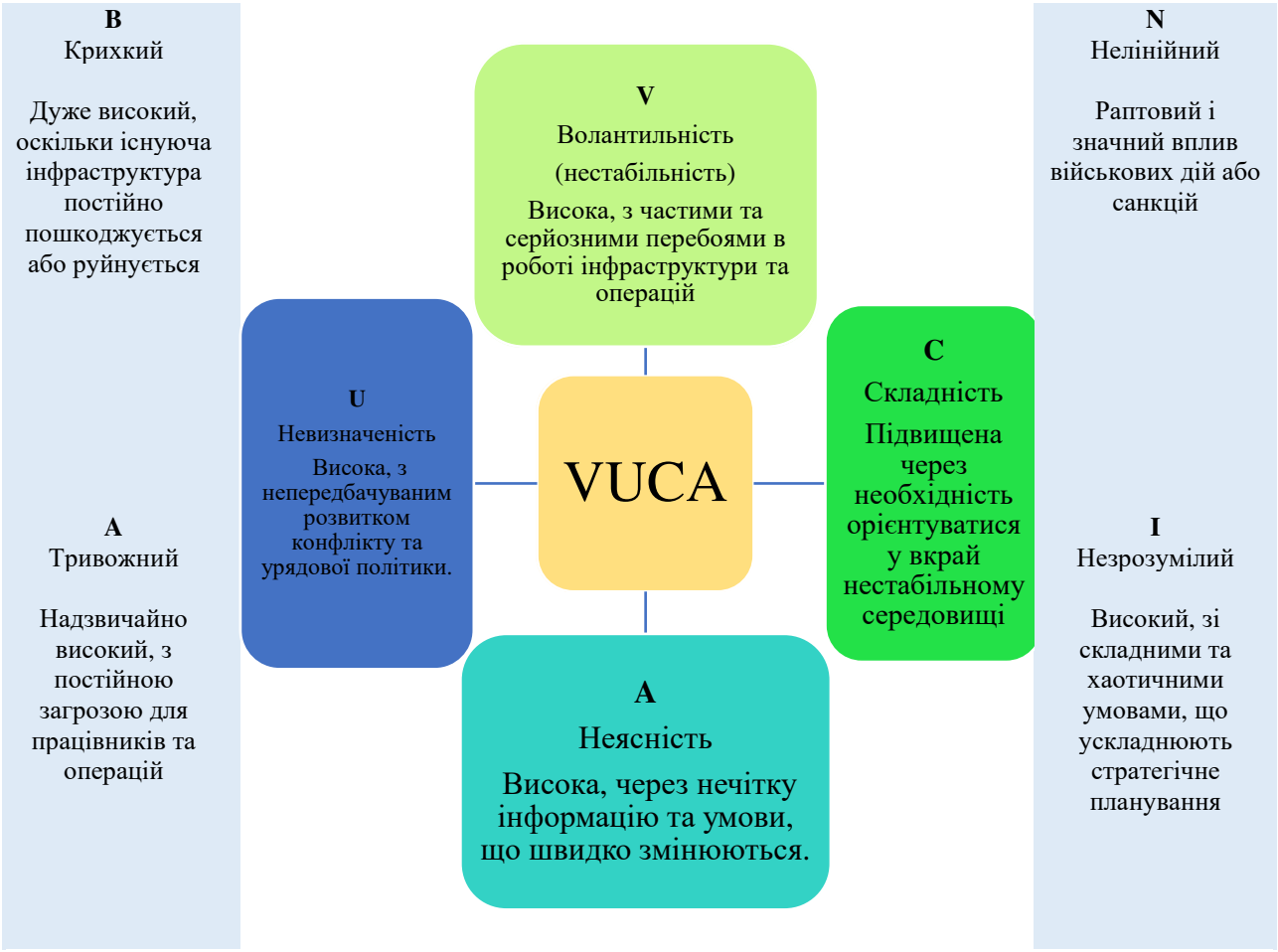


Рис. 5.7. Аналіз VUCA та BANI для сценарію 2 – ескалація та довготривалість невизначеностей

(авторська розробка)

За даного сценарію підприємства-постачальники електронних комунікацій мають створювати асоціації постачальників послуг зв'язку з метою підвищення готовності до нестабільності функціонування та надзвичайних умов функціонування, розробляти спільні плани щодо управління (антикризового управління), використовувати адаптивн технології, здійснювати переключення між мережами та децентралізувати мережеві системи з метою забезпечення їх функціональності, створювати максимально безпечні умови роботи для персоналу (захист об'єктів, захисні споруди, віддалена робота).

Сценарій 3 – часткове врегулювання зі збереженням незначної невизначеності вказує на епізодичне продовження виявлених характеристик за сценарієм 4.

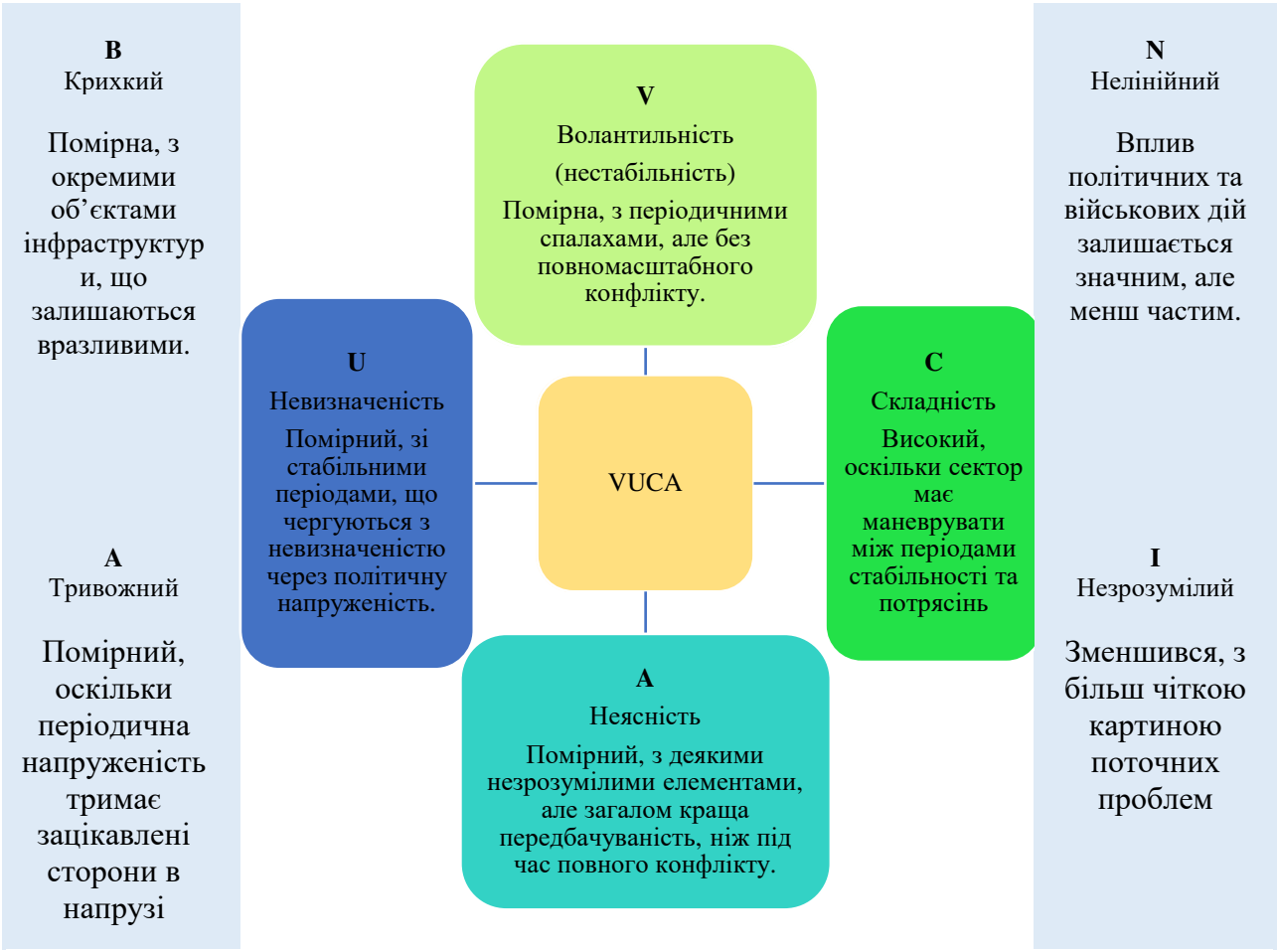


Рис. 5.8. Аналіз VUCA та BANI для сценарію 3: часткове врегулювання зі збереженням незначної невизначеності

(авторська розробка)

Сценарій часткового врегулювання проблеми невизначеності умов із частковим її збереженням передбачає перегляд питань щодо гнучкості стратегій для оперативного вирішення питань щодо збільшення або зменшення обсягів постачання послуг в залежності від умов; захист інфраструктури від загроз, передача ризиків шляхом страхування об'єктів; сприяння розбудові комунікаційних зв'язків з регулятором, інституціями, споживачами, стратегічними партнерами для керованості процесів при зміні поглядів щодо функціонування підприємств зв'язку; інвестування у кібербезпеку та протидіяти дезінформації щодо роботи підприємства з метою збереження репутації.

Останнім до розгляду пропонується найбільш оптимістичний сценарій – позитивне розв'язання конфлікту, відбудова, швидкий розвиток значиться наступними характеристиками (рис. 5.9).

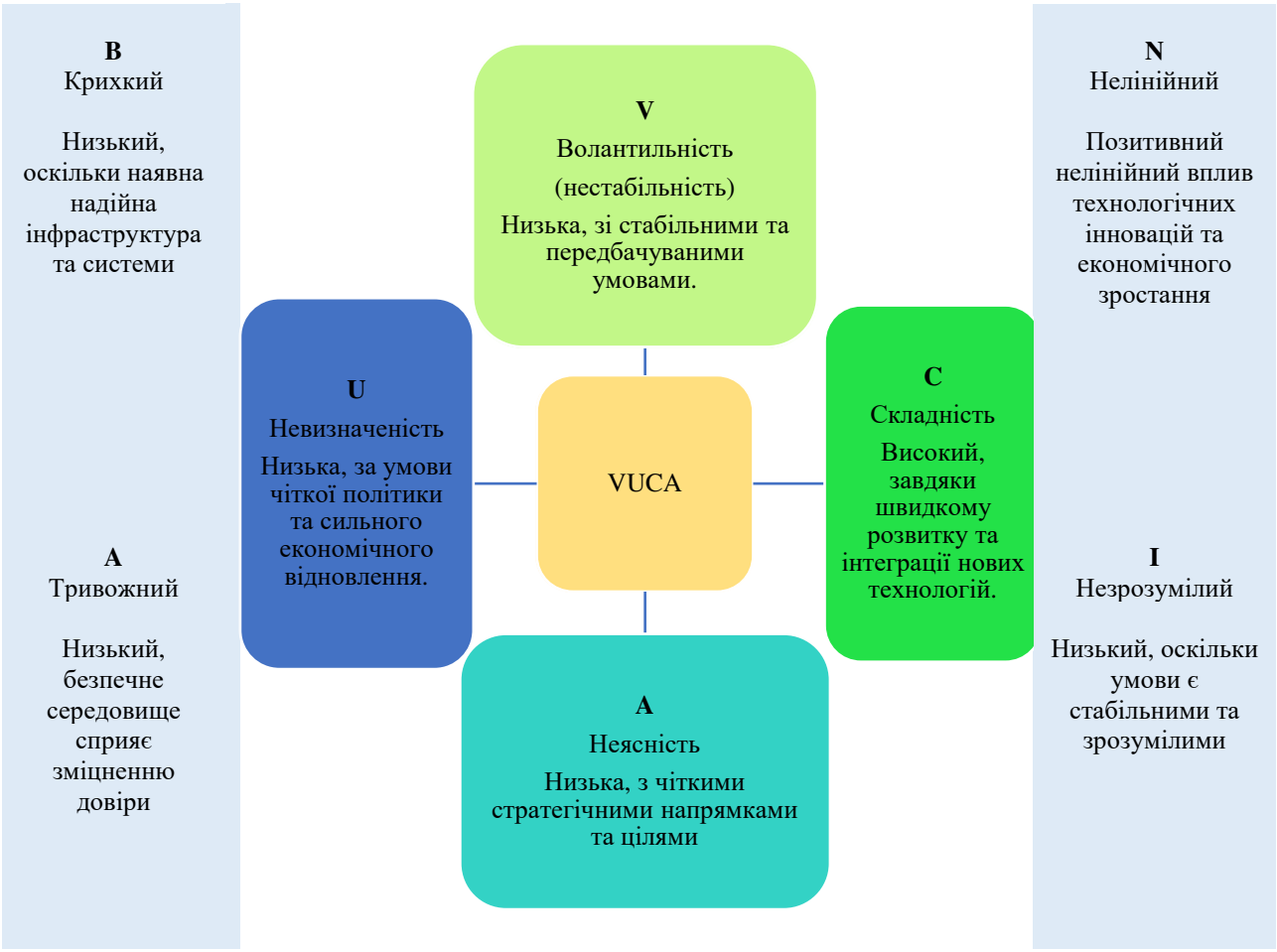


Рис. 5.9. Аналіз VUCA та BANI для сценарію 4 – позитивне розв'язання конфлікту, відбудова, швидкий розвиток

(авторська розробка)

Останній сценарій передбачає врахування наступних аспектів з метою забезпечення функціонування підприємств-постачальників електронних комунікацій: прогресивне інвестування в розбудову мережі та переходу на новітні технології надання зв'язку споживачам послуг, модернізація мереж для відповідності вимог європейського інфокомунікаційного простору; розширення переліку послуг зв'язку, підвищення якості надання послуг для

збільшення швидкості передачі даних в роумінгу; залучення іноземних партнрів до проєктів та інноваційних розробок, дотримання принципів сталого розвитку для підтримки концепції розвитку без загрози існуванню майбутнім поколінням, корпоративна відповідальність.

Передбачені сценарії розвитку подій та їх варіантів дозволяють передбачити зміни умов та надати пропозиції рекомендаційного характеру для врахування їх при побудові стратегічних планів щодо функціонування підприємств-постачальників електронних комунікаційних мереж та послуг для забезпечення стійкості та гнучкості за мінливих та важкопрогнозованих умов.

5.2. Науково-параметрична діагностика безпеки підприємства за умов невизначеності

Умови функціонування підприємств, як вже було зазначено, характеризуються невизначеністю, відсутність інформації щодо розгортання майбутніх подій спрямовує дослідження до пошуку варіантів розв'язання проблеми низької прогностичності щодо розвитку та результатів діяльності суб'єктів господарювання.

У сучасній економіці концепція рівноваги та поінформованості щодо оточення спростовується, оскільки теорії рівноваги економічних систем зазнала змін. Розвиваються нові теорії, що базуються на інформаційній асиметрії, коли у ринковому середовищі одна із сторін (стейкхолдер) більш поінформована за іншу. На думку Л. Вентхаде та Б. Дабаде, такі інформаційні диспропорції стали ще одним виміром якості сучасної нерівноважної економіки [413, с.7].

Дж. Стігліц зробив значний внесок у розуміння впливу інформації на економічні ринки. У своїй праці "Теорія інформаційної економіки" ("The Theory of Information Economics") вчений розкриває ключові аспекти ролі інформації в економічних процесах та пояснює, чому інформаційна асиметрія,

коли одна сторона угоди володіє більшою або кращою інформацією, ніж інша, може призводити до ринкових збоїв [414].

Теорія інформації – це галузь математичної теорії, що досліджує кількісні аспекти інформації, способи її передачі, обробки та зберігання. Вона відіграє ключову роль у розвитку сучасних інфокомунікаційних технологій, комп'ютерних наук та криптографії. Теорія інформації охоплює поняття ентропії, яка вимірює кількість невизначеності в системі, та канальної пропускної здатності, що визначає максимальну швидкість передачі інформації через комунікаційний канал без втрат [412].

Виклики, за яких функціонують підприємства, спричиняють непередбачуваність та низьку прогностичність подій, тому традиційні методи оцінки впливу оточення на підприємство, як нами зазначалося у третьому розділі роботи, є недієвими. Доцільним до використання визначено підхід до оцінки невизначеності на основі врахування ентропії, яка дозволяє виміряти невизначеність, що нині формується за сьогоднішніх незвизначених умов господарювання суб'єктів підприємництва.

Поняття "ентропія" найчастіше використовується в термодинаці, а також теорії інформації, проте, знайшло застосування в економічній науці для вимірювання невизначеності, різноманітності та складності умов, в яких перебувають суб'єкти господарювання, тобто в економіці ентропія найчастіше використовується для аналізу непередбачуваності системи, ринку або економічних параметрів, тому нами буде проводитися параметрична оцінка впливу викликів на підприємства саме за цим показником [415].

Використання підходу, що грунтується на врахуванні ентропії, дозволяє отримувати результати з двовимірним розподілом, досліджувати прямокутну геометричну область [416; 417]. Отриманий розподіл значень, визначений за допомогою запропонованого розподілу, добре узгоджується з експериментально виміряними значеннями динамічності різних модифікацій для поширення ентропії. Ентропія Шеннона враховує безперервну кількість випадкових величин, можна також вираховувати середню ентропію (AE), якою

узагальнюється, неперервні та дискретні вплив викликів. Ентропія є адитивною, додатньою та прирівнюється до нуля лише у разі рівномірного розподілу. Перевагою ентропії є можливість формування рівня невизначеності в різних періодах або за різних сценаріїв, щоб скласти картину невизначеності в динаміці й приймати обгрунтовані рішення для управління підприємствм в умовах невизначеності та задля складння стратегічних напрямів розвитку підприємств для управління.

Важливо, що при визначенні ентропії передбачається врахування взаємозв'язку із інформацією, тобто даними, які отримані щодо оточення, можна графічно представити ентропію у сегментації зображення ефективності, попередньо визначивши її за формулою, що наведена нижче:

$$\mathrm{H(X)} = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i), \qquad (5.1)$$

де H(X) – ентропія;

$p(x_i)$ – ймовірність окремого виклику для постачальників електронних комунікаційних мереж та послуг;

log – натуральний логарифм з основою 2.

Проаналізувавши виклики сучасності, нами було виокремлено найсуттєвіші та явні: руйнування та пошкодження інфраструктури; експлуатаційні порушення; загрози кібербезпеці; невизначеність нормативно-правового, інституційного регулювання; а також нестабільність економіки. На сьогодні перелічені виклики вимірюються відповідними їм ймовірностями, які оцінються наступним чином (рис. 5.10):

- Руйнування та пошкодження інфраструктури (x_1) – 0.3
- Експлуатаційні порушення (x_2) – 0.2
- Загрози кібербезпеці (x_3) – 0,15

– Невизначеність нормативно-правового, інституційного регулювання (x_4) – 0,1

– Нестабільність економіки (x_5) – 0,25

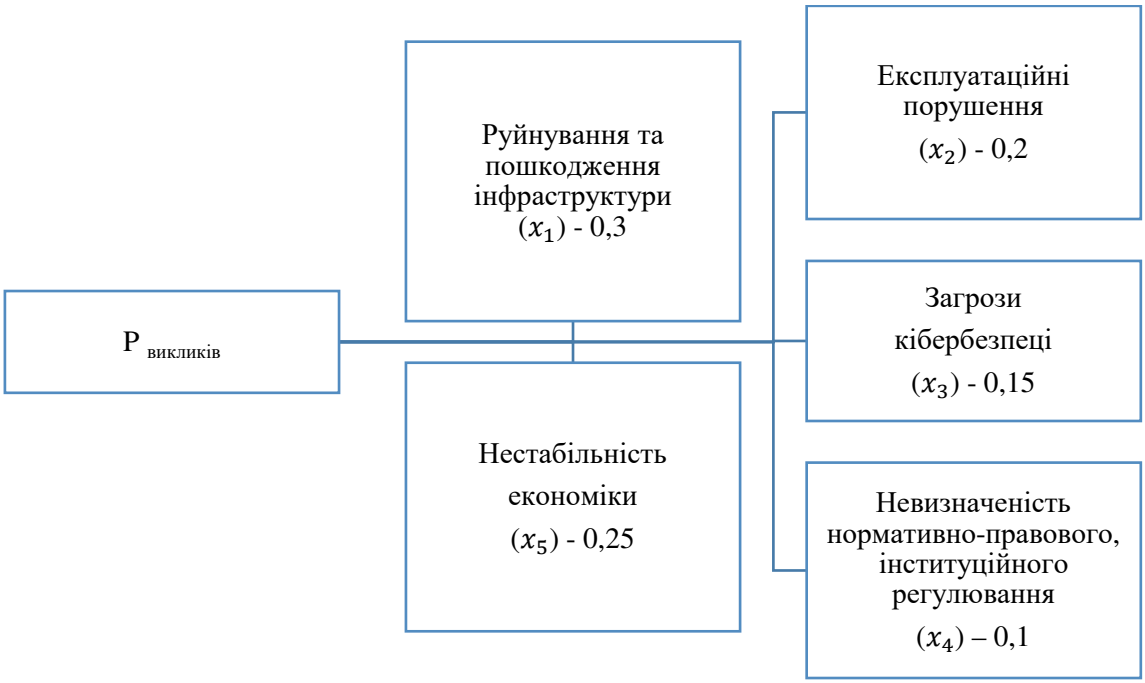


Рис. 5.10. Ймовірності викликів невизначеності для підприємств-постачальників електронних комунікаційних мереж та послуг *(авторська розробка)*

Зважаючи на п’ять викликів, що нині іденифікуються як найвірогідніші, формула 5.1 набуває вигляду:

$$H(X) = -(p\,(x_1)\log_2 p(x_1) + (p\,(x_2)\log_2 p(x_2) + \ (p\,(x_3)\log_2 p(x_3\,) + (p\,(x_4)\log_2 p(x_4) + \ (p\,(x_5)\log_2 p(x_5), \quad (5.2)$$

Підставляючи у формулу 5.2. ймовірності викликів, отримуємо:

$$H(X) = -(0{,}3\ \log_2 0{,}3) + (0{,}2\log_2 0{,}2) + \ (0{,}15\log_2 0{,}15) + (0{,}1\log_2 0{,}1) + \ (0{,}25\log_2 0{,}2\,5) = 0.3\times(-1.737) + 0.2\times(-2.322) + 0.15\times(-2.737) + 0.1\times(-3.322) + 0.25\times(-2.0) = -\,(-2{,}228) = 2{,}228$$

Таким чином, в результаті параметричної оцінки невизначеності за допомогою ентропії отримуємо значення 2,228, що свідчить про високий рівень невизначеності (можна порівняти значення в динаміці або різних сценаріїв розвитку для оцінки змін в невизначеності), результати її оцінки наведено на рис. 5.11

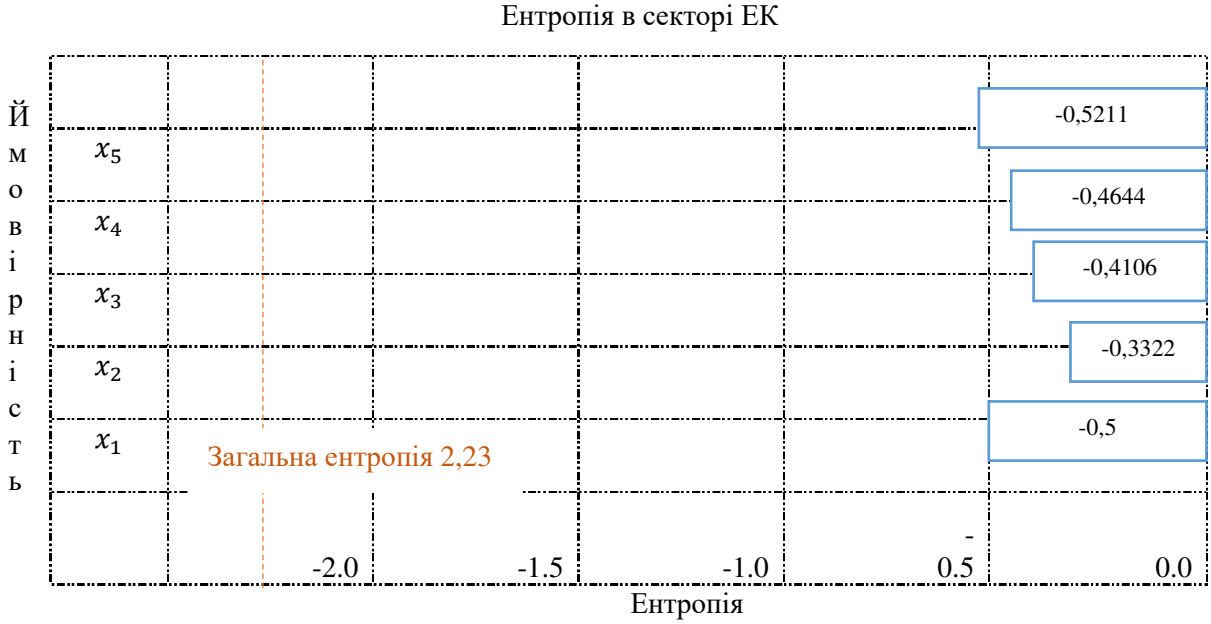


Рис. 5.11. Ентропія у секторі ІКТ за невизначених умов

(розраховано автором)

Слід відмітити, що усталених норм оцінки ентропії немає, за нормальних умов функціонування, доволі часто ентропія оцінюється для визначення середовища функціонування підприємств в залежності від приналежності по типу ринкової структури, нинішній ринок електронних комунікацій можна визначити конкуретним для постачальників послуг інтернет-зв'язку, а увесь можливий спектр послуг надають тільки три основні гравці – ПрАТ "Київстар", ПрАТ "ВФ Україна", ТОВ "Лайфселл", тому він наближений до олігополістичного. Ентропія для підприємств, що господарюють за даного типу ринкової інфраструктури коливаєтьсяу межах до 1,5 біт.

Загалом низька ентропія від 0 до 1 біт, вказує на високу передбачуваність, помірна ентропія від 1 до 2 біт – низьку передбачуваність; висока – від 2 до 3 біт вказує на складність передбаченння та невизначеність.

Аналіз невизначеного середовища дозволив визначити змінні, що описують впливи викликів на результати за визначеними ймовірностями для кожного результату (ретроспективно, по відношеню динаміки зростання прибутку за нормальних умов функціонування), кількісно визначити ентропію в середовищі функціонування підприємств за обчисленими логарифмами ймовірностей. Отже, H(X) викликів сектору електронних комінікацій під час воєнних дій на території України становить приблизно 2,23 біта, що відображає рівень непередбачуваності та складності в управлінні виявленими викликами. Вища ентропія вказує на більшу невизначеність і складність у вирішенні цих проблем. Отримане значення ентропії 2,23 може використовуватися керівниками та зацікавленими сторонами для прийняття обґрунтованих рішення щодо стратегії управління безпекою підприємтсв за умов низької поінформованості.

Для повоєнного відновлення наразі підприємствам варто моделювати стратегії розвитку, підприємства-постачальники електронних комунікаційних послуг мають орієнтуватися на стратегічну спрямованість держави у європейський простір.

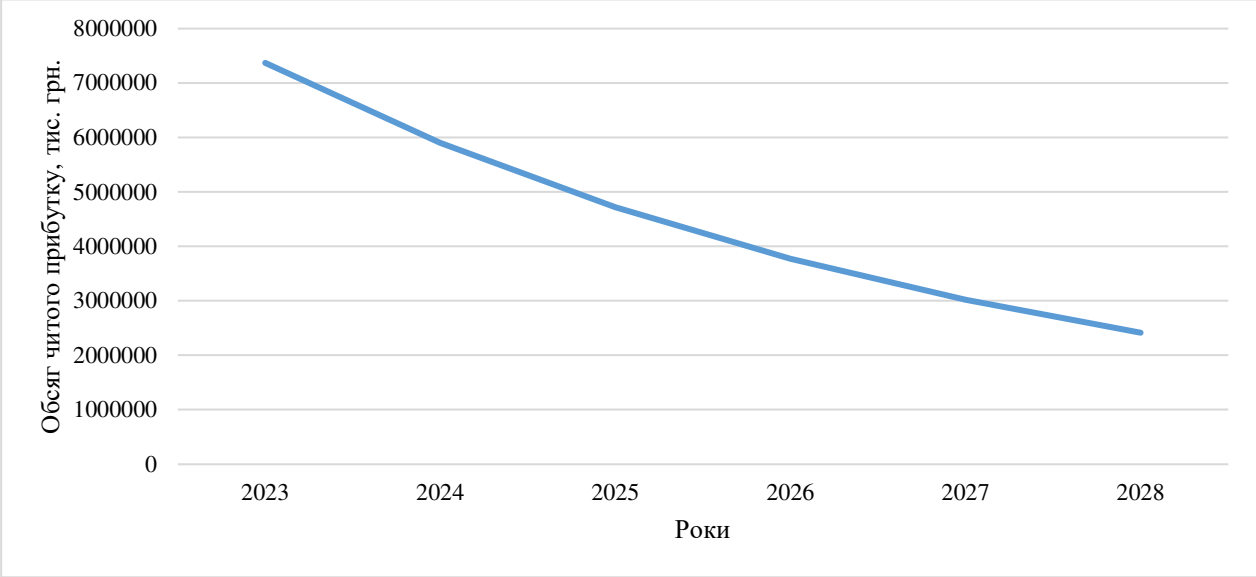


Рис. 5.12. Логарифмічне зменшення сумарного чистого прибутку досліджуваних підприємств у повоєнний період (стадія відновлення) з урахуванням ентропії, тис. грн

(розраховано автором)

У результаті дослідження за сценарієм відновлення й вирахуваними вірогідними впливами викликів та ентропією, отримуємо що прибуток знижуватиметься щороку через зменшення впливу невизначеності, відсоток втрат впродовж 5-ти років становитиме: на початковому етапі – 22,3% (за ентропією), а потім лінійно скорочуватиметься з кроком в 4%, тобто становитиме: 18%; 14%; 10%; 6%; 2% відповідно у кожному наступному році.

Динаміка чистого прибутку підприємств-постачальників електронних комунікаційних послуг за інертним сценарієм відновлення наведена у табл. 5.4.

Таблиця 5.4

Динаміка чистого прибутку підприємств-постачальників електронних комунікаційних послуг за інертним сценарієм відновлення*, тис. грн

Рік	Ентропія прибутку по роках	Зменшення прибутку
2023	22,3%	7372743,2
2024	18%	5898194,56
2025	14%;	4718555,648
2026	10%;	3774844,518
2027	6%	3019875,615
2028	2%.	2415900,492

* без змін та пропозицій, тобто поступове відновлення, розрахунок загального чистого прибутку досліджуваних підприємтсв

(авторська розробка)

Зменшення ентропії позитивно відзначається на прибутку, скорочення якого відбувається впродовж п’ятирічного періоду навіть при природному відновленні умов функціонування підприємств та зменшення викликів, їх наслідків, проте доцільно спрогнозувати прибутки за дотриманням сценарію для відновлення. План вибудовує шлях до швидшого подолання наслідків викликів з кожним наступним роком покращуючи цільові безпекові результати, окрім того, можливо спрогнозувати песимістичний та оптимістичний сценарії для більш точного розуміння результативності.

Спрогнозовано прибуток досліджуваних підприємств за трьох вірогідних сценаріїв розвитку для досліджуваних компаній (рис. 5.13, рис. 5.14, рис. 5.15, рис. 5.16, рис. 5.17).

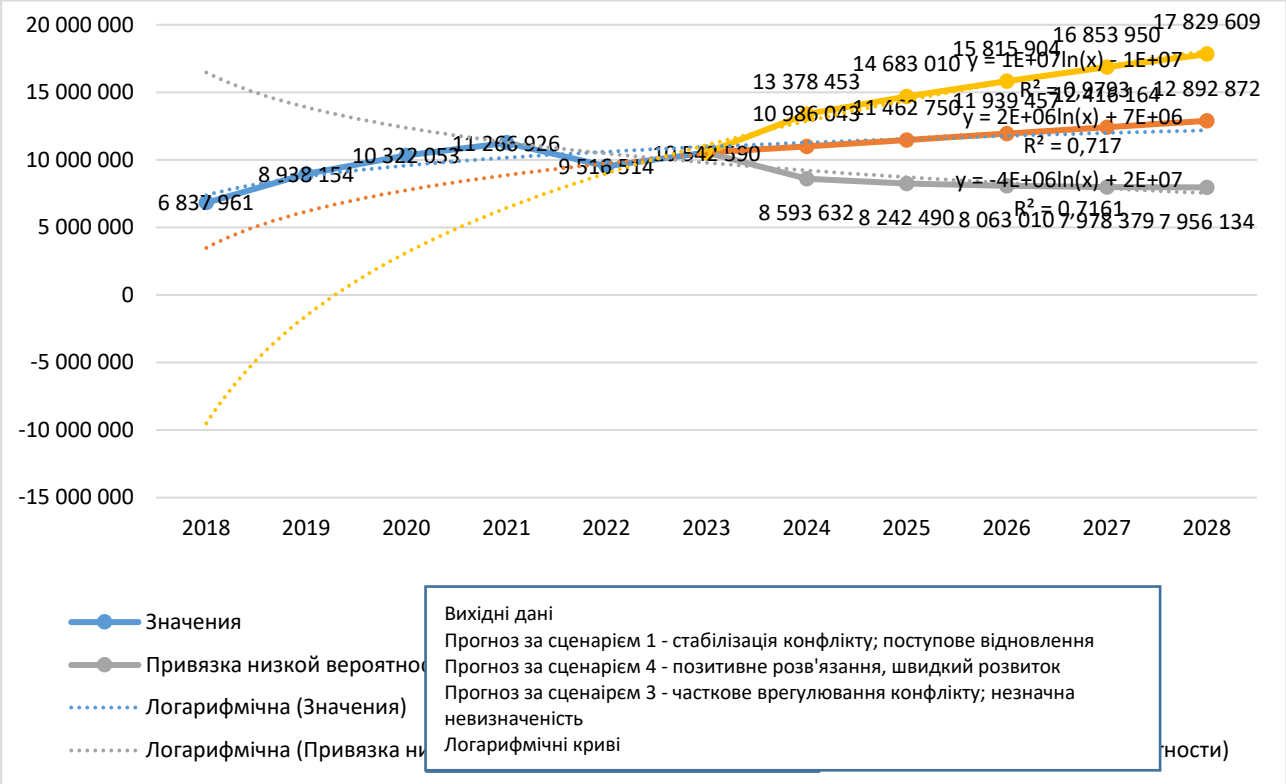


Рис. 5.13. Прогнозування прибутку ПрАТ “Київстар” до 2028 року для трьох вірогідних сценаріїв умов функціонування підприємств (з урахуванням ентропії) *(розраховано автором)*

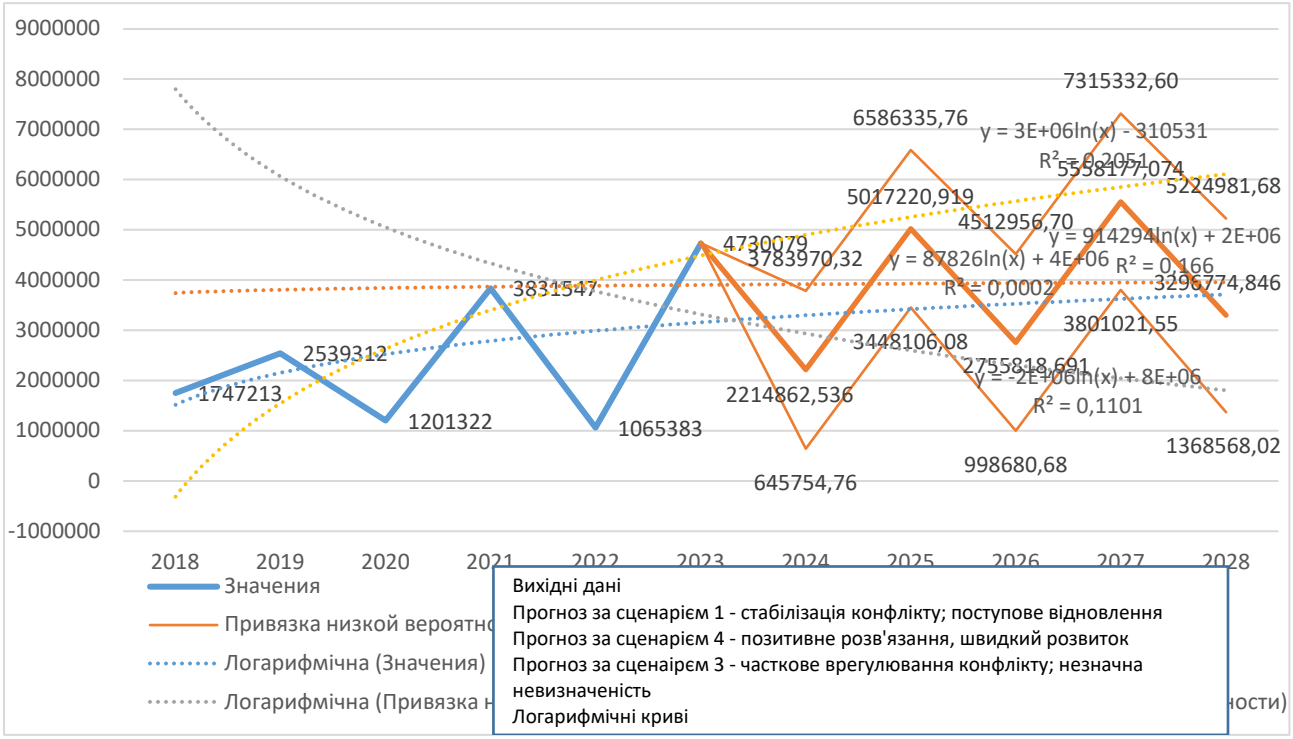


Рис. 5.14. Прогнозування прибутку ПрАТ “Водафон” до 2028 року для трьох вірогідних сценаріїв умов функціонування підприємств з урахуванням ентропії *(розраховано автором)*

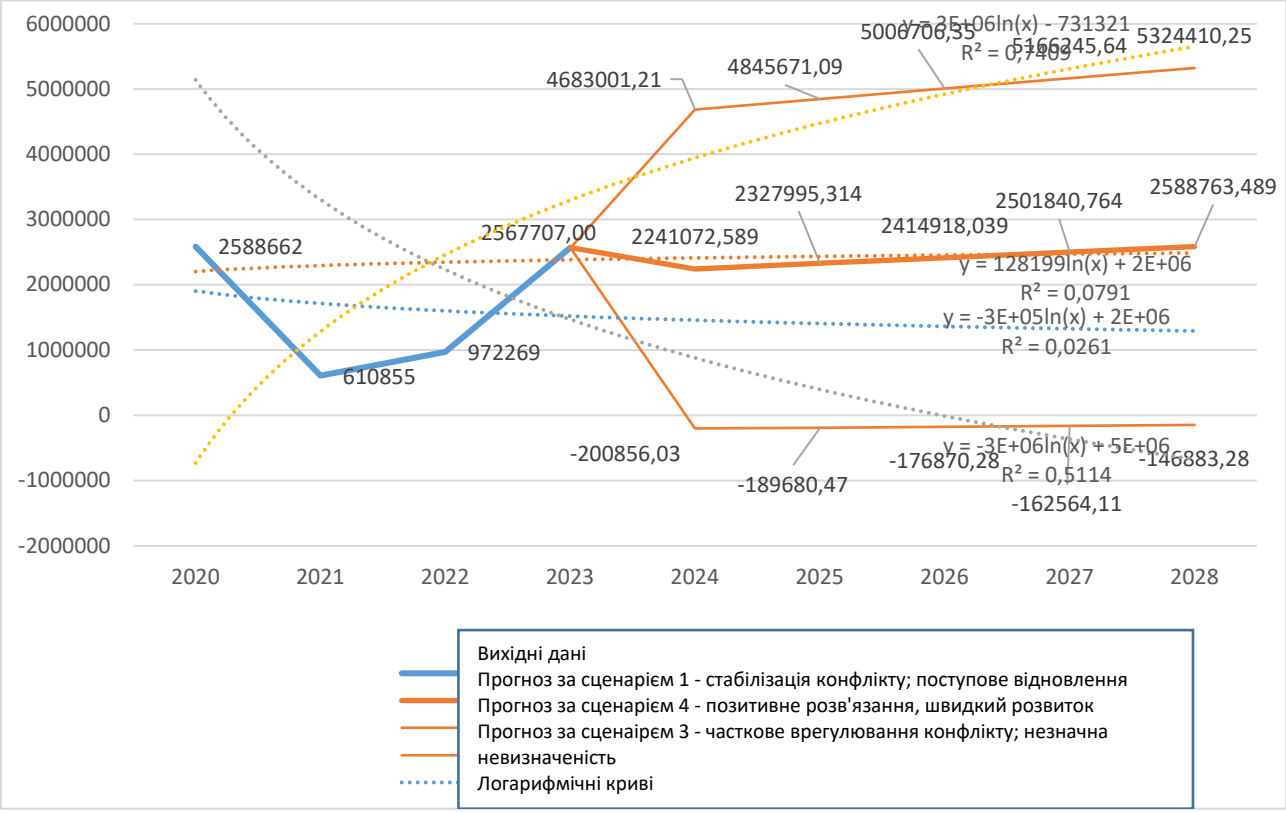


Рис. 5.15. Прогнозування прибутку ПрАТ “Лайфселл” до 2028 року для трьох вірогідних сценаріїв умов функціонування підприємств з урахуванням ентропії *(розраховано автором)*

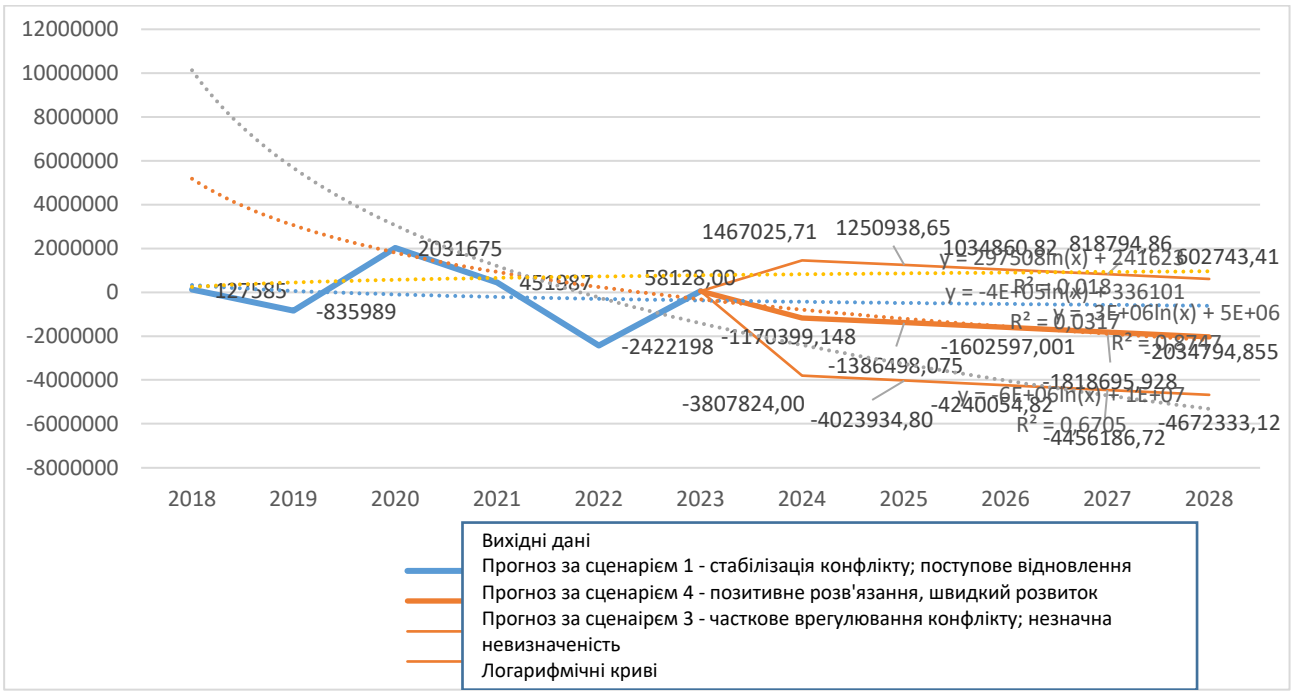


Рис. 5.16. Прогнозування прибутку ПрАТ “Укртелеком” до 2028 року для трьох вірогідних сценаріїв умов функціонування підприємств з урахуванням ентропії *(розраховано автором)*

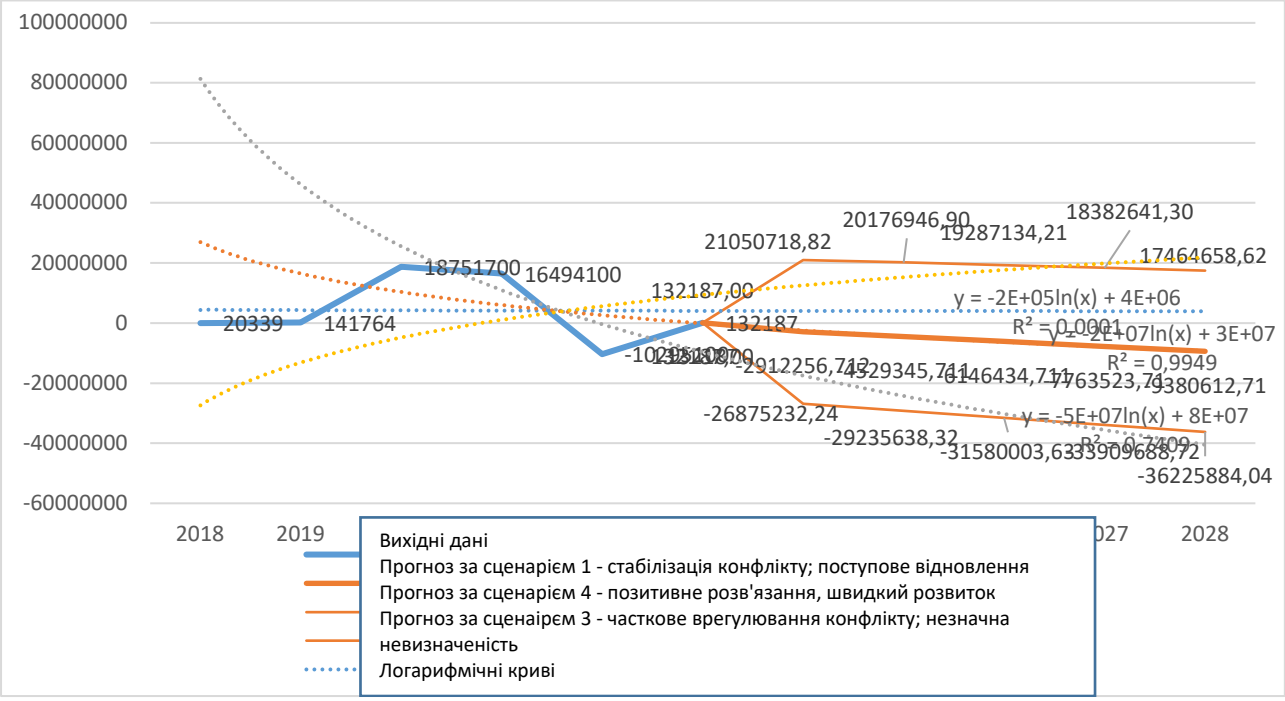


Рис. 5.17. Прогнозування прибутку ПрАТ “Датагруп” до 2028 року для трьох вірогідних сценаріїв умов функціонування підприємств з урахуванням ентропії *(розраховано автором)*

5.3. Стратегічні напрями розвитку підприємства як підгрунтя для управління безпекою підприємства в повоєнний час

Стратегічні напрями розвитку відновлення грунтуються на комбінації, що націлені на пришвидшення усунення викликів та нейтралізації їх наслідків за рахунок наступних ініціатив: відбудова та модернізація інфраструктури; операційна ефективність та стійкість; посилення заходів кібербезпеки; регуляторна відповідність та адвокація; економічна адаптація та зростання (рис. 5.18).

Стратегічний напрям слугуватиме дорожньою картою для забезпечення цільових безпекових орієнтирів в умовах сьочасних викликів та забезпечення

безпеки, оскільки, в противагу звичайним умовах господарювання, невизначеність не дозволяє гарантувати безпеку, формує тільки траєкторію руху її досягнення.

Перша стратегія націлена на *відбудову та модернізацію інфраструктури та* вирішує виклик пошкодження інфраструктури (ЕН) – 0,3, досягається шляхом:

– державно-приватного партнерства (співпраця з урядом та міжнародними донорами, організаціями для забезпечення фінансування відновлення і, за можливості, розбудови інфраструктури)

– технологічної модернізації (інвестування в сучасні технології, такі як 5G, волоконна оптика та Інтернет речей, щоб побудувати стійкі та сучасні мережі).

– децентралізації (впровадження децентралізованої мережевої архітектури для підвищення надійності та зменшення вразливості до локальних пошкоджень).

У результаті забезпечується підвищення надійності та пропускної здатності мережі, підвищення якості послуг для споживачів та бізнесу, підвищення стійкості до майбутніх збоїв. Слід тримати курс на активну та орієнтовану на довгострокову перспективу стратегію розвитку підприємств ПЕКМП, яка передбачає високу швидкість реакції на зміни; формування конкурентних переваг; гнучкість; інтенсивність використання факторів виробництва; інноваційність [377; 381]. Враховуючи рівень розвитку об’єктів і суб’єктів ринку ЕК, а також рівень їх впливовості, доцільно виокремити основні із них, які першочергово враховуватимуться при формуванні стратегій або напрямків розвитку підприємства сфери електронних комунікацій (рис. 5.19).

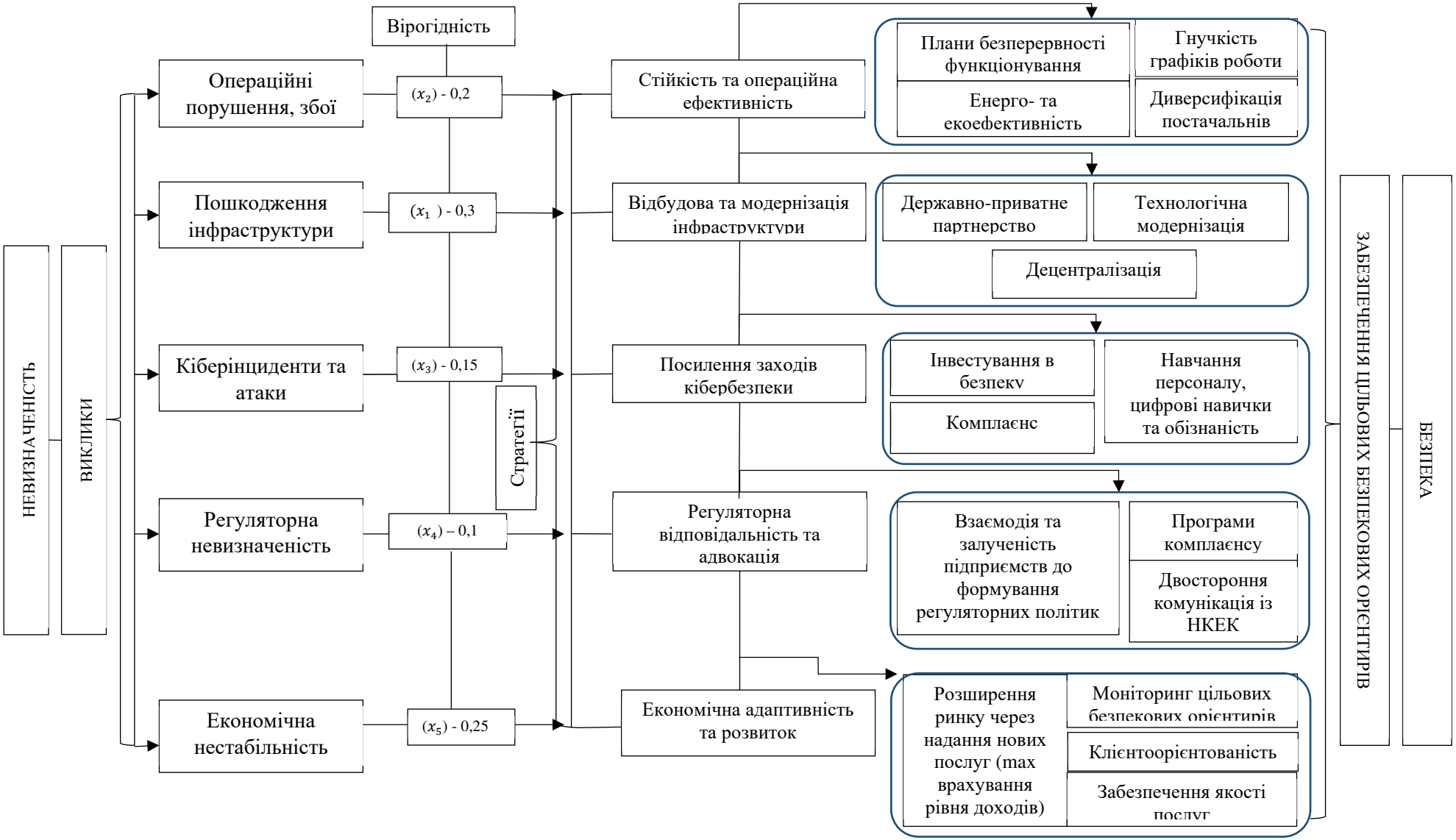


Рис. 5.18. Стратегічні напрями подолання викликів для забезпечення цільових безпекових орієнтирів підприємств-постачальників електронних комунікаційних мереж та послуг *(авторська розробка)*

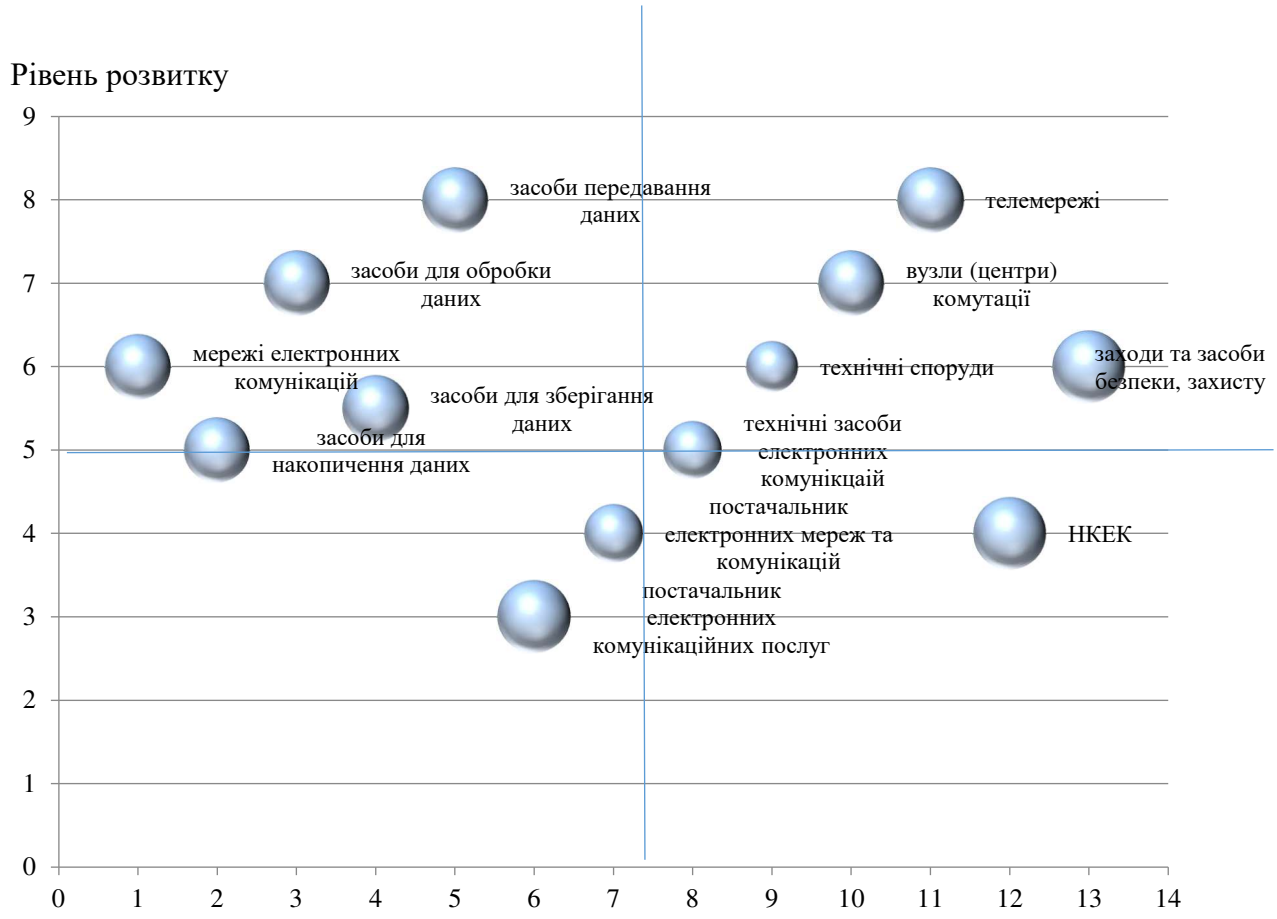


Рис. 5.19. Визначення ключових складових (об’єктів і суб’єктів) у формуванні напрямків розвитку підприємств ПЕКМП в умовах цифровізації та невизначеності

(складено автором [382])

В умовах воєнного стану в Україні та масованих обстрілів об’єктів критичної інфраструктури відзначається вагомість сектору електронних комунікацій та енергетики, чітко окреслюється необхідність їх спільної роботи для сталого розвитку.

Неприпустимо, щоб населення залишатися без зв’язку, більшість інформації отримується саме із глобальної мережі, система оповіщення працює, коли наявний інтернет. Через масовані обстріли, які чиняться з боку країни агресора, відчутними є суттєві порушення у каналах зв’язку, тому безпечність їх роботи є пріоритетною. Тобто, належна увага має приділятися питанням безпеки, що нині забезпечується через розгляд питань, що стосуються інтересів

споживачів електронних комунікаційних послуг та регулюється національним регулятором у сфері зв’язку.

Наразі, у випадку розташування базових станцій у важкодоступних для подання або відновлення електропостачання районів нині використовуються генератори (як правило дизельні). Актуалізується питання застосування відновлюваної енергетики, гібридних методів для забезпечення безперебійної роботи електростанцій, при чому, окрім стабільного надання ЕК послуг, усувається втрата доходів, яка могла б виникнути через неможливість надання послуг в тих, чи інших регіонах, які знаходяться без зв’язку. Ще одним позитивним моментом є те, що при використанні відновлюваної енергетики та гібридних методів постачальники електронних комунікаційних послуг знизять витрати за рахунок економії коштів від альтернативних джерел енергії.

Стабільність мережі та послуг для забезпечення безпечної, безперебійної роботи ІТ сектору наріжним є питання створення гідридних міні-мережевих систем змінного струму, при якій електроенергія передається від джерела енергії безпосередньо в мережу, при одночасній подачі енергії від відновлюваного джерела (попередньо перетворена інверторами) в загальну мережу змінного струму, що дозволить у разі відсутності струму через масовані атаки інфраструктурних об’єктів користуватися енергією із заряджених резервних батарей відновлюваними джерелами. Однозначно, що переформатування станцій у нинішніх невизначених умовах дозволить використовувати накопичену енергію за нормальних умов в пікові години навантаження на мережу. Користь за рахунок гібридних мереж є високою за рахунок енергоефективності та високої стійкості, а також можливості керування штучним інтелектом дизель-генератора, що вмикається за потреби через зниження до мінімально допустимого значення напруги акумулятора (зазвичай менше 12%), що й в додачу, мінімізує інвестиційні витрати та оптимізує капітальні та операційні витрати.

Міжнарожний альянс “Zero Waste” фокусується на управлінні з “нульовими відходами” та цінності ресурсів, стверджуючи, що таке управління

забезпечуватиме стійкість природного капіталу для майбутніх поколінь. Концепція “ZeroWaste”, зосереджується на збереженні наявних ресурсів, дотриманні принципу відповідальності у виробництві, споживанні, вторинному використанні й, за можливості, відновленні ресурсів та продуктів,пакування та матеріалів, виключаючи спалювання, викиди в повітря, злив у воду, що несе загрозу здоров’ю населення та навколишньому середовищу [189].

У сфері інформаційно-комунікаційних технологій започатковано мережу C-SERVEES, яка спрямована на активацію циркулярних послуг в електричному та електронному секторі шляхом розробки, тестування, перевірки та передачі нових циркулярних економічних бізнес-моделей на основі системних еко-інноваційних послуг, які включають [189189]:

– еко-лізинг електричного та електронного обладнання (EEO);

– персоналізація продукту;

– покращене управління відходами електричного та електронного обладнання (WEEE);

– та послуги ІКТ для підтримки інших екологічних послуг.

Інструменти ІКТ (на основі QR-кодів) розроблятимуться як рушійна сила запропонованих еко-інноваційних послуг з метою використання потенціалу та синергії новітніх революцій сучасності: recycline (циркулярної) економіки та Індустрії 4.0.

Мережа C-SERVEES відкриватиме нові можливості для споживачів ЕК послуг (участь у розробці, доступ до продукту як послуги) Техніко-економічна, екологічна та соціальна спроможність нових бізнес-моделей циклічної економіки буде підтверджено шляхом демонстрації можливостей використання ЕК обладнання, телевізорів [190].

Друга стратегія – *операційна ефективність та стійкість дозволить* вирішити виклик операційних збоїв – 0,2, орієнтована на:

– планування безперервності бізнесу шляхом розробки надійних планів безперервності бізнесу для забезпечення надання послуг під час кризових ситуацій.

– гнучкість інтелектуального капіталу (персоналу) через впровадження гнучкого графіку роботи та можливість віддаленої роботи, щоб підтримувати діяльність під час збоїв.

– управління ланцюгами постачання за рахунок підвищення стійкості ланцюга постачання через диверсифікації постачальників та створення планів на випадок непередбачуваних ситуацій для критично важливих компонентів.

Із метою задоволення потреб споживачів у інформатизації, а також потреб держави у побудові інформаційного суспільства на законодавчому рівні регулюються питання щодо доступу та використання електроенергетичних об’єктів, акцентується увага на інвестуванні інфраструктурних галузей задля посилення ролі в економіці сфери послуг, щоб сприяти зростанню макроекономічних показників, добробуту населення.

Реалізація даних стратегічних напрямів розвитку надасть можливість скоротити час простою та швидше відновлюватися після збоїв, підвищити операційну стабільність та задоволеність клієнтів, покращити адаптивність до мінливих умов.

Третій стратегічний напрям націлений на *посилення заходів кібербезпеки та вирішує проблему загрози кібербезпеки (0,15),* вбачається у реалізації заходів:

– інвестування в безпеку для збільшення вкладень в інфраструктуру кібербезпеки, включаючи брандмауери, шифрування та системи виявлення вторгнень;

– навчання персоналу (інтелектуального капіталу) та обізнаність шляхом проведення регулярних тренінгів та інформаційних програми з кібербезпеки для працівників, щоб зменшити ризики людських помилок [372].

– реагування на кіберінциденти та атаки за рахунок розробки та регулярного оновлення планів реагування на інциденти для оперативного реагування та відновлення після кібератак.

Позитивними змінами відзначатимуться питання захисту від кіберзагроз, які на сьогодні, як нами було визначено, є однією із глобальних проблем та вважається серйозною загрозою для безпеки підприємства; зниження ризику витоку даних та перебоїв у наданні послуг; підвищення довіри клієнтів та впевненості в наданні кібербезпечної послуги [375].

Слід зважити на відсоток порушень кібербезпеки, що припадає на на людський фактор – близько 95% порушень кібербезпеки пов'язані із низькою поінформованістю персоналу щодо загроз, зокрема інформаційних, тому вирішення питання безпеки через надійні системи захисту та протоколи спостережень щодо можливих атак мають комбінуватися із цифровою обізнаністю персоналу щодо поводження з інформаційними активами підприємств [369].

Нині атаки на підприємства здійснюються у трьох напрямах, а саме: через мережеві пристрої, вебресурси, а також людей. Такі атаки найбільше загрожують підприємству, оскільки поєднують техніко-технологічні й соціальні вразливості, що призводить до максимально руйнівного ефекту. До таких атак відноситься Advanced Persistent Threat (APT) – досконала стійка загроза, що характеризується сукупністю дій зловмисника, за якими вибудувано ланцюг, що формує його стратегію та тактику, щоб досягти порушення цілісності, конфіденційності, захищеності інформації. Але сценарій таких атак передбачає, що дії зловмисників будуть поступовими та розтягнутими, тож можуть відбуватися непомітно. Зазначається, що для досконалих стійких загроз є характерним складний набір взаємозв'язаних дій зловмисника щодо часу та простору. Самі дії можуть не викликати підозр, оскільки підготовка до цілеспрямованої атаки підприємства-жертви може тривати від кількох місяців та сягати понад один рік [383], причому засоби досягнення використовуються різні, а сама тактика (або їх кількість та

комбінації) залишається перманентною. Тому захист має ґрунтуватися на виявленні атак, що спрямовуються на технології, а також персонал, який має добре орієнтуватися у питаннях соціальної інженерії та вміти вчасно розпізнавати соціального інженера, який використовує слабкі (вразливі) місця людини для швидкого отримання необхідної інформації. Убезпечити персонал від подібної загрози та сформувати його стійкість до дій зловмисників можливо лише за розуміння ймовірних сценаріїв поведінки соціальних інженерів [321]. Підтверджується важливість дослідження поведінки персоналу та користувачів, які мають доступ до інформації, для можливості їх захисту від зловмисників, які за використання знань про вподобання або слабкості людей, або під дією тиску на них, потрапляють у коло їх довіри, що дозволяє отримувати інформацію легко, без застосування складних технічних комбінацій, прийомів, засобів.

На сьогодні соціальна інженерія реалізується, як правило, віддалено засобами сучасних інформаційно-комунікаційних засобів шляхом використання інтернету та телефону, рідше – особистий контакт, оскільки важче вводити людину в оману безпосередньо спілкуючись із нею.

Слід зазначити, що у переліку категорій кіберінцидентів (розроблений з використанням та відповідає рекомендації ENISA Reference Incident Classification Taxonomy (Європейської агенції з кібербезпеки)), документу Common Taxonomy for Law Enforcement and The National Network of CSIRTs та Європейського центру боротьби з кіберзлочинністю Європолу) знаходимо серед інцидентів “шахрайство” – фішинг, який відноситься до інструментів соціальної інженерії, що підтверджує частоту атак даного виду [385].

Використання традиційних засобів захисту таких, як антивіруси, міжмережеві екрани, системи запобігання вторгненням не забезпечують цілковитий захист від внутрішніх порушників, що обумовлює необхідність застосування комбінованих та системних інструментів контролю діяльності користувачів [386]. Слід підкреслити важливість вивчення дії людського фактора та моніторингу й аналізу діяльності користувачів, оскільки

маніпулювання вразливостями людини (слабкості, потреби, манії (пристрасті), захоплення) призводить до нової моделі її поведінки, створення сприятливих умов реалізації загроз безпеці інформації і, як наслідок, зменшенню здатності систем захисту інформації протидіяти їх впливові. Саме тому, загроза використання соціальної інженерії є однією з найбільш небезпечних у кіберпросторі та у цілому для підприємств [387].

Нині, у соціальних мережах легко отримати інформацію про вподобання, роботу, захоплення, цілі та прагнення людини, тому персонал стає вразливим до дій соціального інженера, який чинить атаку. Доступ до інформації за соціоінженерним підходом представлено на рис. 5.20.

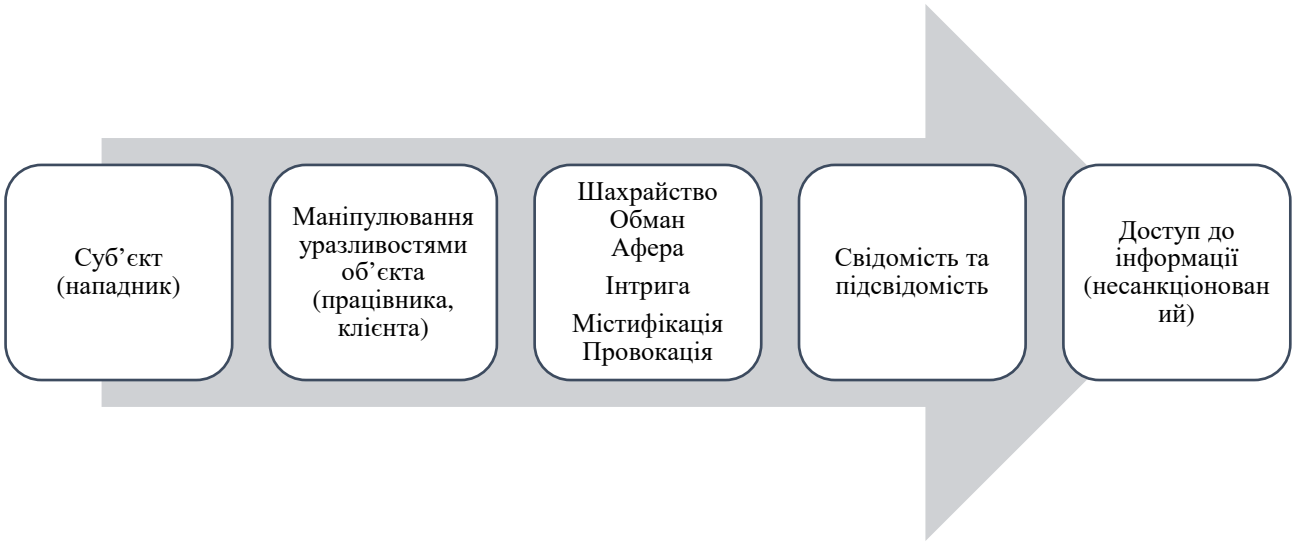


Рис. 5.20. Доступ до інформації за соціоінженерним підходом

(складено автором [385; 386])

Загроза – соціальна інженерія полягає у маніпулятивному впливові на свідомість (підсвідомість) людини через властиві їй уразливості (довірливість, страх, жадібність, відкритість, зверхність, милосердя).

Основою використання методів соціальної інженерії є:

– особливості, що керують людською свідомістю;

– аудиторія або поле діяльності;

– некомпетентність аудиторії у визначених термінах і предметних областях у сфері інформаційної безпеки;

– нестійкість психологічних властивостей особистості, що характеризуються поведінковими стереотипами. Їх можна використовувати для маніпулювання через основні потреби, слабкості, бажання, ідеали.

Рис. 5.21. Підсистеми системи управління інформаційними ризиками підприємства з урахуванням атак соціального інженера *(складено автором [385;386])*

Підсистема захисту інформації (рис. 5.21) передбачає виявлення інформації, що підлягає захисту, визначення місць зосередження та носіїв інформації, яка підлягає захисту, визначення можливих способів несанкціонованого доступу до такої інформації, розроблення й упровадження організаційних, правових, технічних, програмних, криптографічних та апаратних засобів захисту інформації.

Функціями цієї підсистеми є:

– формування комплексу організаційних, технічних, апаратних, криптографічних заходів і забезпеченння гарантованого захисту від посягань на електронну інформацію підприємства;

– забезпечення контролю за носіями інформації, своєчасне реагування на всі порушення в захисті інформації, що зберігається та функціонує в інформаційних мережах підприємства;

– запровадження надійної системи документообігу в підприємстві;

забезпечення надійної охорони підприємств, особливо з точки зору виключення можливості несанкціонованого доступу до них та викрадення документів чи електронних носіїв інформації

Саме фішинг, як зазначалося вище, внесений до переліку категорій кіберінцидентів, який розроблений з використанням рекомендацій ENISA Reference Incident Classification Taxonomy (Європейської агенції з кібербезпеки) [389], що підтверджує його вагу у структурі інцидентів загроз безпеці даних та інформаційним ресурсам з використанням як техічних засобів, так і впливу на працівника, який має доступ до інформації.

Урахування впливу інформаційних атак на персонал гарантуватиме посилення безпеки функціонування підприємства та унеможливить фінансові втрати від кіберзагроз, які можуть виникнути у результаті реалізації дій зловмисника, за якими вибудувано ланцюг його стратегії та тактики, спрямований на порушення цілісності, конфіденційності, захищеності інформації під час досконалих стійких загроз стосовно персоналу.

Крім того, слід врахувати, що сьогоднішні невизначені умови суттєво впливають на психоемоційний стан персоналу, на прийняття ним рішень та поведінку в критичних ситуаціях. Важливим є сприйняття працівниками кризових ситуацій, їх стресостійкість та реакція на деструктивні зміни, готовність до вирішення проблем. Обізнаність персоналу у таких питаннях, як: безпека, захист інформації та відстеження потенційних загроз дає йому змогу чітко окреслювати проблеми, оцінювати ступінь небезпеки, ранжувати ризики та загрози, шукати шляхи їх усунення. Вагому роль у правильній інформованості персоналу щодо небезпек відіграє керівник вищого рівня – CISO (Chief Information Security Officer), який здійснює нагляд за інформаційною, кібер- та технологічною безпекою організації, працює разом з керівництвом компанії, бізнес-менеджерами, командами кібербезпеки та IT-менеджерами для ефективного моніторингу та підтримки безпеки додатків, баз даних, комп’ютерів, вебсайтів своєї організації. Такі керівники також відповідають за створення політики безпеки на рівні підприємства, розроблення

планів стійкості до витоків даних, здійснюють нагляд за комунікаціями щодо оновлення систем управління безпекою.

Аналіз процесів та явищ навколо, що стосуються зовнішнього та внутрішнього оточення, дозволяє виявити виклики, мінімізувати ризики та упередити появу загроз, які призводять до небезпек. Беручи до уваги безпеку інформації як фактора виробництва, виокремлюють такі складові інформаційної безпеки: безпека інформаційних ресурсів; безпека інформаційної інфраструктури, безпека інформаційного поля.

Безпека інформаційних ресурсів полягає у збереженні інформації від несанкціонованого розповсюдження, використання та порушення конфіденційності. Безпека інформаційної інфраструктури полягає у такому стані захищеності електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, мереж електрозв'язку підприємства, за якого забезпечується цілісність інформації, що в них обробляється (зберігається чи циркулює). Безпека "інформаційного поля" ґрунтується на контрольованості здебільшого несистематизованих потоків інформації, що оприлюднюється різноманітними учасниками інформаційних відносин: телерадіоорганізаціями, друкованими засобами масової інформації, інтернет-виданнями, конкурентами, органами державної влади, місцевого самоврядування тощо.

За сьогоднішніх посягань на роботу підприємств ПЕКМП, захист їх роботи у напрямку формування безпечного та безперебійного надання послуг надважливий. Потрібно здійснювати постійний пошук варіантів можливих заходів, засобів, інструментів безпеки, залучаючи при цьому організації, які ефективно борються із загрозами у світовому масштабі. За результатами досліджень компанії IBM нині слабко використовується штучний інтелект безпеки (28% організацій), автоматизованість дій з ідентифікації загроз у мережі теж низька, що сповільнює реакцію підприємств на загрозу та її упередження. Вбачається, що штучний інтелект безпеки та автоматизація суттєво скорочують втрати підприємств, оскільки зростає ефективність кібербезпеки підприємств (рис. 5.22).

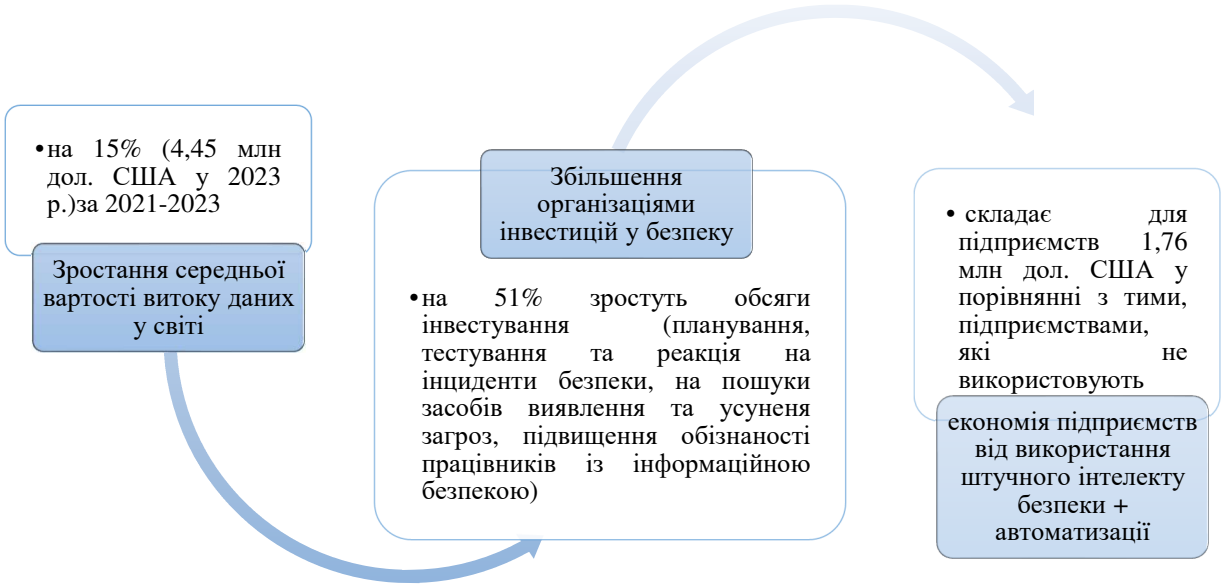


Рис. 5.22. Зменшення ризиків та мінімізація втрат підприємств від використання штучного інтелекту безпеки та автоматизації

(складено автором за [391])

До проблем безпеки даних підприємств ПЕКМП додається використання хмарних сервісів, на які припадає 82% викрадень даних. Інформація – важливий ресурс для підприємств, тому надаючи послугу із її передачі, обробки, зберігання підприємства ЕК мають захищати дані у процесі переміщення у хмарному середовищі (між хмарами, базами даних, програмами, службами).

З метою розвантаження IT-відділу від зростаючої кількості завдань безпеки інформаційної інфраструктури, підприємства користуються послугою SECaaS (Security as a Service) – безпеки як послуги. Постачальники безпеки як послуги повинні відповідати наступним критеріям: SecaaS включає продукти або послуги безпеки, які надаються як хмарні служби, крім того, відповідати основним характеристикам NIST для хмарних обчислень. Також спостерігається зростання світового ринку безпеки як послуги (SECaaS), за оцінками 2022 року розмір ринку складав 10,2 млрд дол. США, вважається, що у 2033 році він складе понад 81 млрд дол. (прогнозовані дані) [394]. Попит на дані послуги зростатиме через переміщення даних у хмару та підвищення інтересу до масивів даних, що

Слід звернути увагу на виклик, перед яким постає світ – квантові атаки, які виникають на основі спродукованих квантовими ком'ютерами алгоритмами.

Галузями, що мають приділити увагу захисту даних є фінансова сфера (захист фінансових послуг), а також критичної інфраструктури, серед якої на Міжнародному економічному форумі озвучено сферу електронних комунікацій.

Компанією GSMA опублікувано звіт "Оцінка впливу пост-квантових телекомунікаційних мереж", в якому відображено оцінку впливу на електронні комунікаційні мережі після впровадження квантових технологій, а також керівні принципи для управління квантовими ризиками для компаній сфери ЕК. У звіті вказано, що підприємства-постачальники електронних комунікаційних послуг відіграють вагому роль у захисті доступності власної інфраструктури, а також конфіденційності та цілісності даних споживачів послуг зв'язку, як підприємств, так і для фізичних осіб, тобто йдеться про забезпечення квантової стійкості інфраструктури.

В загальну стратегію кібербезпеки має інтегруватися квантова стратегія, яка грунтуватиметься на:

– інвентаризацію поточних криптографічних активів для розуміння профілю ризиків і визначення пріоритетів критично важливих активів або систем;

– планування переходу на наступне покоління криптографічних алгоритмів, які будуть стійкими до атак, а також на контроль якості.

– впровадження криптоспроможності для забезпечення кіберстійкості (оновлення алгоритмів або технологій).

Дотримання стандартів NIST (Національний інститут стандартів і технологій) підвищує кіберспроможність підприємств, тому впровадження стандартів на підприємствах має регулюватися та забезпечуватися, контрулювтися на державному рівні. Крім того, на чолі з NIST розробляється програма з пошуку, оцінки і стандартизації квантово-стійких криптографічних

алгоритмів з відкритим ключем (також широко відомих як постквантова криптографія або PQC), поява стандартів яких планується на 2024 рік [394].

Четверта стратегічний напрям націлений на *посилення регуляторної відповідальності та адвокації, вирішує проблему регуляторної невизначеності* (0,1), досягнення безпеки за якою вбачається у:

– активній взаємодії з регуляторними органами для врахування потенційно можливих змін та виступати за сприятливу політику розбудови цифрової економіки та надійної, ефективної інформаційно-комунікаційної інфраструктури підприємств-постачальниківелектронних комунікаційних мереж;

– впровадженню комплексні програми комплаєнсу для забезпечення дотримання чинного законодавства, нормативно-правового регулювання питань щодо функціонування підприємств сфери інфокомунікацій;

– активна участь у програмах та проєктах, формуванні стратегій розвитку сфери ІКТ за рахунок участі у роботі галузевих асоціацій, прийнятті рішень для впливу на формування політики та сприяння розвитку сприятливого регуляторного середовища.

Стратегія відкриває можливості для покращення узгодження з правовими та регуляторними вимогами, зменшення ризику недотримання правил та регуляторних політик, підвищує здатність впливати на сприятливі регуляторні результати.

П’ятий стратегічний напрям *сприятиме налагодженню економічної адаптивності та зростання, спрямована на вирішенню виклику економічної нестабільності* (ЕН) – 0,25 та передбачає:

– диверсифікацію джерел надходжень шляхом вивчення нових ринків та послуг, таких як цифрові фінансові послуги, платформи електронної комерції та рішення для “розумного міста”;

– управління витратами, що передбачає управління витратами для підтримки фінансовой стабілізації під час економічних спадів та утримання підприємства цільового рівня платоспроможності;

– клієнтоорієнтованість, що передбачає розробку цільових (таргетованих послуг) та цінових стратегій для різних сегментів клієнтів, включаючи домогосподарства та підприємства з низьким рівнем доходу.

Реалізація даного плану стратегії сприятиме підвищенню стабільності доходів та потенціалу для розвитку, посилюватиме здатність витримувати економічну нестабільність, що наразі особливо відчуваються за рахунок валютних коливань, зростанню рівня проникнення на ринок та розширення клієнтської бази. Індекс цін постачальників поштових та комунікаційних послуг за категоріями в 2023 р. представлено у табл. 5.4.

Таблиця 5.4

Індекс цін постачальників поштових та комунікаційних послуг за категоріями в 2023 р. (%)

Категорія послуг	I кв.	II кв.	III кв.	IV кв.	За рік
Діяльність національної пошти	101,5	100,7	101,8	100,7	104,8
Інша поштова та кур'єрська діяльність	105,2	102,5	106,3	102,3	117,3
Електрозв’язок	104,9	101,7	101,6	101,3	109,8

(складено автором за [410])

Клієнтоорієнтовність вказує на потребу задоволення потреб споживача у послугах зв’язку, сформовану за інтересами споживачів електронних комунікаційних послуг, які теж є стейкхолдерами. Однією із ключових потреб значиться безпечність послуги у частині забезпечення інформаційного та кібернетичного захисту споживачів послуг.

В епоху діджиталізації постало питання посилення безпеки та конфіденційності даних кілєнтів, обрання належних заходів безпеки: техніко-технологічного, фізичного, організаційного спрямування. Паралельно цифровізація та доступ до Інтернету, як загальнодоступної послуги, має відповідати наступним принципам: інклюзивність; відсутність дискримінації; та, знову ж таки, безпечність.

Доступ до мережі інтернет має відбуватися безперешкодно, незалежно від того, хто його потребує, територіальної, етнічної приналежності, переконань політичних та релігійних, фізіологічних особливостей (інклюзія). Нейтральність вбачається у тому, що користувач сам обирає програмне забезпечення, технології, застосунки, браузер, яким користуватися.

Що стосується інституційного забезпечення, ЗУ “Про електронні комунікації” [378] також визначається, яким чином регулюється питання щодо сприяння інтересам кінцевих споживачів послуг електронних комунікацій (рис. 5.23)

Сприяння інтересам стейкхолдерів (кінцевих користувачів послуг ЕК)					
створення умов для розвитку, доступності і використання електронних комунікаційних мереж високої та надвисокої пропускної здатності, у тому числі мереж фіксованого, мобільного зв’язку та безпроводового доступу, а також електронних комунікаційних послуг	створення умов для отримання максимальної користі під час вибору електронних комунікаційних послуг за ціною і якістю шляхом забезпечення ефективної конкуренції	підтримка безпеки електронних комунікаційних мереж і послуг	забезпечення потреб споживачів в універсальних електронних комунікаційних послугах, у тому числі щодо їх цінової доступності для вразливих соціальних груп споживачів	забезпечення захисту прав та законних інтересів споживачів шляхом нормативно-правового регулювання	забезпечення вибору та рівноцінного доступу до електронних комунікаційних послуг осіб з інвалідністю

Рис. 5.23. Регулювання питань щодо сприяння інтересам споживачів у сферах електронних комунікацій та радіочастотного ресурсу.

(складено автором за [378])

Інтереси користувачів послуг електронних комунікацій регулюються державою та вбачаються у:

– створенні умов розвитку та доступності використання електронних комунікаційних мереж;

– конкуренції для можливості обрання електронних комунікаційних послуг за вигідною ціною;

– наданні універсальних електронних комунікаційних послуг населенню;

– захисті прав та законних інтересів споживачів послуг;

– інклюзивному підході у забезпеченні доступу до електронних комунікаційних послуг; безпеці мереж та послуг.

Регульовані питання мають враховуватися і, крім того, грунтуватися на принципах [379]:

– забезпечення кожному громадянинові рівні можливості доступу до послуг, інформації та знань, що надаються на основі інформаційно-комунікаційних технологій (ІКТ);

– спрямованості на створення переваг (вигід) у різноманітних аспектах повсякденного життя;

– є механізмом (платформою) економічного зростання завдяки приросту ефективності, конкурентоздатності, продуктивності від використання цифрових технологій.

За першим принципом визначається універсальність послуг зв'язку та потреба розбудови стійкої інфокомунікаційної інфраструктури сфери електронних комунікацій, розвитку мережі та забезпеченості споживачів е-послугами та е-сервісами.

Належна увага має приділятися безпеці, яка забезпечується через захист від несанкціонованого доступу, протиправного доступу, викривлення даних, їх використання та розповсюдження, що має контролюватися на початковому рівні постачальником та контролером. У глобальній мережі безпечність даних, конфіденційність інформації, захист персональних даних регламентується Конвенцією 108, статтею 7 [380].

Стратегічно важливим є питання якості електрозв'язку, як пріоритету у виборі споживачем постачальника послуг електронних комунікацій (або їх пакету). За результатами аналізу швидкості передачі Інтернет-мережею (у р.4 роботи), нами отримані значення нижчі (завантаження даних), ніж у країнах Європи, враховуючи націленість на конвергентність мереж постачальників

послуг, нещодвано ухвалений Закон України (реєстраційний номер 10265) щодо приєднання України до єдиної роумінгової зони (“Роумінг як вдома”), що актуалізує питання якості надання інтернет-послуг, пріоритетності заходів щодо підвищення рівня якості послуги.

Від якості наданих послуг зв’язку залежить виконання тих чи інших функцій окремих господарюючих суб’єктів та сектору загального державного управління, адміністративних послуг, освітніх послуг, саме тому, важливо приділяти увагу питанням щодо якості їх надання, відслідковувати показники, що визначають їх рівень, щоб вчасно усувати виявлені недоліки або невідповідність щодо нормативів їх надання, а саме:

1) Показники (параметри) якості доступу до мережі передачі даних загального користування (МПДЗК): показники (параметри), що характеризують доступ до передачі даних загального користування;

2) Показники (параметри) якості послуг із передачі даних і доступу до Інтернету: показники, які характеризують доступність послуг із передачі даних і доступу до Інтернету; показники, що характеризують повноцінність надання послуг;

3) Показники (параметри) якості обслуговування споживачів: показники, які характеризують надійність надання послуг; показники, які характеризують проведення нарахувань за послуги; показники задоволеності споживачів обслуговуванням.

Проаналізувавши затверджені Державною службою спеціального зв’язку та інформатизації України показники якості із передачі даних, доступу до Інтернету та їх рівнів. Відповідно до Положення про якість послуг ЕК, параметри якості послуги – це значення, отримані в результаті вимірів, опитувань або за даними статистичної звітності, за допомогою яких оцінюються показники якості [313]. Показники якості послуги – значення, отримані в результаті розрахунків з параметрів якості, що характеризують відповідність рівня якості вимогам користувачів, технічним вимогам до робочих характеристик мережі зв’язку та вимогам, закріпленим в договорах між

оператором зв'язку та абонентом [313]. За стандартом ISO 8402:1994, якість послуги (Quality-of-service, QoS) – сукупність характеристик послуги електронних комунікацій, що відносяться до здатності задовольнити встановлені і передбачувані потреби користувача послугою (визначення запозичене зі стандарту ISO 8402 [399].

Щодо рівнів показників якості, то вони мають виконуватися в нормальних умовах функціонування та роботи мережі постачальника електронних мереж (тобто в у мовах невизначеності не беруться до уваги), а також незалежно від технологій, які застосовуються в мережі. Параметричні дані для визначення та оцінки якості надання послуги Інтернет (передачі, доступу до Інтернет) наведено в табл. 5.5.

Таблиця 5.5

Рівні показників якості надання Інтернет послуг (передача, доступ)

Параметри		Рівень параметра
Якості доступу до мережі передачі даних загального користування (МПДЗК)	($T_{нчвз}$)	до 24 робочих днів
	$Q_{звнч}$)	> = 85%
Якості послуг із передачі даних і доступу до Інтернету	$Q_{прм}$ - передачі даних; - доступ до Інтернету	 > = 90% > = 90%
	$Q_{відм}$ - передачі даних - доступу до Інтернету	 < = 10% < = 10%
	$T_{нпрм}$ - передачі даних; - доступу до Інтернету	 < = 30% < = 30%
	$Q_{чвзв}$ - передачі даних; - доступу до Інтернету	 > = 90% > = 90%
	$R_{нршп}$	> = 56 кбіт/с
	$Q_{нзшп}$ - передачі даних; - доступу до Інтернету	 < = 10% < = 10%
	$T_{пер}$ - передачі даних; - доступу до Інтернету	 не досліджено не досліджено
Якості обслуговування споживачів	$T_{чупн}$	< = 24 години
	$Q_{зупн}$	> = 65%
	$Z_{зупл}$	< = 0,8
	$Q_{зикр}$	< = 1%
	$Q_{зоао}$	< = 1%
	$Q_{зтао}$	< = 1%

(складено автором)

Зрозуміло, що при проведенні експертної оцінки якості надання послуг електронних комункацій, ключову роль відіграє саме споживач, він дає змогу комплексно підійти до формування уявлення та оцінки якості послуги. Використовуючи добре відомий метод оцінки за Парето, з врахуванням вражень споживачів, можна визначити вагомі причини та ступінь їх впливу на оцінку якості послуг електронних комунікацій (табл. 5.6)

Таблиця 5.6

Кумулятивна вага причин погіршення якості надання Інтернет-послуги підприємством-постачальником зв'язку (передача, доступ)

Параметр якості	Питома вага скарги, %	Вага проблеми (кумулятивно),%
(Тнчвз)	21,21	21
Qпрм (передачі даних)	15,15	36
Qвідм (передачі даних)	9,09	45
Qнзшп (передачі даних)	9,09	55
Qзтао	9,09	64
Qвідм (доступ до Інтернет)	6,06	70
Тнпрм (доступ до Інтернет)	6,06	76
Zзупл	6,06	82
Qзвнч	3,03	85
Qпрм (доступ до Інтернет)	3,03	88
Тнпрм (передачі даних)	3,03	91
Qзупн	3,03	94
Qзнкр	3,03	97
Qзоао	3,03	100

(розраховано та складено автором)

За отриманими в результаті розрахунків даними (що отримані з урахуванням опитування серед користувачів послуг електронних комунікацій: доступу та передачі даних через Інтернет), для більшої наочності побудовано

діаграму Парето з метою визначення ступеня впливу окремих показників на якість надання послуги ЕК (надання доступу та передачі даних через Інтернет) (рис. 5.24.).

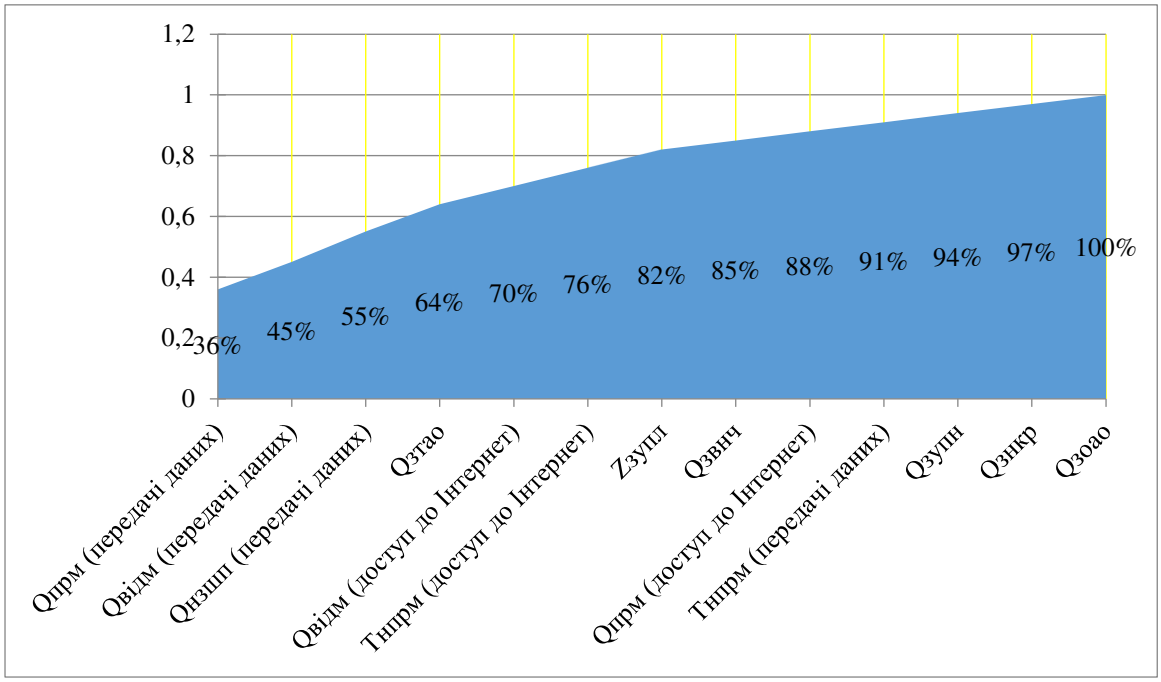


Рис. 5.24. Кумулятивна крива визначення вагомості впливу показників на якість послуги електронних комунікацій (доступ та передача даних через Інтернет)

(складено автором)

За ступенем вагомості впливу на якість послуг виокремлюються 3 групи визначених причин:

1) Найбільш вагомі (А) – до 70%: нормований час виконання заяви на підключення кінцевого обладнання споживачів до мережі передачі даних загального користування; відсоток успішних реєстрацій у мережі (передача даних); відсоток незадовільних з'єднань за швидкістю передачі даних (передачі даних); відсоток звернень щодо технічних аспектів обслуговування; відсоток відмов (доступ до Інтернет).

2) Проміжкові або середньої вагомості (В) – 20%: нормований час реєстрації в мережі (доступ до Інтернет); кількість заяв про пошкодження

МПДЗК із розрахунку на одну лінію доступу за рік; коефіцієнт вчасності підключення; відсоток успішних реєстрацій у мережі для послуг (доступ до Інтернет); нормований час реєстрації в мережі (передачі даних).

3) Найменш вагомі (В) – 10%: відсоток заяв про пошкодження мережі передачі даних загального користування, виконаних за нормований час; відсоток рахунків, на які були отримані звернення від споживачів щодо їх некоректності (неправильності); відсоток звернень щодо організаційних аспектів обслуговування.

Вищенаведене ранжування дозволить запровадити комплекс заходів щодо усунення проблем, що впливають на якість послуги електронних комунікацій (доступ та передача даних через Інтернет). Першочергово необхідно усунути недоліки зони А, як найбільш важливі і значущі. Для підтримки належної якості надання послуги ЕК в умовах невизначеності, підприємства ПЕКМП мають постійно проводити експертну оцінку якості надання послуг і впроваджувати заходити щодо усунення проблемних питань (параметрів групи А).

Оцінка вагомості впливу показників на якість ЕК послуги (доступ та передача даних через Інтернет) з врахуванням сприйняття споживачем наданої послуги, надає змогу виокремити найбільш вагомі (проблемні), які займають левову частку у формуванні комплексного показника вражень щодо якості надання ЕК послуги оператором або провайдером. В подальшому це дозволить окреслити, які із показників якості є нагальними для вчасного їх усунення та забезпечення безперебійної та бездоганної роботи постачальника послуг електронних комунікацій, що надає послугу з доступу та передачі даних через Інтернет. Тобто, за умови проведення вчасної та вдалої експертної оцінки якості наданих послуг, уможливлюється збереження позитивних вражень споживачем послуг електронних комунікацій. [400].

Отже, за результатами досліджень вбачається потреба у вирішення питання безпечного та стабільного функціонування інфраструктурних об’єктів за використання системи контролю загроз.

Використання систем контролю загроз підприємств критичної інфраструктури є доречним заходом, оскільки в нинішніх умовах невизначеності надає можливість упередити кібернетичні та фізичні загрози, що виникають у результаті наслідків бойових дій, які ведуться на території нашої країни. Захисту мають підлягати всі підприємства, а особливо – критично важливі об'єкти та підприємства.

При розробці планів та політик безпеки на підприємствах зв'язку доцільно розпочинати забезпечення цифрової обізнаності (нами пропонується кіберспроможність) персоналу підприємства. Далі продовжуючи аналізом даних, які отримані в результаті витоку інформації від потенційних джерел (персонал, технології), закінчуючи послідовним рухом до ідентифікації ризиків. При чому паралельно проводиться оцінка ризиків з урахуванням техніко-технологічних та соціальних вразливостей із подальшим окресленням подій за ступенем дії та ймовірністю настання для визначення швидкості реагування на порушення (середній час виявлення загрози, середній час реакції на загрози) та розробленням плану реагування.

Врешті-решт, за використання системи контролю загроз після ідентифікації ризиків, усунення загроз та ліквідації їх негативної дії діяльність підприємства стабілізується, що допоможе йому перейти із небезпечного стану функціонування в безпечний (рис. 5.25).

Доцільним у процесі формування заходів безпеки, політики безпеки для підприємств є розрахунок показників ефективності (особливо окупності інвестицій в безпеку), які визначаються після закінчення руху у напрямку від викликів до загроз та повернення підприємства до стабільного, безпечного стану.

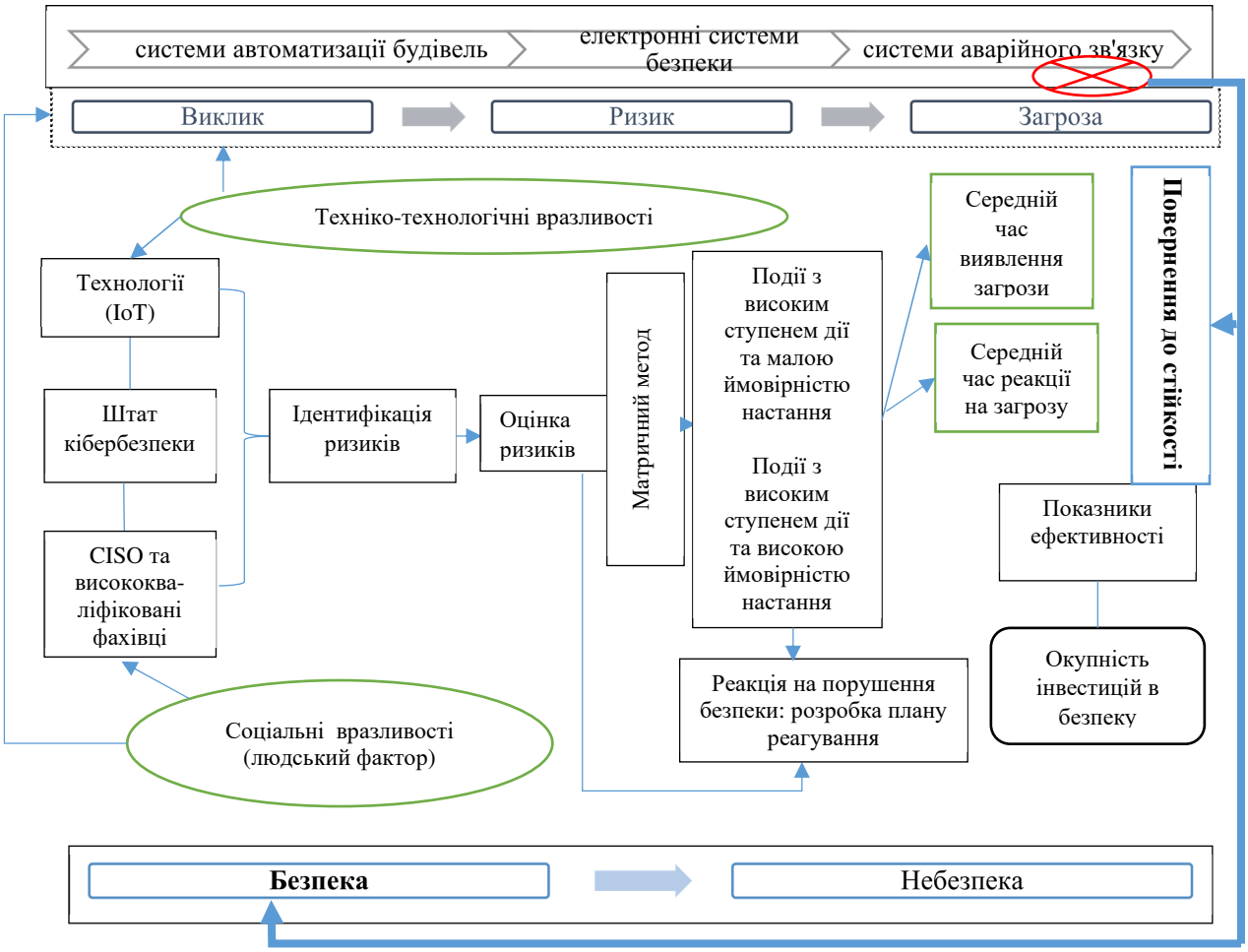


Рис. 5.25. Вектор безпеки підприємства у сучасних невизначених умовах за використання системи контролю загроз

(авторська розробка)

Результативність діяльності структурного підрозділу підприємства з економічної безпеки є важливою, оскільки визначає:

– міру наближення фактичного рівня економічної безпеки підприємства до запланованого (встановленого або бажаного);

– міру наближення кількості виявлених потенційних та реальних загроз діяльності підприємства до їх реальної кількості;

– точність визначення ймовірності реалізації загроз діяльності підприємства;

– точність визначення наслідків реалізації загроз діяльності підприємства.

Ефективність є найважливішою характеристикою результатів функціонування об’єкта або системи, будь-якого процесу, що визначається співвідношенням ефекту до витрат ресурсів на його досягнення.

Показники, що описують результати діяльності структурного підрозділу підприємства з економічної безпеки такі:

– показник “величина відвернених збитків”, який відображає ефективність діяльності структурного підрозділу підприємства з економічної безпеки у ретроспективі, але його складно визначити на майбутній (або планований) період.

– величина відвернення недоотриманого прибутку (прибутку, який вдалося отримати завдяки тому, що працівники цього структурного підрозділу своєчасно звернули увагу на загрозу недоотримання прибутку та здійснили низку безпекозабезпечувальних заходів.

Важливим у процесі виявлення стану безпеки (небезпеки) є зворотний зв’язок, який у системі управління інформаційною безпекою дає змогу не тільки виявити окрему загрозу, а й відреагувати на цілий ряд подій, на перший погляд ніяк між собою не пов’язаних.

У цьому можуть допомогти продукти, що забезпечують централізоване зіставлення даних журналів подій з мережевих пристроїв і систем безпеки в режимі реального часу, шляхом автоматичного зіставлення даних та виділення подій та загроз безпеці, що вимагають вжити рішучих заходів.

Слід підкреслити важливість еволюції інформаційно-комунікаційних технологій, які продовжують забезпечувати високий рівень взаємопов’язаних та цифрових і електронних операцій у межах безпеки на всіх рівнях: мікробезпеки (підприємства), мезобезпеки (регіонів), макробезпеки (держави).

Окрім звичайних складових економічної безпеки (фінансової, техніко-технологічної, виробничої, енергетичної, ринкової, інтелектуальної, кадрової, інтерфейсної, інформаційної, фізичної (силової), політико-правової, екологічної, інформаційно-інноваційної) доцільно ввести електронно-комунікаційну [85]. Пояснення цьому випливає із розглянутого вище –

переходу суспільства та підприємств у цифровий світ із використанням IoT (Internet of Things – Інтернету речей), метапростору, квантових комп'ютерів. Тому техніко-технологічний та електронно-комунікаційний захист підприємств постане як необхідність, змушуючи суб'єктів мікро-, мезо-, макрорівня адаптуватися до новітніх змін, пристосовуватись та застосовувати дієві інструменти, вживати заходів безпеки.

Звісно, що може виникати безліч загроз одночасно, особливо, якщо це сплановані досконалі стійкі загрози. Інколи вектори загроз можуть перетинатися, накладаючись один на одного та викликаючи безліч варіантів подій, на які потрібно реагувати по-різному, розробляти індивідуальні плани реагування стосовно кожної із загроз. Однак нині на допомогу приходить штучний інтелект.

Застосування штучного інтелекту дозволить працювати ефективніше та гарантувати безпеку підприємства, адже виявлення порушень у результаті загроз, збір, аналіз даних, їх обробка, пошук алгоритмів щодо майбутніх тенденцій і варіантів подій відбувається в режимі реального часу. Рішення про те, як налаштувати параметри, щоб оптимізувати роботу підприємства, прийматимутися миттєво.

Використання AI (Artificial intelligence, штучний інтелект) у системах автоматизації будівель може надати низку переваг: підвищення енергоефективності, безпеки та комфорту працівників; скорочення витрат на технічне обслуговування (за рахунок виявлення проблеми до завдання ними руйнівної шкоди).

Розвиток технологій штучного інтелекту сприяє його інтегруванню в системи автоматизації на підприємствах, як результат – ефективне управління будівлями та ефективна, рентабельна робота підприємства.

Автоматизований аналіз даних на основі використання штучного інтелекту, прогнозне технічне обслуговування можуть допомогти підприємствам зменшити операційні витрати, підвищити продуктивність, а головне – посилити безпеку.

Системи автоматизації будівель підприємства представляють собою централізовані, взаємопов'язані мережі обладнання та програмного забезпечення для того, щоб контролювати і керувати навколишнім середовищем на всіх функціонуючих підприємствах та організаціях. Оскільки існують ризики витоку водню чи радіоактивних речовин або виникнення пожежі, використання систем, що ідентифікують перелічені загрози, убезпечує від невідворотних негативних наслідків.

При формуванні підприємством безпекозабезпечувальної діяльності слід брати до уваги положення Директиви ЄС SEVESO II (96/82/ЄС), за якою промислові оператори (власники) підприємств мають дотримуватися політики щодо запобігання великим аваріям та впроваджувати систему керування безпекою. У Директиві представлено вимоги щодо надання звітів та доповідей про безпеку, а також порядок і розроблення планів на випадок аварії з докладною оцінкою ступеня ризику з урахуванням можливих варіантів аварійних ситуацій [411].

Беручи до уваги інтеграційні процеси України щодо вступу до Євросоюзу та посилення взаємодії із країнами ЄС внаслідок повномасштабного вторгнення РФ на територію України, для нашої країни посилюється зміст Директиви й процес її еволюції. Особливо актуалізується це питання для підприємств критичної інфраструктури, забезпечення захисту яких стає вкрай важливим. До секторів критичної інфраструктури за Постановою Кабінету Міністрів України (2020) відносять: паливно-енергетичний сектор; цифрові технології; захист інформації; системи життєзабезпечення; харчова промисловість та агропромисловий комплекс; державний матеріальний резерв; охорона здоров'я; ринки капіталу та організовані товарні ринки; фінансовий сектор; транспорт та пошта; промисловість; сектор громадської безпеки; цивільний захист населення і територій; міграція; охорона навколишнього середовища; сектор охорони; національна безпека; правосуддя; тримання під вартою; наукові дослідження та розробки; фінансовий сектор; вибори та референдуми; соціальний захист; інформаційні послуги; державна влада та місцеве самоврядування.

Підприємствами, що функціонують у цих секторах (як ми бачимо, їх перелік чималий), враховуючи умови невизначеності, в яких нині перебувають підприємства в Україні, та положення директиви ЄС SEVESO II, доцільною у використанні є система аварійного зв'язку для захисту життя персоналу, населення через інформування про появу надзвичайної ситуації з подальшою передачею інформації (необхідної для полегшення реагування на дії та наслідки) через системи голосового оповіщення про пожежу, двосторонні внутрішньобудинкові системи зв'язку аварійних служб, системи масового оповіщення підприємств, організацій та населення.

Підприємства також мають задіювати електронні системи безпеки, призначення яких полягає у виявленні вторгнень, упередженні крадіжок, контролі доступу, управлінні відео та внутрішнім зв'язком

Варто врахувати доцільність інтеграції стратегій, загальна інтегрованість сфери ІКТ сприятиме швидкому відновленню та розбудові сфери електронних комунікацій [216].

Доцільним є поєднання та взаємоузгодження пропонованих стратегій для створення комплексного плану відновлення, їх загальна інтегрованість спродукує потужномий синергетичний ефект.

Пріоритетними залишатимуться завдання по розбудові та відновленню пошкодженої інфраструктури, нагальність вирішення якого є беззаперечною, оскількі від цього залежить спроможність надавати послугу зв'язку і отримання якісної послуги.

Вирішуючи виявлені проблеми за допомогою цих стратегічних ініціатив, підприємства ПЕКМП в післявоєнній Україні можуть відновити сильніші, стійкіші та інноваційніші операції. Такий підхід дозволить їм не лише оговтатися від наслідків війни, але й вийти на новий рівень розвитку.

Проведене дослідження дозволило визначити безпеку підприємств сфери, електронних комунікацій як один із пріоритетних напрямків розвитку країни, оскільки її відносять до критичної інфраструктури та дана сфера є важливою у забезпеченні нормального функціонування та роботи інших підприємств та

організацій, економічних суб'єктів в нестійких умовах роботи, крім того підприємства ПЕКМП слугують підґрунтям на шляху до євроінтеграції та конвергентності послуг.

Загроза порушення цілісності інформації, втрата її конфіденційності для підприємств особливо зростає в часи криз: економічних, фінансових, або, як сьогодні, воєнного стану. Врахування цього потенційного втручання у роботу підприємства дозволяє упередити потенційні негативні явища, що можуть постати перед підприємством та порушувати його нормальне функціонування та призвести до: кризових явищ, втрат економічних вигід та проявів від загроз поширення інформації, що стосується виробництва, побудови збутової мережі, контрагентів, формування цін та перспективних напрямків розвитку підприємства, актуальних маркетингових досліджень щодо вподобань, розширення асортименту, стратегії розвитку. Саме людський фактор часто стає джерелом витоку інформації через необізнаність, неуважність, низьку інформованість щодо поводження з інформацією та шляхами її отримання зловмисником за допомогою технічних засобів та сконструйованої поведінки.

У результаті аналізу, підтверджується важливість дослідження поведінки персоналу та користувачів, що мають доступ до інформації для можливості їх захисту від зловмисників, які за використання знань про вподобання або слабкості людей, або під дією тиску на них, потрапляють у коло їх довіри, що дозволяє легко отримувати інформацію без застосування складних технічних комбінацій та прийомів, засобів.

Висновки до п'ятого розділу

Проаналізовано виклики управління безпекою підприємства в умовах невизначеності, переважна більшість яких екзогенного характеру та не підлягає впливу з боку підприємства, проведено їх узагальнення вніслідок ведення бойових дій на території України. Основними викликам, що загрожують підприємствам електронних комунікацій є: стихійні лиха та руйнації у результаті бойових дій; втрата електроживлення, неспроможність надання послуг через брак

енергоефективних технологій GPON; кібератаки. Середовище функціонування відзначається невизначеністю через брак інформації щодо майбутнього розвитку подій на території України, тому під постійною загрозою перебувають активи, персонал, операції, ліквідність коспаній.

Позитивно відзначається євроінтеграціний виклик, що створює сприятливі умови для розвитку: перегляд радіочастот для розширення спектру надання послуг за технологією 5G, яка сприяє збільшенню пропускної здатності та зменшення затримок, збільшення швидкості передачі даних, пришвидшення конвергенції, прийняття закону про роумінг Roam Like At Home. Відзначено активізацію кібератак на оборонні та високотехнологічні компанії, проведено їх аналіз, найбільше нападів чинилася із боку Росії, Ірану, Китаю, нанесені збитки вимірювалися в млн та млрд дол. США, проаналізовано масовані кібератаки на українські підприємства та організації ІТ-сфери впродовж 2022-2023 рр, відзначено, що найбільше постраждала компанія “Київстар”.

З урахуванням ускладення аналізу викликів та їх кількісного виміру за умов невизначеності, проведено VUCA і BANI-аналіз для якісної оцінки ситуації та викликів, під дією яких перебувають підприємства. Побудовано матрицю сильних сторін, проблем, можливостей та невизначеностей, за результатами якої інфраструктура підприємств-постачальників електронних комунікаційних мереж та послуг відзначається стабільністю та збереженням функціонування в регіонах, що знаходяться територіально віддалено від зони бойових дій та дозволяє продовжувати надавати послуги та обслуговувати клієнтів. Клієнтська база є стійкою через лояльність до клієнтів та тривалим користуванням полсугами конкретного оператора, крім того якісний зв’язок забезпечується 3 основними операторами, що стримує перехід до інших постачальників електронних комунікаційних послуг, тим самим забезпечує компаніям надходження оплат та приросту доходів від послуг.

Із урахуванням низької прогностичості та постійного мінливого середовища існування підприємств зв’язку, спираючись на результати щодо можливостей та виликів за матрицею SPOD, сформано чотири вірогідні сценарії

розвитку конфлікту за сценаріями розвику подій для підприємств сфери електронних комунікацій (стабілізація конфлікту та поступове відновлення; ескалація та довготривалість невизначеностей; часткове врегулювання зі збереженням незначної невизначеності; позитивне розв'язання конфлікту, відбудова, інтенсивне відновлення).

Розроблено та проведено параметричну діагностику безпеки підприємства за умов невизначеності та динамічності процесів, визначено змінні, що описують впливи викликів за їх ймовірністю на результат (ретроспективно, по відношеню динаміки зростання прибутку за нормальних умов функціонування) та кількісно визначено ентропію в середовищі функціонування підприємств. Встановлено що за отриманим значенням ентропії H(X) рівень непередбачуваності та складності управління є високим.

Розраховано динаміку чистого прибутку послуг за інертним сценарієм відновлення та спрогнозовано чистий прибуток досліджуваних підприємств за трьох вірогідних сценаріїв розвитку.

Сформовано стратегічні напрями розвитку відновлення підприємств-постачальників електронних комунікаційних мереж та послуг, що грунтуються на взаємній комбінації наступних ініціатив: відбудова та модернізація інфраструктури; операційна ефективність та стійкість; посилення заходів кібербезпеки; регуляторна відповідність та адвокація; економічна адаптація та зростання, які націлені на пришвидшення усунення викликів та нейтралізацію їх наслідків.

Основні ідеї та наукові положення, презентовані у даному розділі, викладені у піблікаціях та працях [321; 347; 357; 359; 360; 362; 365; 369; 372; 373; 382].

ВИСНОВКИ

1. Відзначено, що термінологічний базис розуміння безпеки підприємства нашаровується із часом відповідно до нових умов функціонування, науково-технічного прогресу, проте суть поняття залишається незмінною, та передбачає перебування підприємства у стані захищеності від небезпек. У результаті критичного аналізу напрацювань щодо питань безпеки підприємства, розгляду її етимології, надано визначення її, як стану стійкого функціонування й потенціальної спроможності його розвитку за умови відсутності небезпек (викликів, ризиків, загроз), а у разі їх появи – захищеності, що гарантує досягнення цільових безпекових результатів діяльності.

2. З'ясовано, що безпека підприємства окреслюється сукупністю елементів, серед яких визначають: суб'єкти, об'єкти, виклики, ризики, загрози, оточення та його впливи; виявлено, що на безпеку підприємства чинять вплив об'єктивні негативні впливи, що йдуть усупереч інтересам підприємства, виникають самі по собі без участі керівництва та персоналу. Також значаться суб'єктивні негативні впливи на безпеку підприємства, що є результатом неправильного та неефективного керування, з'являються через помилки або некомпетентність керівництва, персоналу.

3. Проаналізовано складові, які відзначено як загальноприйняті при дослідженні безпеки (фінансова, техніко-технологічна, виробнича, енергетична, ринкова, кадрова, інтерфейсна (репутаційна), інформаційна, фізична (фізична (силова), політико-правова, екологічна, інвестиційно-інноваційна). Запропоновано додати електронно-комунікаційну складову безпеки у відповідь на посилення ролі електронних комунікаційних послуг в умовах активної цифровізації та зростанні кількості кібератак на підприємства ПЕКМП.

4. З'ясовано, що ризик є ймовірністю настання події, тому прийняття рішень відбувається гіпотетично, із можливістю множини варіантів прийняття рішень на основі передбачень розвитку подій. Відзначено, що загроза вказує на

дію, яка відбувається, підприємство відчуває коливання стану безпеки під дією деструктивних змін, тому поняття не є тотожним із ризиком. Розуміння управління бізнес-процесами несе різне смислове навантаження на безпеку підприємства й диференціює управління ним за умов визначеності та невизначених умов.

5. Окреслено ризики та загрози безпекової площини у визначеному та невизначеному середовищі, як рушії небезпеки; відмічено, що від умов та середовища функціонування підприємства залежить ступінь їх впливу на стійкість підприємства: у визначеному середовищі ризики та загрози усуваються, як правило швидко через поінформованість щодо підприємства, у разі невизначеності (низької поінформованості щодо середовища існування підприємства) – усуваються повільно, час на відновлення збільшується, виникає висока вірогідність ліквідації господарюючого суб'єкта, що знову ж таки підтверджує стани перебування підприємства, як безпечні та небезпечні.

6. З'ясовано, що еволюція підходів до виробництва змінює економіку та управління безпекою підприємства, зокрема індустрія 1.0. та 2.0 передбачала орієнтованість на виробника та постачальника, безпека підприємства вбачалася у захисті прибутку, що втратило актуальність в епоху індустрії 3.0. та 4.0, коли розвиток технологій призвів до порушення стабільного отримання прибутків виробником без орієнтованості на вподобання споживача. Відзначено, що четверта технологічна революція докорінно змінила направленість безпеки, котра зорієнтована на клієнтів, стейкхолдерів (захисті їх інтересів), врахування екологічної складової (сталий розвиток), що свідчить про динамічність та ситуативність управління, геополітична нестабільність передбчає врахування енергетичної небезпеки, як головної умови функціонування підприємств за умов диверсифікації джерел живлення та їх часової спроможності.

7. Узагальнено та виокремлено зв'язки у структурі категорій безпеки, теоретичний блок методології управління безпекою підприємства вибудовано навколо наукових напрацювань питань безпеки, за яким узагальнено понятійний апарат безпеки підприємства, визначено елементи та складові

(ризики, загрози, виклики, невизначеність, цільові безпекові орієнтири, об’єкти, суб’єкти управління, стейкхолдери), за якими формується площина безпеки підприємства, що дозволило сконструювати онтологічний базис методології управління безпекою підприємства.

8. Запропоновано концепт траєкторії площин станів безпеки та управління ним під дією тривекторного синергетичного управління (гармонізація інтересів – захист від небезпек – захист результатів діяльності). Сформовано композитарний зв’язок між складовими безпеки, метриками безпеки та цільовими безпековими результатами, а також побудована мережева складова ємність цільових безпекових результатів управління.

9. Запропоновано методологію управління безпекою підприємств, зважаючи на: інформованість, ризики та загрози, складові (критерії), оцінки ризиків та сценарії прийняття рішень, відповідність цільових результатів безпеки нормативним значенням та рівню задоволеності стейкхолдерів результатами (рівня гармонізації інтересів стейкхолдерів), що дозволить враховувати окремо ризики та загрози з визначенням репелер та біфуркаційних точок, за якими вибудовуватиметься безпекова площина та визначатиметься стан безпеки.

10. Визначено затребуваність послуг зв’язку через активну цифровізацію держави та надання електронних послуг підприємствам (надання публічних е-послуг, е-ідентифікації, е-декларування через створений портал державних послуг “Дія”) та потребу у гармонізації стандартів, нормативно-правових актів із країнами Євросоюзу. Проаналізовано основні інституційні зміни щодо впровадження цифрових інновацій та розширення переліку надання е-послуг. З’ясовано, що на ринку електронних комунікацій відбувається приріст доходів зв’язку по відношенню до 2022 року, темп росту доходів від надання електронних комунікаційних послуг за 2023 рік по відношенню до попереднього року становив 116,95% (найбільша частка доходів припадає на мобільний зв’язок). Відзначено, що Україна посідає 88 місце за швидкістю мобільного Інтернету та відповідно 76 за фіксованим широкосмуговим

доступом до глобальної мережі, що вказує на потребу удосконалення технологій надання послуг.

11. З'ясовано, що ПрАТ "ВФ Україна" знаходиться на межі втрати здатності генерувати грошовий потік та втрати фінансової потужності, АТ "Укртелеком" та "Датагруп" перебувають в зоні загроз, подолавши критичну точку біфуркації, в зоні ризику перебуває ПрАТ "ВФ Україна". Загрози втрати генерації прибутку (за рахунок власного капіталу, а також активів) та зростання боргового навантаження відзначаються у "ВФ Україна", "Лайфселл", "Укртелеком", "Датагруп". Загроза втрати спроможності до самофінансування, інвестиційної привабливості, зниження операційної ефективності наявна у компанії "Укртелеком"; загрози втрати конкурентоспроможності через зниження ефективності компанії в продукуванні нових, послуг по відношенню до конкурентів відзначаються у компанії "Лайфселл", "Укртелеком", "Датагруп"; ризик нестійкості бізнесу характерний для "Лайфселл" та "Датагруп", під загрозою "Укртелеком"; загроза втрати ефективності інвестицій та ризик гальмування розвитку є в "Укртелеком" та "Датагруп"; ризик зниження продуктивності та мотивації персоналу прослідковується в "Датагруп", загроза - в "Укртелеком".

12. Побудовано модель управління безпекою підприємств-постачальників електронних комунікаційних послуг з визначенням безпекових відхилень у безпеко-небезпечній площині дотичності репелерних точок впливу ризиків і біфуркаційних точок дії загроз та вибором відповідного підходу до управління безпекою підприємства для досяжності цільових показників безпеки підприємства. Відзначено, що за результатами моделювання, стан безпеки ПрАТ "Київстар" визначається, як нормальний, ПрАТ "ВФ Україна" – відносної безпеки; ТОВ "Лайфселл" – кризовий стан безпеки; "Укртелеком" – критичний, ПрАТ "Датагруп" – критичний. Доведено, що змодельовані відхилення площин станів безпеки дозволяють диференціювати підходи до управління безпекою підприємства з урахуванням втрат (відхилень) від цільових метрик безпеки (результатів).

13. Проаналізовано виклик для управління безпекою підприємства в умовах невизначеності, переважна більшість яких екзогенного характеру та не підлягає впливу з боку підприємства, проведено їх узагальнення внаслідок ведення бойових дій на території України. Відзначено виклики, що загрожують підприємствам електронних комунікацій: стихійні лиха та руйнації у результаті бойових дій; втрата електроживлення; неспроможність надання послуг через брак енергоефективних технологій GPON; кібератаки. Проведено VUCA і BANI-аналіз для якісної оцінки ситуації та викликів, під дією яких перебувають підприємства. Побудовано матрицю сильних сторін, проблем, можливостей та невизначеностей, за результатами якої інфраструктура підприємств-постачальників електронних комунікаційних мереж та послуг відзначається стабільністю та збереженням функціонування в регіонах, що знаходяться територіально віддалено від зони бойових дій та дозволяє продовжувати надавати послуги, обслуговувати клієнтів. Сформовано чотири вірогідні сценарії розвитку сфери електронних комунікацій (стабілізація конфлікту та поступове відновлення; ескалація та довготривалість невизначеностей; часткове врегулювання зі збереженням незначної невизначеності; позитивне розв’язання конфлікту, відбудова, інтенсивне відновлення).

14. Розроблено та проведено науково-параметричну діагностику безпеки підприємства за умов невизначеності та динамічності процесів, визначено змінні, як впливи викликів за їх ймовірністю на результат (ретроспективно, по відношенню динаміки зростання прибутку за нормальних умов функціонування) та кількісно визначено ентропію в середовищі функціонування підприємств. Встановлено, що за отриманим значенням ентропії H(X) рівень непередбачуваності та складності управління є високим.

15. Сформовано стратегічні напрями розвитку відновлення підприємств-постачальників електронних комунікаційних мереж та послуг, що ґрунтуються на взаємній комбінації ініціатив (відбудова та модернізація інфраструктури; операційна ефективність та стійкість; посилення заходів кібербезпеки;

регуляторна відповідність та адвокація; економічна адаптація та зростання), які націлені на пришвидшення усунення викликів та нейтралізацію їх наслідків.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (Дата звернення: 07.09.2022).

2. Деякі питання об'єктів критичної інфраструктури: порядок, перелік, методика : Постанова Кабінету Міністрів України від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n42. (Дата звернення: 08.09.2022).

3. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20/sp:max50:nav7:font2#Text (Дата звернення: 10.09.2022).

4. Presidential Policy Directive – Critical Infrastructure Security and Resilience. *The White House*. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (Дата звернення: 11.09.2022).

5. Rosenstain-Rodan P. N. The Notes of the Theory of the “Big Bush” in Economic Development for Latin America. London. New York, 1961.

6. Rabotin Y. The Essence of economic Security and the Principles of its Provision at the Enterprise. *Revista Română de Statistică – Supliment*. 2022. Vol. 8. P. 37-42.

7. Voronina V. Economic Security of Enterprises: the Essence, Factors of Influence, and Methods of Protection. Security Of The Xxi Century: National And Geopolitical Aspects : collective monograph. Prague : Nemoros s.r.o., 2019. P. 217-223.

8. Melikhova T. Analysis of available Methods for Assessing the Level of Economic Security of an Enterprise for Conducting Modern Diagnostics of its Financial Condition. *Innovative Economy.* 2020. Vol. 1-2. P. 223-227.

9. Burkynskyi B., & Gryshchenko, V. Factors Of Ensuring Economic Security In The Process Of Innovative Development Of Entrepreneurship. *Economic Innovations*. 2020. Vol. 22, no. 3(76). P. 6-29. URL: https://doi.org/10.31520/ei.2020.22.3(76).6-29

10. Ілляшенко О. В. Механізм функціонування системи економічної безпеки підприємства: підхід до побудови. *Економіка. Менеджмент. Підприємництво*. 2014. № 26(1). С. 160-168.

11. Дуб Б. С. Система економічної безпеки підприємства: поняття та структура. *Управління проектами та розвиток виробництва*. 2016. №4(60.) С. 5-9. URL: https://www.researchgate.net/publication/322958986_Sistema_ekonomicnoi_bezpeki_pidpriemstva_ponatta_ta_struktura (дата звернення: 11.10.2022)

12. Покропивний С. Ф. Економіка підприємства. Київ : КНЕУ, 2000. 526 с.

13. Геєць В. М. Моделювання економічної безпеки: держава, регіон, підприємство. Харків : ВД "ІНЖЕК". 2006. 240 с.

14. Гудзь О. Є., Сотниченко В.М. Принципи та умови забезпечення економічної безпеки телекомунікаційних підприємств. *Економіка. Менеджмент. Бізнес*. 2016. № 4. С. 12-19. URL: http://nbuv.gov.ua/UJRN/ecmebi_2016_4_4 (дата звернення: 17.09.2022)

15. Сосновська О. О. Методичний підхід до оцінки рівня економічної безпеки підприємств зв'язку. *Облік і фінанси*. 2019. № 1. С. 168-176. URL: http://nbuv.gov.ua/UJRN/Oif_apk_2019_1_22 (дата звернення: 18.09.2022)

16. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства. *Економіка. Менеджмент. Бізнес*. 2015. № 3. С. 87-92. URL: http://nbuv.gov.ua/UJRN/ecmebi_2015_3_18 (дата звернення: 18.09.2022)

17. Пильнова В. П., Капелюшна Т. В., Овсійчук В. Я., Красник О. А. Місце інноваційних ризиків у системі економічної безпеки підприємства. *Економіка. Менеджмент. Бізнес*. 2021. № (4). С. 61-68.

18. Данілова Е. І. Концепція системного підходу до управління економічною безпекою підприємства : монографія. Вінниця : Європейська наукова платформа, 2020. 342 с.

19. Secure Internet Servers. *World Bank Group*. URL: https://data.worldbank.org/indicator/IT.NET.SECR?end=2020&start=2010&type=shaded&view=map&year=2020 [accessed Oct 15 2022].

20. 5G – Fifth generation of mobile technologies. *ITU*. URL: https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx (accessed Oct 9 2022).

21. Fischer F. Ulrich Beck and the politics of the risk society: The environmental threat as institutional crisis. *Organization & Environment*. 1998. Vol. 11, no. 1, P. 111–115. URL: http://www.jstor.org/stable/26164879

22. Daase C. Von der nationalen zur menschlichen Sicherheit: Politische und rechtliche Konsequenzen des erweiterten Sicherheitsbegriffs. *Recht und Politik globaler Sicherheit.* 2013. C. 11-42.

23. Капелюшна Т. В., Сіненко А. О. Формування соціально-психологічних компетенцій підприємця для досягнення ефективних результатів діяльності. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку:* матеріали III міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 35-37. *(0,12 д.а., авторський внесок 0,08 д.а., полягає в дослідженні впливу соціально-психологічних компетенцій підприємця на результати діяльності підприємства).*

24. Ситник Г. П., Орел М. Г. Публічне управління у сфері національної безпеки : підручник. Київ : ВПЦ “Київський університет”, 2022. 464 с.

25. Зеліско І. М., Захаржевська А. А. Глобалізаційні імперативи діагностики розвитку управління ризиками телекомунікаційних підприємств. *Управління змінами та інновації*. 2022. № С. 9-13. https://doi.org/10.32782/CMI/2022-4-2.

26. Глобальна та національна безпека: словник-довідник / Г.П. Ситник та ін. Київ : НАДУ, 2016. 140 с.

27. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

28. Зубко Т. Л. Економічна безпека підприємства: виклики XXI сторіччя : монографія. Київ : КНТЕУ, 2021. 420 с.

29. Денисов О.Є. Економічна безпека галузей промисловості в системі економічної безпеки держави : дис. на здоб наук ступеня д.е.н. : 21.04.01. Київ, 2019. 496 с.

30. Мелих О. Ю. Фінансова безпека держави: сутність, критерії оцінки та превентивні заходи зміцнення. *Економічний аналіз*. 2013. №. 12(2). С. 266-272.

31. Гуляєва Н. М., Камінський С. І. Економічна безпека підприємства: історична проекція розвитку змісту і тлумачення. *Інноваційна економіка*. 2017. № 9-10. С.139-142. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/297860.pdf

32. Швиданенко Г. О., Кузьомко В. М., Норіцина Н. І. Економічна безпека бізнесу : навч. посіб. Київ : КНЕУ, 2011. 511 с. URL: https://core.ac.uk/download/pdf/197268629.pdf

33. Язлюк Б. О. Теоретичні основи сутності та змісту соціально-економічної безпеки. *Економічний аналіз*. 2014. № 16(1). С. 149-154. URL: http://dspace.wunu.edu.ua/bitstream/316497/9884/1/457-3453-1-PB%20%281%29.pdf

34. Пехник А.В, Кройтор А.В., Завгородня Ю.В. Теорія ризику: історія та сучасні підходи. Актуальні проблеми політики. 2019. №.63. С. 33-47. DOI: https://doi.org/10.32837/app.v63i0.5

35. Fireside Chats (F. Roosevelt). *The American Presidency Project*. URL: https://www.presidency.ucsb.edu/documents/presidential-documents-archive-guidebook/fireside-chats-f-roosevelt.

36. Обиденко Г. О. Формування економічної безпеки сільськогосподарських підприємств : автореф. дис. ... к. е. н. : 08.00.04. 2021.

37. Кучмєєв О. О. Формування економічної безпеки підприємств оптової торгівлі.: автореф. дис. ... д. е. н. : 08.00.04. 2021.

38. Чубаєвськицй В. І. Економічна ефективність систем захисту корпоративної інформації : автореферат дис. ... д. е. н. : 08.00.04. 2023.

39. Зубко Т. Л. Економічна безпека підприємств торгівлі в умовах євроінтеграції : автореф. дис. ... д. е. н. : 08.00.02. 2023.

40. Нестеров Ю. О. Механізми управління економічною безпекою підприємства в умовах нестабільного економічного середовища : автореф. дис. ... канд. екон. наук : 08.00.04. 2011. 20 с.

41. Сосновська О. О. Управління економічною безпекою підприємств зв'язку: теорія та методологія : автореф. дис. ... д. е. н. : 08.00.04. Київ, 2019. 41 с.

42. Шуміло О. С. Управління економічною безпекою підприємств роздрібної торгівлі : автореф. дис. ... д. е. н. :08.00.04. 2019.

43. Тютченко С. М. Забезпечення економічної безпеки підприємств вумовах трансформаційних змін в економіці : автореф. дис. ... к. е. н. : 08.00.04. 2020.

44. Ліщенко А. В. Інформаційне забезпечення економічної безпеки молокопереробних підприємств: автореф. дис. ... к. е. н. : 08.00.04. 2021.

45. Єфімова Г.В. Визначення категорій “економічна безпека підприємства” і “безпечний розвиток підприємства”. *Бізнес Інформ*. 2013. № 11. С. 8-13. URL: http://nbuv.gov.ua/UJRN/binf_2013_11_2

46. Ткачук, Г. Ю. Інструментарій забезпечення економічної безпеки підприємства. *Економічний простір*. 2022. № 178, С. 55-59. URL: https://doi.org/10.32782/2224-6282/178-9

47. A. H. Maslow. A Theory of Human Motivation. *Psychological Review*. 1943. Vol. 50, P. 370-396.

48. Литвинов В.Д. Латинсько-український словник. Київ : Укр. Пропілеї, 1998. 644 с.

49. Ткачук Г.Ю., Підходи до сутнісного наповнення категорії “безпека”. *Вісник ЖДТУ. Серія: Економічні науки*. 2014. № 2(68). С. 178-184.

50. Lambert D. La defense de l’ekonomie: la conjugasion des efforts de l’Etat, de l’entreprise et d’individy. *Strategigue*. 1990. Vol. 2. P. 83–98.

51. Ляшенко О. М. Концептуалізація управління економічною безпекою підприємства : монографія. Київ : НІСД, 2015. 348 с.

52. Дунда. С. П. Розвиток підприємства та оцінка чинників, що на нього впливають. *Ефективна економіка*. 2016. № 12. URL: http://www.economy.nayka.com.ua/?op=1&z=5329

53. Філиппова С. В., Нізяєва С. А. Аналітичні інструменти системи економічної безпеки суб’єктів господарювання : монографія. Донецьк : НОУЛІДЖ, 2012. 179 с.

54. Arefieva O. V., Miahkykh I. M., Shkoda, M. S. Diagnostics of external environment effects upon enterprise competitive positions in the context of its economic security. *Bulletin of the Kyiv National University of Technologies and Design. Series: Economic sciences.* 2019. Vol. 135, no. 3. P. 8–17.

55. Захарченко В. І., Меркулов М. М., Ширяєва Л. В. Економічна безпека та конкурентна розвідка : конспект лекцій. Одеса : БАХВА, 2018. 520 с.

56. Соломіна Г. В. Забезпечення фінансово-економічної безпеки підприємництва : навчальний посібник. Дніпро : ДДУВС, 2018. 234 с.

57. Ситник Г. П., Орел М. Г. Національна безпека в контексті європейської інтеграції України : підручник. Київ : МАУП, 2021. 372 с.

58. Сосновська О. О., Житар М. О. Економічна безпека підприємства: сутність та ознаки забезпечення. *Облік і фінансиу* 2018. № 3(81). С. 124-132. URL: https://core.ac.uk/download/pdf/185262433.pdf

59. Методичний посібник щодо аспектів управління ризиками, як складової системи внутрішнього контролю у розпорядника бюджетних коштів. *Міністерство Фінансів Укаріни*. URL:https://mof.gov.ua/storage/files/B8.pdf

60. Рязанова Н. О. Формування системи управління ризиками на промислових підприємствахакадемічний огляд. *Бізнес інформ*. 2022. № 1(56). С. 63-71.

61. Вахлакова В. В. Безпекозабезпечувальна діяльність підприємства: зміст, принципи та способи. *Бізнес-Інформ*. 2020. № 3. С. 200-207.

62. Погорелов Ю. С. Безпекозабезпечувальна діяльність як об'єкт менеджменту безпеки. *Менеджмент і безпека в умовах війни: теоретичні та прикладні аспекти* : матеріали-науково-практичної інтернет-конференції, м. Львів, 13 травня 2022 р. Львів : ЛьвДУВС, 2022. С. 97-100.

63. Євтушенко Н.О. Планування як ефективний інструмент управління підприємством в умовах невизначеності та ризику. *Інтелект XXI*.2023. № 1. С. 53-59

64. Овчаренко Є. І. Перспективи захисного підходу у безпекології. *Економічна безпека: держава, регіон, підприємство* : матеріали III Всеукраїнської науково-практичної Інтернетконференції з міжнародною участю, 1 грудня 2016 р., 10 січня 2017 р. Полтава : ПолтНТУ, 2017. С. 39-42.

65. Чуприн Є. Формування системи забезпечення економічної безпеки підприємств : автореф. дис. ... д.філософ : 051. Харків, 2021.

66. Сосновська О. Формуання системи забезпечення економічної безпеки підприємств. : автореф. дис. ... д.е.н. 08.00.04. Київ, 2019.

67. Отенко І. Комарков Д., Шкребень Р. Д. Стратегічний інструментацій безпеко-орієнтованого розвитку підприємства. *Проблеми економіки*. 2018. С. 235-241.

68. Шкребень Р. П., Харнам М. В., Отенко І. П. Формування стратегічного потенціалу безпеко-орієнтованого розвитку підприємства. *Проблеми економіки*. 2020. № 4(46). С. 256-264. URL: www.problecon.com/export_pdf/problems-of-economy-2020-4_0-pages-256_264.pdf

69. Чуприн Є. Формування системи забезпечення економічної безпеки підприємств : автореф. дис. ... д.філософ : 051. Харків, 2021.

70. Кучмєєв О. Формування економічної безпеки підприємств оптової торгівлі : автореф. дис. ... д. е. н. : 08.00.04. Київ, 2021.

71. Герасименко О. М. Ризик-орієнтоване управління в системі економічної безпеки підприємства : автореф. дис. ... д. е. н. : 21.04.02. Київ, 2021.

72. Дідик А. М., Кузьмін О. Є., Ортинська В. Л., Козаченко Г. В., Погорелов Ю. С., Ілляшенко О. В. Економічна безпека підприємства : підручник. Львів : НУ "Львівська політехніка", ТзОВ "Видавнича група" "Бухгалтери України", 2019. 624 с.

73. Мельник С. І. Дослідження викликів, ризиків, загроз та небезпеки в системі забезпечення фінансової безпеки підприємства. *Проблеми системного підходу в економіці*. 2019. № 4(72). С. 172-177.

74. Haddon S. G. Risk Analysis, Institutions and Public Policy. Port Washington NY, New York City, London, Associated Faculty Press, 1984. P. 7.

75. Berting J. Europe: a heritage, a challenge, a promise. Eburon Academic Publishers, 2006. P. 223

76. Villain-Gandossi C. Origines du concept de risque en Occident. Les risques maritimes ou fortune de mer et leur compensations: les débuts de l'assurance maritime. Le risque et la crise, Malta, Foundation for International Studies, 1990. P.73.

77. Friedman M., Savage L. J. The Utility Analysis of Choices Involving Risk. *Journal of Political Economy*. 1948. Vol. 56, no. 4. P. 279–304. URL: https://www.journals.uchicago.edu/doi/10.1086/256692

78. Горячева К. С. Механізм управління фінансовою безпекою підприємства : автореф. дис. … канд. економ. наук : 08.00.09. Київ, 2006.

79. Короленко О. Б. Кутова Н. Г. HR-менеджмент підприємства: виклики та реалії сьогодення. *Економіка та суспільство*. 2023. № 53. URL: https://economyandsociety.in.ua/index.php/journal/article/view/2682/2597

80. Thomas del Marmol. PESTLE-аналіз: Розуміти та планувати своє бізнес-середовище. 50Minutes.com, 2023. 31 с.

81. What is a PESTLE Analysis? Understanding Macro-Environmental Factors. *The Power Business School*. URL: https://www.thepowermba.com/en/blog/pestle-analysis

82. Šopíková M. Risk Management in the Selected Industry. 2021.

83. Wood R. What's the Difference Between Qualitative and Quantitative Risk Analysis. *Safran*. URL : https://www.safran.com/blog/whats-the-difference-between-qualitative-and-quantitativerisk-analysis

84. Bc. Michaela Šopíková. Risk Management in the Selected Industry. Master Thesis. Liberec, 2022. 65 p. URL: https://dspace.tul.cz/server/api/core/bitstreams/c51eedb1-f859-4931-9edd-fa292d0f219b/content

85. Капелюшна Т. В. Розширення базових складових економічної безпеки підприємства з урахуванням умов невизначеності. *Ефективна економіка*. 2022. № 10. URL: https://www.nayka.com.ua/index.php/ee/article/view/675/683

86. Капелюшна Т. В. Безпека функціонуючих господарюючих суб'єктів в сучасних умовах за систематизованого управління ризиками. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу* : матеріали Всеукраїнської науково-практичної Інтернет-конференції, м. Київ, 23 лютого 2023 р. Київ : ДУТ, 2023. С. 40-42.

87. Кравченко М. О., Бояринова К. О., Копішинська К. О. Управління ризиками : навчальний наочний посібник. Київ : КПІ ім. Ігоря Сікорського, 2021. 432 с.

88. Данкевич В. Є. SWOT та PESTEL-аналіз сучасного стану земельних відносин в Україні. *Економіка АПК*. 2018. № 7. С. 93-103.

89. Тулуб О. Денотативне значення та відмінності складових ланцюга "ризик-небезпека-загроза". *European Journal of Economics and Management*. 2017. Vol. 3, Is. 3. P. 5-11.

90. Шевченко І. Особливості формування системи економічної безпеки підприємств. *Наука молода.* 2008. № 10. С.178-181.

91. Філіпова С. В., Дашковський О. С. Система формування і забезпечення економічної безпеки підприємства. *Економіка: реалії часу*. 2012. № 2(3). С.17-21. URL: https://economics.net.ua/files/archive/2012/No2/17-21.pdf

92. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення : монографія / Васильців Т. Г. та ін. Львів : Видавництво. 2012. 386 с.

93. Мельник С. І. Управління фінансовою безпекою підприємств: теорія, методологія, практика : монографія. Львів : "Растр-7", 2020. 384 с.

94. Newbould G., Luffman, G. Successful Business Politics. London : Gower, 1989. 78 p.

95. Freeman R. E. Strategic Management. A Stakeholder Approach. Boston : Pitman, 1984. 275 p.

96. 2050 low-carbon economy. *European Commission*. URL : https://ec.europa.eu/clima/policies/strategies/2050_en

97. Oxford English Dictionary, s.v. "security (n.), Etymology," December 2023, https://doi.org/10.1093/OED/3785881144.

98. Oxford English Dictionary, s.v. "security (n.), Forms," December 2023, https://doi.org/10.1093/OED/1054675364.

99. Ткаченко Т.П. Генезис розвитку теорії економічної безпеки та системний підхід до її трактування. *Економічний вісник НТУУ*. 2021. № 19. С. 20-25.

100. G. Schönberg. Handbuch der Politischen Ökonomie. Tübingen, 1885. P. 670.

101. Васильців Т. Г., Лупак Р. Л., Куницька-Іляш М. В., Наконечна Н. В. Економічна безпека суб'єктів господарювання та держави: аспект гарантування фінансово-економічної безпеки пріоритетних галузей національної економіки України. *Наукові записки Львівського університету бізнесу та права*. 2023. № 37. С.22-30. URL: http://dx.doi.org/10.5281/zenodo.7769997

102. Russell L. Ackoff. Ackoff's Best: His Classic Writings on Management. John Wiley & Sons, 1999. 368 p.

103. Капелюшна Т. В., Лисогор М. Л., Купрієнко Є. О. Фінансовий механізм забезпечення розвитку та конкурентоспроможності торговельного підприємства. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали І міжнар. наук.-практ. конф., м. Київ, 11 лют. 2020 р. Київ, 2020. С. 32-35. *(0,13 д.а., авторський внесок 0,1 д.а. полягає у дослідженні дієвих механізмів забезпечення розвитку та конкурентоспроможності підприємств)*

104. Пойда-Носик Н. Н. Фінансова безпека акціонерних товариств: теоретико-методологічний та практичний аспекти системного підходу : монографія. Чернігів : ЧНТУ, 2020. 304 с.

105. T. N. Carver, The Risk Theory of Profits. *The Quarterly Journal of Economics*. 1901. Vol. 15, Is. 3. P. 456–458. URL: https://doi.org/10.2307/1885200

106. Frank H. Knight. *Risk,* Uncertainty, and Profit. Boston and New York : Houghton Mifflin Company, 1921. 388 p.

107. Kapeliushna T., Goloborodko A., Nesterenko S. Bezhenar I., Matviichuk B. Analysis of digitalization changes and their impact on enterprise security management under uncertainty. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2023. No. 4. P. 150–156. URL: https://doi.org/10.33271/nvngu/2023-4/150. *(1,01 д.а., авторський внесок 0,21 д.а., полягає в обґрунтуванні врахування трансформаційних змін, що викликані діджиталізацією в управлінні безпекою)*

108. Капелюшна Т. В., Пильнова В. П., Полякова А. О., Купрієнко Є. О. Роль електронної комерції в умовах формування цифрової держави та інформатизації суспільства. *Економіка. Менеджмент. Бізнес.* 2021. № 4. С. 68-75. URL: http://nbuv.gov.ua/UJRN/ecmebi_2021_4_13 *(0,45 д.а., авторський внесок 0,18 д.а., полягає в відзначенні потреби посилення захисту та безпеки підприємств, що представляють товари та послуги на електронних комерційних платформах).*

109. Коренюк П.І. Ризик-менеджмент : конспект лекцій для здобувачів вищої освіти другого (магістерського) рівня спеціальності 073 – Менеджмент. Кам’янське : ДДТУ, 2017. 185 с.

110. Фролова Л., Жадько К., Ілляш О., Єрмак С., Носова Т. Модель оцінки можливостей підвищення інноваційної активності підприємства. *Бізнес: теорія і практика.* 2021. №. 22. С. 1-11.

111. Штамбург Н. В. Складові економічної безпеки підприємства. *Бюлетень Міжнародного Нобелівського економічного форуму*. 2011. № 1 (4). С. 490-496.

112. Верескун М.В., Камишникова Е.В., Ісаєв О. Ю, Криклива Є.Ю. Загальна політика безпеки, як фундамент економічної безпеки підприємства. *Сталий розвиток економіки*. 2024. № (1(48). С. 170-175. https://doi.org/10.32782/2308-1988/2024-48-23

113. Живко З. Б. Економічна безпека підприємства: сутність, механізм забезпечення та управління : монографія. Львів : ЛігаПрес, 2012. 256 с

114. Про затвердження Інструкції з організації та здійснення внутрішнього контролю в Міністерстві економіки України, на підприємствах, в установах та організаціях, що належать до сфери управління Мінекономіки : Наказ Міністерства економіки України від 11.04.2023 № 2035. URL: https://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=282a5ede-df34-47c0-bee0-5 (дата звернення: 17.01.2023).

115. Про затвердження Основних засад здійснення внутрішнього контролю розпорядниками бюджетних коштів та внесення змін до постанови Кабінету Міністрів України від 28 вересня 2011 р. № 1001 Постанова Кабінету Міністрів України від 12 грудня 2018 р. № 1062. URL: https://zakon.rada.gov.ua/laws/show/1062-2018-п?find=1&text=ризик#w1_1 (дата звернення: 10.10.2022).

116. Про схвалення Стратегії реформуваня системи управління державними фінансами на 2022 - 2025 рр. Розпорядження Кабінету Міністрів України від 29 грудня 2021 № 1805-р. URL: https://zakon.rada.gov.ua/laws/show/1805-2021-%D1%80#Text

117. ВВП за роками. *Незалежна асоціація банків України*. URL: https://nabu.ua/images/uploaded/com_chart/file_3e35039f41bb1542a59c4773b6db1169.xls

118. Національні рахунки ВВП. *Офіційний сайт Держстату України*. URL: https://ukrstat.gov.ua/imf/arhiv/nr/nr_u.htm

119. Орлов В. М. Економіка телекомунікацій : навч. посіб. Одеса : ВМВ, 2014. 516 с.

120. Економіка телекомунікацій : навч. посіб. Одеса : ОНАЗ, 2015. 140 с.

121. Орєхова К. В. Управління загрозами фінансовій безпеці підприємства. Економіка промисловості. 2013. № 1–2(61–62). С. 77–83.

122. Череп О. Г., Калюжна Ю. В., Михайліченко Л. В. Особливості управління персоналом в умовах воєнного стану в україні. *Економіка та суспільство*. 2023. № 48. URL: https://economyandsociety.in.ua/index.php/journal/article/view/2214

123. Karpenko O, Bonyar S, Tytykalo V, Belianska Y, Savchenko S. The Mechanism of the Investment Resources Involvement in Order to Introduce Innovations at Enterprises in the Conditions of Digitalization. International Journal of Computer Science and Network Security. № 21(11). P. 81–88.: URL: https://doi.org/10.22937/IJCSNS.2021.21.11.11

124. Копчак Ю. С., Слюсаренко К. В., Чумаков К. І. Сучасні виклики до менеджменту підприємств та організацій в Україні: врахування зарубіжного досвіду у вітчизняній практиці. *Економіка та суспільство*. 2023. № 48. URL: https://economyandsociety.in.ua/index.php/journal/article/view/2286/2207

125. Franchuk V., Sylkin O. Implemention of Anti-Crisis Management in the Contex of Insuring Sustainable Development of Enterprise. *Advances in Economics, Business and Management Research*. 2022. Vol. 170. P. 37–38

126. VUCA – volatility | uncertainty | complexity | ambiguity. *VUCA*. URL: https://www.vuca.de/

127. VUCA – volatility | uncertainty | complexity | ambiguity. *Quality.* URL: https://www.quality.de/lexikon/vuca/

128. N. Bennett, G. J. Lemoine. What VUCA Really Means for You. *Harvard Business Review*. URL: https://hbr.org/2014/01/what-vuca-really-means-for-you

129. VUCA Welt: Definition, Beispiele und 5 Workhacks für agile Führungskräfte. *Me&Company*. URL: https://www.me-company.de/magazin/vuca-welt/#vuca-welt-beispiele

130. Esprino D. K. Management for Decision Making: Public Hospitals. *HCI International 2023* : 25th International Conference on Human-Computer Interaction, Copenhagen, July 23–28, 2023. Copenhagen, 2023. P.187-194.

131. Про інноваційну діяльність : Закон України від 05.12.2012р. № 40-IV. Дата оновлення 16.10.12. URL: https://zakon.rada.gov.ua/laws/show/40-15 (дата звернення 03.09.2019).

132. Шваб К. Четверта промислова революція. Харків : Інжек, 2016. 230 с.

133. Кондратьєв М. Д. Великі цикли коньюнктури та теорія передбачення. Харків : Інжек, 2002. 767 с.

134. Шумпетер Й. Теорія економічного розвитку. Дослідження підприємницького прибутку, капіталу, циклу економічної коньюнктури. Львів : ЛігаПрес, 1992. 231с.

135. Ефремов В.С. Бізнес-процеси постіндустіального світу. *Менеджмент за кордоном*. 1999. №5. С.15-23.

126. Ліацин І.В. Економіка. ИНФРА-Б, 2018. 607 с.

136. What is Horizon 2020. *European Commission.* URL: https://ec.europa.eu/programmes/horizon2020/what-horizon-2020 (дата звернення 28.08.2019)

137. Горизонт 2020: рамкова програма ЄС з досліджень та інновацій. *Кабінет Міністрів України.* URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/broshura-gorizont-2020-1201.pdf (дата звернення 16.05.2019)

138. Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 : Розпорядження КМУ від 10.07.2019 р. № 526-р. URL: https://zakon.rada.gov.ua/laws/show/526-2019-%D1%80 (дата звернення: 03.08.2019).

139. Гудзь О. Є. Інноваційне підприємництво. Київ : Планета людей, 2018. 187 с.

140. Hawley F. B. The Risk Theory of Profit. *The Quarterly Journal of Economics.* 1893. № 7(4). P. 459–479.

141. Мойсеєнко І. П. Адаптивне управління в системі економічної безпеки. *Науковий вісник Львівського державного університету внутрішніх справ.* 2016. № 1. С. 102-111.

142. Кустовська О. В. Методологія системного підходу та наукових досліджень : курс лекцій. Тернопіль : Економічна думка, 2005. 124 с.

143. Пархоменко Н. О. Особливості управління економічною безпекою будівельного підприємства. *Ефективна економіка*. 2020. № 5. URL: http://www.economy.nayka.com.ua/?op=1&z=7877 (дата звернення: 15.09.2023).

144. Шовкова О. Д. Види ілюзії мислення у когнітивній психології. *Наукові записки Національного університету "Острозька академія". Серія "Психологія"*. 2018. № 7. С. 33–39

145. Özen-Akın, G., Cinan, S. People with jumping to conclusions bias tend to make context-independent decisions rather than context-dependent decisions. *Consciousness and Cognition: An International Journal*. 2022. Vol. 98. P. 1–14. URL: https://doi.org/10.1016/j.concog.2022.103279

146. Hilbert, M. Toward a synthesis of cognitive biases: How noisy information processing can bias human decision making. *Psychological Bulletin,* 2012. Vol. 138(2), P. 211–237.URL: https://doi.org/10.1037/a0025940

147. Чеберячко С. Когнітивне упередження та оцінка ризику. *Охорона праці.* 2022. № 3(333). С.38-42.

148. Lichtenstein B., 'Dissipative Structures - Theory and Experiments', *Generative Emergence: A New Discipline of Organizational, Entrepreneurial, and Social Innovation*. 2014. P. 149-168.

149. Shiozawa Y. Economy as a dissipative structure. *Paper read at Keihanna Prigogine Conference, organized and sponsored by Keihanna Co. and Sankei Newspaper,* May 28, 1996. URL: https://www.researchgate.net/profile/Yoshinori-Shiozawa/publication/296467573_The_New_Interpretation_of_Ricardo's_Four_Magic_Numbers_and_the_New_Theory_of_International_Values_A_Comment_on_Faccarello's_Comparative_advantage/links/56d58b5808ae5c281ca43b52/The-New-Interpretation-of-Ricardos-Four-Magic-Numbers-and-the-New-Theory-of-International-Values-A-Comment-on-Faccarellos-Comparative-advantage.pdf.

150. Song Y., Guo K. (2015). Empirical Study of Chinese Stock Market Structural Changes Based on Dissipative Structure Theory. Procedia Computer Science. 2015. P. 1040-1049. № 55. 10.1016/j.procs.2015.07.064.

151. Козенков Д. Є., Альошина Т. В. Процесний підхід до управління підприємством. *Економіка та суспільство*. 2022. № 38. URL: https://doi.org/10.32782/2524-0072/2022-38-67

152. TeleManagement Forum. Telecom Operations Map. Evaluation Version 2.1. Morristown : TMF, 2000. P. 82.

153. Виноградова О. В. Реінжиніринг бізнес-процесів у сучасному менеджменті : монографія. Донецьк : ДонДУЕТ, 2005.195 с.

154. Бліхар В. Організація наукових досліджень у сфері менеджменту та безпеки організації : підручник. Хмельницький : Вид-во ХУУП імені Леоніда Юзькова, 2022. 443 с.

155. Приходько В. П. Управління економічною безпекою підприємства. *Економіка та держава*. 2013. № 10. С. 10-12.

156. Сак Т. В. Стратегічні підходи в управлінні економічною безпекою підприємства. *Збірник наукових праць Хмельницького кооперативного торговельно-економічного інституту*. 2011. №5. С. 50-59

157. Чернодубова Є. В., Мартинов А. А. Переваги функціонального підходу до управління витратами і доходами підприємства. *Глобальні та національні проблеми економіки*. 2018. № 22. С. 860-864.

158. Ареф'єва О. В. Компетентнісно-функціональний підхід в інноваційному управлінні конкурентоспроможністю авіапідприємств в умовах економіки знань. Стійкий розвиток підприємств у міжнародному економічному просторі : монографія. Київ : ФОП Маслаков, 2018. С. 7-17. URL: https://core.ac.uk/download/pdf/344934679.pdf

159. Феєр О. В., Товт Т. Й., Машкаринець М. С. Аналіз теоретичних підходів до управління підприємством. *Міжнародний науковий журнал "Освіта і наука"*. 2021. № 2(31), С. 173-176. URL: https://msu.edu.ua/educationandscience/wp-content/uploads/2022/01/Освіта-і-наука-231-2021.-2-варіант-pdf-173-176.pdf

160. Черноіванова Г. С. Функціональний підхід до управління інноваційним складником підприємства. Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент. 2017. Вип. 28. С. 129–133.

161. Гринчишин Я. М. Стратегічний підхід до антикризового управління підприємствами. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління.* 2021. Т. 32(71), № 1. С. 38-41. URL: https://www.econ.vernadskyjournals.in.ua/journals/2021/32_71_1/8.pdf

162. Польова О. Л. Вибір стратегії антикризового управління підприємством. *Ефективна економіка*. 2015. № 11. URL: http://www.economy.nayka.com.ua/?op=1&z=4597/

163. Загородна О. М. Функціональний та процесний підходи до управління. *Актуальні задачі сучасних технологій* : матеріали V Міжнародної науково-технічної конференції молодих учених та студентів, м. Тернопіль 17-18 листопада 2016 р. Тернопіль, 2016. С. 328-329.

164. Князєва О.А., Банкет Н.В. Організаційно-економічний механізм проактивного управління економічною стійкістю підприємства в умовах

цифрових трансформацій. *Цифрова економіка та економічна безпека*. 2023. № 6 (06). С. 75-80. URL: https://doi.org/10.32782/dees.6-14

165. Стец І. І. Процесний підхід до управління як інструмент підвищення ефективності діяльності підприємства. *Інфраструктура ринку*. № 23. 2018. С. 161-167.

166. Туленков М. В., Лобанова А. С., Яремчук С. С. Системний аналіз у соціології : підручник. Чернівці : Чернівец. нац. ун-т ім. Ю. Федьковича, 2023. 508 с.

167. Полянська А. Ситуаційний підхід до управління затратами підприємства. *Вісник Економіки*. 2017. № 1. С. 134-140. URL: https://visnykj.wunu.edu.ua/index.php/visnykj/article/view/253.

168. Чорна. Л. О. Ситуаційний підхід до адаптації підприємств до кризових умов. *Ефективна економіка*. 2011. № 8. URL: http://www.economy.nayka.com.ua/?op=1&z=916

169. Vulić I., Prodanović R., Tot I. An Example of a Methodology for Developing the Security of a Distributed Business System. *Proceedings of the 5th IPMA SENET Project Management Conference (SENET 2019)*, Belgrade, Serbia, 19–21 May 2019. Paris, France, 2019. URL: https://doi.org/10.2991/senet-19.2019.34

170. Fayol H. Administration industrielle et générale; prévoyance, organisation, commandement, coordination, controle. Paris : Dunod et Pinat, 1917. 174 p.

171. Безгін К. С., Гришина І. В. Порівняльний аналіз процесного та функціонального підходів до управління підприємством. *Вісник економічної науки України*. 2009. № 2. С. 3-7.

172. Хринюк О. С., Солосіч О. С. Процесно-функціональний підхід до формування сучасних систем управління економічною безпекою підприємства. *Приазовський економічний вісник*. 2021. № 3(26). С. 87-91.

173. Мороз О. В., Сметанюк О. А. Фінансова діагностика у системі антикризового управління на підприємствах : монографія. Вінниця : Універсум, 2006. 167 с.

174. Василик Н. М. Впровадження та розвиток стрес-менеджменту в організації. *Ефективна економіка*. 2022. № 2. URL: http://www.economy.nayka.com.ua/?op=1&z=10034 (дата звернення: 17.03.2024). DOI: 10.32702/2307-2105-2022.2.91

175. Кривов'язюк І. В. Антикризове управління підприємством : навчальний посібник. Київ : Видавничий дім "Кондор", 2020. 396 с.

176. Кузьмін О. Є., Мельник О. Г., Адамів М. Є. Антисипативне управління підприємствами: процесно-структурований підхід. *Економіка: реалії часу*. 2012. № 2(3). С. 71-77. URL: http://www.economics.opu.ua/n3.html

177. Адамів М. Є. Сутність та роль антисипативного управління на підприємствах. *Галицький економічний вісник*. 2010. № 3(28). С.112-121.

178. Швець Ф.Д. Методологія та організація наукових досліджень. Навчальний посібник. Рівне : НУВГП, 2016. 151 с.

179. William C. A., James L. M. Anticipatory Management: Tools for Better Decision Making. *The Futurist*. 1997. № 31(5). P. 47-50. URL: http://www.entrepreneur.com/tradejournals/article/182930117_2.html

180. Економічна енциклопедія : У трьох томах. Т. 1. Київ: Видавничий центр „Академія". 2000. 864 с/

181. Руденський Р. А. Моделювання процесів антисипативного управління економічною безпекою : автореф. дис. ... канд. екон. наук : 08.03.02. Донецьк, 2002. 16 с.

182. Тімінський О. Г. Технології адаптивного управління як механізм забезпечення ефективності організаційноуправлінських систем. *Управління розвитком складних систем*. 2016. № 27. С. 122–131.

183. Гладка О. М, Карпович І. М., Сінчук А. М. Моделі економічної динаміки для фахівців з інформаційних технологій : навчальний посібник. Рівне : РДГУ. 2019. 158 с.

184. Костюк Т. О. Виробнича складова економічної безпеки сільського господарства: теорія і практика. *Економічний вісник Донбасу*. 2017. № 2(48). С.

105-112. URL: http://www.evd-journal.org/download/2017/2(48)/pdf/12-Kostuyk.pdf

185. Марченко О. С. Економічна безпека підприємства : навч. посіб. Харків : Право, 2022. 246 с.

186. Надтока Т., Амельницька О. Енергетична безпека підприємства як інструмент забезпечення його сталого соціально-економічного розвитку. Економіка та організація управління. 2010. № 2(8). С. 15–24

187. Матвійчук Н. М. Коленда Н. В. Сидорук С. В. Енергетична безпека підприємства як інструмент забезпечення його сталого розвитку. *Економіка і суспільство*. 2019. №. 20. С. 317-323.

188. Чорна О. Ю. Основні функціональні складові економічної безпеки інтегрованої промислової структури. *Вісник східноукраїнського національного університету імені Володимира Даля*. 2016. № 6(230). С. 187-193.

189. About zero waste. *Zero Waste Europe*. URL: https://zerowasteeurope.eu/about/about-zero-waste/

190. European Circular Economy Stakeholder Platform. *European Union.* URL: https://circulareconomy.europa.eu/platform/en/dialogue/existing-eu-platforms/c-servees

191. Тітенко З. Інноваційна складова фінансової безпеки підприємств. *Економіка та суспільство.* 2023. № 48. URL: https://doi.org/10.32782/2524-0072/2023-48-14

192. Перерва П. Г. Романчук Т.В. Інноваційна діяльність як чинник економічної безпеки промислового підприємства. Інструменти та методи комерціалізації інноваційної продукції : монографія. Суми : Триторія, 2018. Розд. 2.1. С. 56-74

193. Тертична Л. І., Безпалько О. В., Рибак Н. О. Політико-правова безпека підприємства: сутність, діагностика її рівня. *Науковий вісник Херсонського державного університету*. 2018. № 32. С. 117-121.

194. Зайченко К. С. Економічна безпека підприємства: сутність та роль. *Ефективна економіка*. 2021. № 5. URL: http://www.economy.nayka.com.ua/pdf/5_2021/92.pdf

195. Кравчик Ю. В., Каткова Т. І. Структурно-функціональна характеристика економічної безпеки промислового підприємства. *Innovation and sustainability*. 2022. Vol. 1. С. 84-95

196. Равлінко З. П. Інтелектуально-кадрова безпека торговельного підприємства: теоретичні засади забезпечення. *Цифрова економіка та економічна безпека*. 2022. № 2(02). С. 168–172. URL: https://doi.org/10.32782/dees.2-28

197. Пуйда Г. В. Комплексний аналіз філософсько-економічної дефініції "інтелектуальна безпека підприємства". *Економічний аналіз* : зб. наук. праць. 2017. Т. 27, №4. С. 261–272.

198. Воронько-Невіднича Т., Демиденко Л., Здоров В. Особливості формування та забезпечення кадрової безпеки підприємства. *Економіка та суспільство*. 2021. № 28. URL: https://doi.org/10.32782/2524-0072/2021-28-57

199. Гусєва О.Ю., Захаржевська А.А. Діагностика розвитку управління ризиками телекомунікаційних підприємств. *Бізнес Інформ*. 2023. № 1. С. 196-202. URL: http://nbuv.gov.ua/UJRN/binf_2023_1_29

200. Кузьомко В. М. Концептуальні підходи до виокремлення функціональних складових економічної безпеки підприємства. *Формування ринкової економіки* : зб. наук. пр. Київ : КНЕУ, 2011. Вип. 26, ч. 1. С. 206–215.

201. Капелюшна Т. В., Стріканов Д. О. Інформаційна безпека підприємства: важливість дотримання міжнародних стандартів безпеки. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу* : матеріали IV всеукр. наук.-практ. конф., м. Київ, 28 лют. 2024 р. Київ, 2024. С. 277-280. *(0,16 д.а., авторський внесок 0,12 д.а., полягає в дослідженні стандартів управління інформаційною безпекою підприємства).*

202. Капелюшна Т. В. Актуалізація питань інформаційної та кібернетичної безпеки підприємства в діджитал-умовах. *Глобалізаційні процеси та їх вплив на*

соціально-економічний та правовий розвиток України : зб. матеріалів II всеукр. наук.-теор. конф., Київ 20 груд. 2023 р. Київ, 2023. С.92-93. *(0,1 д.а.).*

203. Resistência. Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/portuguese-english/resistencia

204. Капелюшна Т. В. Багаторівневий захист даних підприємств критичної інфраструктури задля зменшення поверхонь атак. *"Забезпечення кібероборони держави" Національного університету оборони України:* матеріали IV наук.-практ. вебінару, *м. Київ,* 10 лист. 2023 р. Київ, 2023. С. 62-65. URL: https://drive.google.com/file/d/1VpULkcweKcyZ-KR8EvxtxQSGYbyS1JSq/view *(0,16 д.а.).*

205. Yakymenko Yu., Rabchun D., Kapeliushna T. Use of methodological approaches of system analysis to ensure information security of critical infrastructure objects. *Challenges and threats to critical infrastructure : Collective monograph.*. Detroit : NGO Institute for Cyberspace Research, 2023. P. 46-51. URL: https://conference.cyberspace.org.ua/wp-content/uploads/2023/06/Monograph-09-06-2023.pdf#page=46 *(0,36 д.а., авторський внесок 0,12 д.а., в частині пропозицій проведення системного аналізу безпеки функціонування підприємств).*

206. Капелюшна Т. В. Роль інноваційного підприємства в умовах нового технологічного укладу. *Економіка. Менеджмент. Бізнес.* 2019. № 3(29). С. 71-77. URL: https://doi.org/10.31673/2415-8089.2019.037177 *(0,42 д.а.).*

207. Конверський А. Є. Основи методології та організації наукових досліджень: навч. посіб. для студентів, курсантів, аспірантів і ад'юнтів. Київ: Центр учбової літератури, 2010. 352 с.

208. Пильнова В. П., Гавриш О. М., Капелюшна Т. В. Формування системи управління підприємницькими ризиками. *Інвестиції: практика та досвід.* 2020. № 24. С. 51-57. URL: http://www.investplan.com.ua/?op=1&z=7258&i=6 *(0,38 д.а., авторський внесок 0,13 д.а., полягає в обґрунтуванні доцільності інвестування ризикових інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).*

209. Сінчук О.М., Берідзе Т.М., Барановська Л.М. Данілін О.В., Кальмус О.Д. Безпека підприємства. Кременчук. 2022. 196 с.

210. Про затвердження Указу Президента України "Про введення воєнного стану в Україні" : Закон України від 24.02. 2022 р. № 2102-IX. URL: https://zakon.rada.gov.ua/laws/show/2102-20#Text

211. Господарський кодекс України: від 16.01.2003 р. URL: https://zakon.rada.gov.ua/laws/show/436-15#Text

212. Quantification, n. *Oxford english dictionary*. 3rd ed. 2023. URL: https://doi.org/10.1093/oed/1188788129

213. Kapeliushna T. Organizational Mechanism for the Formation of an Innovative Enterprise in the Conditions of a New Technological Structure. *Science and Education a New Dimension.* 2019. Vol. VII, Is. 213, №. 35. P. 16-19. URL: https://doi.org/10.31174/send-hs2019-213vii35-03 *(0,42 д.а.).*

214. Дименко Р. А., Капелюшна Т. В., Лобань О. О. Ризики впровадження та проблеми правового регулювання цифрової валюти в Україні. *Економіка. Менеджмент. Бізнес.* 2019. № 2(28). С. 72-79. URL: https://journals.dut.edu.ua/index.php/emb/article/view/2153 *(0,68 д.а., авторський внесок 0,22 д.а., полягає в аналізі ризиків впровадження та безпеки цифрової валюти).*

215. Капелюшна Т. В., Згурська О. М. Динаміка розвитку інтернет-речей та їх вплив на управління підприємствами. *Економіка. Менеджмент. Бізнес.* 2018. № 3(25). С. 79-86. URL: https://journals.dut.edu.ua/index.php/emb/article/view/1943 *(0,41 д.а., авторський внесок 0,21 д.а., полягає в дослідженні ризиків, додаткових можливостей та безпеки використання інтернет-речей в управлінні підприємствами).*

216. Голобородько А. Ю., Капелюшна Т. В. Формування цифровізації інтегративного розвитку економіки та підприємств, як її елементів. *European Journal of Economics and Management.* 2022. Т. 8, № 6. С.5-13. URL: https://doi.org/10.46340/eujem.2022.8.6.1 *(0,88 д.а., авторський внесок 0,08 д.а.,*

полягає в обґрунтуванні імперативів цифровізації економіки та розвитку підприємств).

217. Капелюшна Т. В. Роль технологій у розбудові фондового ринку. *Телекомунікаційний простір XXI сторіччя: ринок, держава, бізнес* : матеріали I міжнар. наук.-прак. конф., м. Київ, 18-19 груд. 2019 р. Київ, 2019. С. 33-38. *(0,2 д.а.).*

218. Капелюшна Т. В. Формування площини безпеки підприємства під дією ризиків і загроз. *Бізнес інформ.* 2024. Т. 3, № 554. С. 255–262. URL: https://doi.org/10.32983/2222-4459-2024-3-255-262 *(0,42 д.а.).*

219. Єршова Н. Ю. Науково-теоретичні проблеми діагностики в процесах управління сучасним підприємством. *Вісник ДДФА*. Сер.: Економічні науки. 2012. № 1 (27). С. 168–173.

220. Ваніна Д.А. Методи управління ризиками в страхових організаціях. *Науковий вісник Одеського національного економічного університету*. 2015. № 3. С. 16–28.

221. Lee, H. COSO ERM Framework. *Risk Management. Springer Texts in Business and Economics*. Springer, Singapore. 2021. URL: https://doi.org/10.1007/978-981-16-3468-0_4

222. Masood, Omar, et al. Enterprise Risk Management Program Effectiveness, Determinants, Execution and effect on Financial Performance: Evidence from Global Takaful Industry. *Journal of Islamic Financial Studies*. Dec. 2020vol. 6, no. 2, pp. 77+. URL: https://go.gale.com/ps/i.do?p=AONE&u=anon~3912a3c9&id=GALE|A680990156&v=2.1&it=r&sid=googleScholar&asid=c3b19cd8%20.

223. ISO 31000. Risk management — Guidelines. 2018. URL: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

224. Карпович І.М, Гладка О.М., Наконечна Ю.А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: технічні науки. 2020. Том 31 (70). № 5. С. 69-74. https://www.tech.vernadskyjournals.in.ua/journals/2020/5_2020/14.pdf

225. Дука А. П. Картографування ризиків у системі інтегрованого ризик-менеджменту організації. *Ефективна економіка*. 2017. № 10. http://www.economy.nayka.com.ua/?op=1&z=5794

226. Капелюшна Т. В. Пропозиції щодо упередження ризиків інформаційних активів задля захисту репутації підприємства. *Перспективи та проблематика інтелектуальних систем* : зб. наук.-практ. конф., м. Київ, 31 трав. 2024 р. Київ, 2024. С. 54-55. *(0,1 д.а.).*

227. Капелюшна Т. В. Заходи щодо захисту інформаційного середовища підприємства. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу* : матеріали IV всеукр. наук.-практ. конф., м. Київ, 28 лют. 2024 р. Київ, 2024. С.105-108. *(0,15 д.а.).*

228. Капелюшна Т. В. Іванов Д. А. Врахування репутаційних ризиків при управлінні інформаційною безпекою компанії. *Актуальні проблеми кібербезпеки* : матеріали всеукр. наук.-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 125-127. URL: https://duikt.edu.ua/uploads/p_2626_52007398.pdf#page=125. *(0,16 д.а., авторський внесок 0,12 д.а., полягає в дослідженні впливу репутаційних ризиків на безпеку підприємства).*

229. Про затвердження Положення про вимоги до системи управління страховика : Постанова, Положення, Національний банк України, від 27.12.2023. № 194. https://ips.ligazakon.net/document/pb23255?an=53&scop=11868&fcop=12167

230. Макарчук І., Федулова І. Управління ризик-апетитом у прийнятті рішень. *Scientia·fructuosa*. 2023. 147(1), с. 42–54. https://doi.org/10.31617/1.2023(147)04

231. Шишкіна О. В. Концептуальні основи визначення схильності до ризику промислових підприємств. *Науковий вісник Ужгородського національного університету*. 2019. Випуск 28, Ч.2. С. 153-157.

232. Капелюшна Т. В. Системи управління бізнесом – невід'ємна складова оптимізації бізнес-процесів. *Нові інформаційні технології управління бізнесом* :

матеріали VI всеукр. наук.-практ. конф., м. Київ, 16 лют. 2022 р. Київ, 2022. С. 113-116. URL: http://unionba.com.ua/osvita *(0,15 д.а.).*

233. Капелюшна Т. В., Хуторна А. В. Формування товарного асортименту на підприємствах. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку :* матеріали III міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 37- 40. *(0,17 д.а., авторський внесок 0,12 д.а., полягає в дослідженні конкрентоспроможності як орієнтиру безпеки підприємства за рахунок клієнтоорієнтованого асортименту).*

234. Караєва Н.В. *Еколого-економічний ризик-менеджмент: методи оцінювання ризиків* : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2019.

235. Kapeliushna T., Lehominova S., Goloborodko A., Lysetskyi Yu., Nosova T. Methodological approaches to enterprise security management: traditional and transformed to the conditions of functioning. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024. №. 3. P. 204-209. URL: https://doi.org/10.33271/nvngu/2024-3/204. *(0,99 д.а., авторський внесок 0,2 д.а., полягає в аналізі методичних підходів до управління безпекою підприємства).*

236. Panciatici P. Security management under uncertainly: From day-ahead planinning to intraday operation. *Bulk power system dynamics and control.* 2010. № 8. P. 1-8. URL: https://www.academia.edu/82866698/Security_management_under_uncertainty_From_day_ahead_planning_to_intraday_operation?email_work_card=title.

237. Капелюшна Т. В. Методологічний концепт управління безпекою підприємства. *Інвестиції: практика та досвід.* 2024. № 10. С. 69-74. URL: https://doi.org/10.32702/2306-6814.2024.10.69 *(0,4 д.а.).*

238. Капелюшна Т. В. Підхід до оцінки ефективності механізму управління підприємством в контексті сталого розвитку. *Економіка. Менеджмент. Бізнес*. 2016. № 2(16). С. 62-68. URL: https://journals.dut.edu.ua/index.php/emb/article/view/650 *(0,37 д.а.).*

239. Zosym Maxym. Метод Дельфі (Delphi method). URL: https://www.maxzosim.com/delphi-method/

240. Васильєва Т.А. Кривич Я.М. Економічний ризик: методи оцінки та управління : навч. посібник. Суми : ДВНЗ “УАБС НБУ”, 2015. 208 с.

241. Економічні ризики: методи вимірювання та управління: навч.пос. / Скопенко Н.С., Федулова І.В., Мазник Л.В., Кириченко О.М., Удворгелі Л.І. Київ : НУХТ, 2021. 344 с.

242. Зянько В.В. Методи аналізу фінансових ризиків суб’єктів господарювання. *Економічний вісник Запорізької державної інженерної академії*. 2017. Випуск 1-1 (07). с.99-102.

243. Економічний ризик: методи оцінки та управління: навч. посібник / Васильєва Т. А., Лєонов С. В., Кривич Я. М. та ін. Суми : ДВНЗ “УАБС НБУ”, 2015. 208 с.

244. Петрова В. Ф. Методичне забезпечення оцінки ризиків підприємства. *Соціальна економіка*. 2015. Вип. 50, , №2. С.148-153.

245. Балджи М. Д. Економічний ризик та методи його вимірювання: навч. пос. Харків: Промарт, 2015. 300 с.

246. Nitank Rastogi , Trivedi. M.K. PESTLE Technique – a Tool to identify external Risks in Construction Projects. *International Research Journal of Engineering and Technology*. Jan-2016. Volume: 03. Issue: 01. P. 384-388.

247. PEST Analysis Ultimate Guide: Definition, Template, Examples. URL: https://pestleanalysis.com/pest-analysis

248. Капелюшна Т. В., Ткаченко І. С. Private label як дієвий захід формування товарного асортименту. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали II міжнар. наук.-практ. конф., м. Київ, 11–12 лют. 2021 р. Київ, 2021. С. 189-193. *(0,17 д.а, авторський внесок 0,13 д.а. полягає у формуванні власної товарної марки для гарантування й забезпечення інтересів споживачів).*

249. Мельник К.М. Фінансові інтереси підприємства як основа забезпечення його фінансової безпеки. *Економіка, фінанси, менеджмент: актуальні питання науки і практики.* 2015, №2. С.38-45.

250. Висновок антикорупційної експертизи проєкту Закону України “Про електронні комунікації”. URL: https://nazk.gov.ua/uk/documents/27645/

251. Мінцифри – підсумки 2023. URL: https://www.kmu.gov.ua/news/mintsyfry-pidsumky-2023

252. IT-індустрія України 2023: адаптивність та стійкість під час війни. *IT research Ukraine*. URL: https://itcluster.lviv.ua/projects/it-research-ukraine/

253. Kovshova I., Dubovyk N., Kyryliuk N. Tendencies of Telecommunication Companies Development in the Conditions of Ukrainian Society Digitalization. *International Journal of Management and Humanities*. 2020. № 4, Issue 9. P. 124-130.

254. Recorded Future продовжує надавати критично важливі розвіддані для захисту України від кібер-, фізичних та кінетичних загроз. *Міністерство цифрової трансформації України.* URL: https://thedigital.gov.ua/news/recorded-future-prodovzhue-nadavati-krit…

255. Цифрова трансформація економіки України в умовах війни. Грудень 2023 року. НІСД. URL: https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-hruden-2023

256. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

257. Капелюшна Т.В. Інноваційні інструменти інтернет-реклами в умовах інформатизації та цифровізації суспільства. *Розвиток економіки та бізнес-адміністрування: наукові течії та рішення :* матеріали III Міжнародної науково-практичної конференції 20-25 травня 2022 р. Том 1. Київ: НАУ, 2022. С. 55-57.

258. Капелюшна Т.В. Системи управління бізнесом - невід’ємна складова оптимізації бізнес-процесів. *Нові інформаційні технології управління бізнесом:* Матеріали VI Всеукраїнської науково-практичної конференції. Київ, 2022. С. 113-116. URL: http://unionba.com.ua/osvita

259. Капелюшна Т. В., Берегова В. О. Переваги ведення підприємницької діяльності в інтернет за сучасних невизначених умов. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку:* матеріали III Міжнародної науково-практичної конференції. Київ, 2022. С. 132-139.

260. Капелюшна Т. В. Упередження від кібернетичних загроз підприємств критичної інфраструктури за використання систем їх контролю. *Шкідливі програми як загроза об'єктам критичної інфраструктури в умовах кібервійни:* збірник матеріалів міжвідомчого круглого столу. Київ : ІСТЕ СБУ, 2023. С.63-66.

261. Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку : Постанова від 31.05.2023 № 218. URL: https://zakon.rada.gov.ua/laws/show/z1229-23#Text

262. Деякі питання об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n42

263. Ranking mobile and fixed broadband speeds from around the world on a monthly basis. *Speed Test Global Index*. URL: https://www.speedtest.net/global-index/ukraine#fixed

264. Identify key data about internet performance. *Recent Ookla Research*. URL:https://www.ookla.com/research

265. Рейтинг інтернет-провайдерів. URL:https://2ip.ua/ua/services/providers-rating?act=1&asid=21219

266. Лист № 95 від 30.10.2023 Мінцифри щодо негативних наслідків від рекомендації щодо необхідності якнайшвидшого переходу споживачів на PON-мережі. *Ukrainian internet associaton*. URL: https://inau.ua/document/lyst-no-95-vid-30102023-mintsyfry-shchodo-nehatyvnykh-naslidkiv-vid-rekomendatsiyi-shchodo

267. Реєстр Інтернет-провайдерів України. *UABlocklist*. URL: https://uablocklist.com/providers

268. Код ведення економічної діяльності. *Держстат*. URL: https://stat.gov.ua/uk/datasets/aktyvy-vlasnyy-kapital-zobovyazannya-ta-finansovi-rezultaty-pidpryyemstv-0

269. Питання ведення реєстру постачальників електронних комунікаційних мереж та послуг : постанова Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку постанова URL: https://ips.ligazakon.net/document/re37838?an=606

270. Про врахування висловлених органом державної реєстрації зауважень до постанови Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку, від 16 серпня 2023 року N 314 : Постанова від 06.09.2023 № 343 URL: https://ips.ligazakon.net/document/view/re40634?an=1&ed=2023_09_06

271. Питання ведення реєстру постачальників електронних комунікаційних мереж та послуг. 20.04.2022 № 30 : Постанова Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку. URL: https://zakon.rada.gov.ua/laws/show/z0502-22#Text

272. Україна у цифрах за 2021 рік. Статичтичний збірник. Київ : Державна служба статистики України. URL: https://www.ukrstat.gov.ua/druk/publicat/kat_u/2022/zb/08/zb_Ukraine%20in%20figures_21u.pdf

273. Harris S. Unleashing the Full Potential of SDN and NFV. *BroadBand Library*. URL: https://broadbandlibrary.com/cloud-powered-pon/

274. Recommendation ITU-T G.9802.1 (2021) Amd. 1 (02/2023). SERIES G: Transmission systems and media, digital systems and networks. *ITUPublications*. URL: https://www.itu.int/rec/T-REC-G.9802.1-202302-I!Amd1/en

275. Key WDM-PON Technologies for 5G Fronthaul. *ZTE*. URL: https://www.zte.com.cn/global/about/magazine/zte-technologies/2017/5/en_734/465614.html

276. ITU-T G.989.3 40-Gigabit-capable passive optical networks (NG-PON2): Transmission convergence layer specification. *ITU*. URL: https://handle.itu.int/11.1002/1000/14635

277. Z. Song, C. M. Hackl, A. Anand, A. Thommessen, J. Petzschmann, O. Kamel, R. Braunbehrens, A. Kaifel, C. Roos, S. Hauptmann. Digital Twins for the Future Power System: An Overview and a Future Perspective. *Sustainability*. 2023. Vol.15, no.6. P. 5259.

278. A. Simmons. Software-Defined Networking (SDN) Explained. *GtlInfra*. URL: https://dgtlinfra.com/software-defined-networking-sdn/

279. Average global mobile and fixed broadband download & upload speed worldwide 2024. *Statista*. URL: https://www.statista.com/statistics/896779/average-mobile-fixed-broadband-download-upload-speeds/

280. Veon. URL: https://www.veon.com/

281. Telecommunications services - statistics & facts. *Statista*. URL: https://www.statista.com/topics/2665/telecommunications-services/#topicOverview

282. Оптичний інтернет у ваш дім (GPON). *Київстар*. URL: https://kyivstar.ua/home-internet/service/gpon

283. Тарифи Vodafone – Вигідні тарифні плани. *Vodafone Україна*. URL: https://www.vodafone.ua/rates

284. Уарнет. URL: https://uar.net/

285. Volia. URL: https://volia.com/ukr/internet/

286. Lifecell. URL: https://www.lifecell.ua/uk/

287. UkrTelecom. URL: https://ukrtelecom.ua/internet/)

288. Triolan.NET: Інтернет. *Triolan*. URL: https://triolan.com/net.aspx?lng=uk&reg=kh

289. Оптоволоконний зв'язок. *Fregat*. URL: https://fregat.com/optics/

290. Оптичний Інтернет в квартиру. *Lanet*. URL: https://www.lanet.ua/pon/

291. Про компанію. *O3*. URL: https://o3.ua/about/

292. Тарифи INTERNET. Вартість інтернет-пакетів і підключення. First Telecommunication Company. URL: https://ftc.company/tarifs-2/

293. Фіксований інтернет в Києві. *Data group*. URL: https://www.datagroup.ua/kiev/b2c/internet/fiksovanij-internet

294. Інтернет і кабельне TV від провайдера Інформаційні Технології. *IT-TV*. URL: https://www.it-tv.org/ua/

295. Питання ведення реєстру постачальників електронних комунікаційних мереж та послуг: постанова Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку від 20 квітня 2022 року № 30. URL: https://zakon.rada.gov.ua/laws/show/z0502-22#n122

296. Individuals who own a mobile cellular telephon Ukraine. *DataHub*. URL: https://datahub.itu.int/data/?e=UKR&c=701&i=20719&d=Gender

297. Кількість ліній фіксованого доступу до Інтернет зросла на 12%. *HiTech Expert*. URL: https://expert.com.ua/180191-kilkist-liniy-fiksovanogo-dostupu-do-internet-zrosla-na-12.html

298. ЗВІТ про діяльність Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку за 2022 рік. *Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку*. URL: https://nkrzi.gov.ua/images/upload/142/10509/Dodatok_do_rishennia_NKEK_29.03.2023__125.pdf

299. Дохід інтернет-провайдерів в Україні минулого року зріс на 25% - НКЕК. Mediasat. URL: https://mediasat.info/uk/2024/03/28/dohid-internet-provajderiv-v-ukrayini-mynulogo-roku-zris-na-25-nkek/

300. Дохід провайдерів фіксованого інтернету в Україні у 2023 році зріс на 25% - НКЕК. Interfax-Україна. URL: https://interfax.com.ua/news/telecom/976597.html

301. Individuals who own a mobile cellular telephone. DataHub ITU. URL: https://datahub.itu.int/data/?e=UKR&Markets=Spectrum&Affordability=ICT+prices&Connectivity=International+roaming&Sustainability=Environment+%26+e-waste&Trust=Cybersecurity

302. Big Data methods for SDG indicators. UNBigData. URL: https://unstats.un.org/bigdata/task-teams/sdgs/indicators.cshtml

303. НКЕК. Реєстр постачальників електронних комунікаційних мереж та/або послуг. *Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку*. URL: https://nkrzi.gov.ua/index.php?r=site/index&pg=55&language=uk

304. Телекомунікації України. *YO MARKET Catalog*. URL: https://catalog.youcontrol.market/telekomunikatsii

305. Звіт про діяльність Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку за 2023 рік. *Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку*. URL: https://skilky-skilky.info/wp-content/uploads/2024/04/Zvit-pro-diialnist-NKEK-za-2023-rik.pdf

306. Галузь телекомунікацій: цифри та факти. *Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку*. URL: https://nkrzi.gov.ua/index.php?r=site/index&pg=138&language=uk

307. Офіційний сайт компанії "Київстар". Про нас. *Kyivstar* URL: https://kyivstar.ua/about

308. Офіційний сайт міжнародної групи VEON. We are VEON. *VEON*. URL: https://www.veon.com/investors/#tab-item-104

309. Офіційний сайт компанії "Київстар". Інформація для стейкхолдерів. *Kyivstar* URL: https://kyivstar.ua/about/investors-and-shareholders/issuers

310. Strong organic growth in revenue and ebitda solid execution of VEON 2.0 strategy. *VEON*. URL: https://www.veon.com/fileadmin/user_upload/investors/reports/2024/4Q23_PRESENTATION.pdf

311. Empowering digital futures. Integrated Annual Report 2020. *VEON*. URL: https://www.veon.com/fileadmin/user_upload/investors/reports/2021/veon_2020-integrated_annual-report.pdf

312. Прокопець Н.А. Енергоефективне обслуговування навантаження інформаційно-комунікаційної мережі : дис. ... д-а філ. : 172. Київ, 2022. URL: https://ela.kpi.ua/server/api/core/bitstreams/3626b73f-0610-495e-bc89-a64f469b8df9/content

313. Про затвердження Положення про якість телекомунікаційних послуг : рішення Національної комісії з питань регулювання зв'язку України від 15.04.2010 №174. URL: https://zakon.rada.gov.ua/laws/show/z0429-10#Text (Дата звернення 12.08.2021)

314. Капелюшна Т. В., Мізецький М. М. Підхід до забезпечення економічної стійкості у бізнес-процесах підприємства. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали II міжнар. наук.-практ. конф., м. Київ, 11–12 лют. 2021 р. Київ, 2021. С. 28- 31. *(0,13 д.а., авторський внесок 0,1 д.а. полягає у дослідженні підходів до забезпечення економічної стійкості підприємств як гарантій безпеки функціонування підприємства та його розвитку).*

315. Капелюшна Т. В. Концепція міжнародного управління в сучасних умовах. *Сучасні тенденції розвитку світової економіки* : зб. тез доп. X міжн. наук.-практ. конф., м. Харків, 18 трав. 2018 р. Харків, 2018. С. 130. *(0,09 д.а.).*

316. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест. .№ 8 (серпень). Київ : Державна наукова установа “Інститут інформації, безпеки і права НАПрН України”, 2023. 318 с. https://ippi.org.ua/sites/default/files/2023-8.pdf

317. Хлапонін Ю. І., Козубцова Л. М., Козубцов І. М, Щтонда Р. М. Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка.* 2022. № 3(15). С. 124-134. URL: https://lib.iitta.gov.ua/734869/1/Khlaponin_Kozubtsova_Kozubtsov_Shtonda..pdf.

318. Дем’янчук М. А. Збалансований розвиток телекомунікаційного підприємства в умовах цифрових трансформацій: теорія, методологія, практика : дис. ... д-ра екон. наук : 08.00.04. Херсон, 2020. С. 381

319. Зведена карта покриття всіх 3G/4G операторів в Україні. *V3G*. URL: https://v3g.com.ua/karta-pokrytyya-all

320. Капелюшна Т. В. Безпека даних підприємства у хмарному середовищі: аналіз загроз. *Облік і фінанси*. 2023. № 4(102). С. 97-104. URL: https://afj.org.ua/ua/journals/2023/4/ *(0,49 д.а.).*

321. Капелюшна Т. В. Врахування впливу загроз соціальної інженерії при управлінні безпекою підприємства. *Інвестиції: практика та досвід*. 2023. № 8. С. 125-130. URL: https://www.nayka.com.ua/index.php/investplan/article/view/1374/1384 *(0,36 д.а.).*

322. Капелюшна Т. В., Гавриш О. М. Проблеми неформального інвестування інноваційного підприємництва в Україні. *Ефективна економіка.* 2020. № 12. URL: http://nbuv.gov.ua/UJRN/efek_2020_12_69 *(0,68 д.а., авторський внесок 0,36 д.а., полягає в обґрунтуванні доцільності інвестування ризикових інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).*

323. Пильнова В. П., Гавриш О. М., Капелюшна Т. В. Організація експорту товарів суб’єктами малого та середнього бізнесу. *Агросвіт.* 2020. № 24. С. 29–36. URL: http://www.agrosvit.info/pdf/24_2020/5.pdf *(0,8 д.а.,*

авторський внесок 0,26 д.а., полягає в обґрунтуванні доцільності експорту як заходу захисту та убезпечення підприємства від зменшення продажів на внутрішньому ринку).

324. Гавриш О. М, Згурська О. М., Капелюшна Т. В., Мартиненко М. О. ІТ-послуги як об'єкт міжнародної торгівлі. *Міжнародний науковий журнал "Інтернаука". Серія:"Економічні науки"*. 2020. № 11. URL: https://www.inter-nauka.com/ua/issues/economic2020/11/6585 *(0,7 д.а., авторський внесок 0,16 д.а., полягає в формуванні безпекових засад надання ІТ послуг на зовнішніх ринках).*

325. Капелюшна Т. В., Гавриш О. М., Пильнова В. П. Діагностика та тенденції розвитку міжнародної торгівлі в Україні. *Ефективна економіка.* 2020. № 11. URL: http://www.economy.nayka.com.ua/?op=1&z=8379 *(0,65 д.а., авторський внесок 0,23 д.а., полягає в означення загроз безпеці підприємств з урахуванням тенденцій розвитку міжнародної торгівлі).*

326. Капелюшна Т. В., Воробей К. О. Метрики визначення оптимізації управління запасами на підприємствах. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми* та *перспективи розвитку* : матеріали III міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 32-35. *(0,18 д.а., авторський внесок 0,14 д.а. полягає у деталізації метрик оптимізації управління запасами підприємства для гарантування безпеки постачання й забезпечення безперебійного функціонування підприємств).*

327. Капелюшна Т. В., Дерев'янко Б. О. Дієві методи реклами в сучасних умовах функціонування підприємств. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку :* матеріали III міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 177-180. *(0,13 д.а. авторський внесок 0,1 д.а. полягає у моніторингу впливу реклами на результати діяльності підприємства та обґрунтування доцільності вкладень у рекламу).*

328. Капелюшна Т. В. Інноваційні інструменти інтернет-реклами в умовах інформатизації та цифровізації суспільства. *Розвиток економіки та*

бізнес-адміністрування: наукові течії та рішення : матеріали III міжнар. наук.-практ. конф., м. Київ, 20–25 трав. 2022 р. Київ, 2022. С. 55-57. *(0,14 д.а.).*

329. Капелюшна Т. В., Новикова І.В. Умови ефективного провадження е-торгівлі. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку:* матеріали II міжнар. наук.-практ. конф., м. Київ, 11–12 лют. 2021 р. Київ, 2021. С. 35- 40. *(0,14 д.а., авторський внесок 0,09 д.а. полягає у дослідженні податкових новацій та їх впливу на результати діяльності підприємства).*

330. Капелюшна Т. В. Податкові новації в умовах сьогоднішньої невизначеності. *Модернізація економіки: сучасні реалії, прогнозні сценарії та перспективи розвитку* : матеріали II міжнар. наук.-практ. конф., м. Херсон, 28 квіт. 2020 р. Херсон, 2020. С.701-703 *(0,12 д.а.).*

331. Капелюшна Т. В., Татаринський Г. О. Фіскальні інструменти як стимул для розвитку підприємств. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали I міжнар. наук.-практ. конф., м. Київ, 11 лют. 2020 р. Київ, 2020. С. 35-36. *(0,08 д.а., авторський внесок 0,06 д.а. полягає у дослідженні стимулювання розвитку підприємства за рахунок фіскальних інструментів).*

332. Капелюшна Т. В. Оцінювання динаміки рівня сталості розвитку підприємств. *Актуальні проблеми управління та економічного розвитку в умовах інформатизації суспільства*: матеріали наук.-практ. конф., м. Київ, 20 груд. 2016 р. Київ, 2016. С. 48-49. *(0,1 д.а.).*

333. Фінансова звітність. *Фрінет інтернет-оператор*. URL: https://o3.ua/about/documents/1606986593/#year-1334

334. Фінансові результати. *Vodafone*. URL: https://www.vodafone.ua/company/investors/zvity-ta-rezultaty/finansovi-rezultaty.

335. Фінансові результати. *Vodafone*. URL: https://www.vodafone.ua/company/investors/zvity-ta-rezultaty/finansovi-rezultaty

336. Фінансова звітність за 2006–2023 роки. *Kyivstar*. URL: https://kyivstar.ua/about/investors-and-shareholders/issuers

337. Фінансова звітність. *Укртелеком*. URL: https://ukrtelecom.ua/about/accounting/finansova-zvitnist/

338. Звіт незалежних аудиторів. *Укртелеком*. URL: https://ukrtelecom.ua/about/accounting/zvit-nezalezhnykh-audytoriv/

339. Річні звіти за МСФЗ. *LifeCell.* URL: https://www.lifecell.ua/uk/pro_lifecell/finansovi-ta-operacijni-dani/richni-zviti/

340. Квартальні результати. *LifeCell*. URL: https://www.lifecell.ua/uk/pro_lifecell/finansovi-ta-operacijni-dani/kvartalni-rezultati/

341. Про інформацію: Закон України від від 27.07.2023 № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

342. Царьов Р. Ю. Електронна комерція : навчальний посібник. Одеса : ОНАЗ ім. О.С. Попова, 2010. 112 с.

343. Шалева О. І. Електронна комерція: навчальний посібник. Київ : "Центр учбової літератури", 2011. 216 с.

344. Капелюшна Т. В. Забезпечення безпечного функціонування підприємств за сьогочасних викликів. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали IV Міжнар. наук.-практ. конф., м. Київ, 17 лютого 2023 р. Київ : ДУТ, 2023. С. 97-99.

345. Охріменко І.В. Забезпечення економічної безпеки агробізнесу в умовах збройної агресії. *Український економічний часопис*. 2024. № 4. С. 35–39. URL: https://doi.org/10.32782/2786-8273/2024-4-7

346. AXA Future Risks Report 2022. *Eurasia Group*. URL: https://www-axa-com.cdn.axa-contento-118412.eu/www-axa-com/15c65a87-4d11-49a4-b88e-be5953965b37_axa_futurerisksreport_2022_va.pdf (дата звернення: 12.10.2023).

347. Kapeliushna T. Enterprise security management under uncertainty: a threat control system. *Міжнародний історичний досвід повоєнної реконструкції економіки: уроки для України* : матеріали міжнар. наук.-практ. конф., м. Київ,

27 квіт. 2023 р. Київ, 2023. С. 90. URL: Mizhnar-istor-dosvid-povojen-reconstrukcii-uroky-dla-Ukrainy.pdf (ief.org.ua) *(0,06 д.а.)*.

348. Significant Cyber Incidents Since 2006. *CSIS*. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-09/230911_Significant_Cyber_Events_List.pdf?VersionId=pwkO6dlFR2EhIb5p_WUq5HCiK4Al_6XI (дата звернення: 22.11.2023).

349. Cyber Dimensions of the Armed Conflict in Ukraine. *CyberPeace Institute*. URL: https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf (дата звернення: 28.10.2023).

350. Cyber Dimensions of the Armed Conflict in Ukraine. *CyberPeace Institute*. URL: https://cyberpeaceinstitute.org/wp-content/uploads/2023/05/Ukraine-Report-Q1_FINAL.pdf (дата звернення: 09.11.2023).

351. Шевчук І., Депутат Б. Економічний аспект використання хмарних технологій у діяльності органів публічної влади та бізнес-структур. *Економіка та суспільство*. 2021. № 31. URL: https://doi.org/10.32782/2524-0072/2021-31-26 (дата звернення: 24.10.2023).

352. Нікітенко К. С., Осадчий А. А. Упровадження хмарних технологій у діяльність сучасних підприємств. *Підприємництво і торгівля.* 2022. № 27, С. 53-57. URL: https://doi.org/10.36477/2522-1256-2020-27-09

353. Mykhailovyna S., Matros O., Polishchuk O. Cloud technologies as an important aspect of the development of accounting and taxation. *Efektyvna ekonomika*. 2021. No. 8. URL: https://doi.org/10.32702/2307-2105-2021.8.86 (date of access: 10.10.2023).

354. M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, Sadaqat Ur Rehman. Cyberattacks and Security of Cloud Computing: A Complete Guideline. *Symmetry*. 2023. Vol. 15, no. 11. P. 1981. URL: https://doi.org/10.3390/sym15111981

355. Про хмарні послуги : Закон України від 17.02.2022 р. № 2075-IX. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text (дата звернення: 20.10.2023).

356. Cyberattacks Impact and Harm on the ICT sector | CyberPeace Institute. *Cyber Attacks in Times of Conflict | CyberPeace Institute*. URL: https://cyberconflicts.cyberpeaceinstitute.org/impact/sectors/ict (date of access: 12.11.2023).

357. Kapeliushna T., Dymenko R., Safonov Yu. Kachmala V., Borshch V., Sheremet O. Digital tools for effective student learning and training online in conditions of uncertainty. *Financial and Credit Activity Problems of Theory and Practice*. 2022. Vol. 6, No. 47. P. 469–479. URL: https://doi.org/10.55643/fcaptp.6.47.2022.3817. *(0,9 д.а., авторський внесок 0,15 д.а., полягає в означенні електронних комунікаційних послуг та технологій, як основи забезпечення безпечного функціонування господарюючих одиниць за умов невизначеності).*

358. Kryshtal H., Kapeliushna T., Kalina I., Shuliar N., Martynenko M. Trends of development of financial and economic activity of entrepreneurial structures during the period of quarantine restrictions. Naukovyi *Visnyk Natsionalnoho Hirnychoho Universytetu*. 2022. No. 1. P. 139–144. URL: https://doi.org/10.33271/nvngu/2022-1/139. *(0,74 д.а., авторський внесок 0,14 д.а., полягає в аналізі трендів безпеки та можливостей забезпечення безперебійної роботи підприємства в умовах пандемії).*

359. Zghurska O., Dymenko R., Semkina T., Kapeliushna T. Diversification Strategy of Entrepreneurial Activity in Conditions of European Integration. *International Journal of Innovative Technology and Exploring Engineering*. 2019. Vol. 9, no. 1. P. 4809–4815. URL: https://doi.org/10.35940/ijitee.j9443.119119. *(0,7 д.а., авторський внесок 0,14 д.а., полягає в формуванні безпекових орієнтирів у функціонуванні підприємств в умовах євроінтеграції).*

360. Капелюшна Т. В., Голобородько А. Ю. Врахування інформаційних викликів при управлінні безпекою підприємств у сьогоденних невизначених

умовах. *European Journal of Economics and Management.* 2023. Т. 9, № 1. С. 12-21. URL: https://doi.org/10.46340/eujem.2023.9.1.2 *(0,61 д.а., авторський внесок 0,31 д.а. полягає в обґрунтуванні врахування інформаційних викликів в управлінні безпекою підприємства).*

361. Бойко А. В., Шкуропадська Д. Б.,. Гладка Ю. А. Стійкість економіки: оцінювання та забезпечення : монографія. Київ : Київ. нац. торг.-екон. ун-т. 2021. 444 с.

362. Капелюшна Т. В., Кришталь Г. О., Ващенко О. О. Огляд та аналіз розвитку ринку державних боргових цінних паперів в Україні. *Ефективна економіка*. 2021. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=8811 *(0,7 д.а., авторський внесок 0,24 д.а., полягає в визначенні пріоритетних напрямів вкладення коштів в державні боргові цінні як найбільш безпечні з точки зору ризиків фінансових втрат).*

363. Капелюшна Т. В., Гавриш О. М., Дименко Р. А. Новації оподаткування підприємницької діяльності. *Інфраструктура ринку*. 2020. № 49. URL: http://www.market-infr.od.ua/uk/49-2020 *(0,75 д.а., авторський внесок 0,27 д.а., полягає в визначенні перспектив та ризиків в оподаткуванні для підприємств).*

364. Гавриш О. М., Пильнова В. П., Капелюшна Т. В. Планування торговельної діяльності підприємств на міжнародних ринках. *Підприємництво і торгівля*. 2020. № 27. С. 21-25. URL: http://journals- lute.lviv.ua/index.php/pidpr-torgi/article/view/699/664. *(0,68 д.а., авторський внесок 0,23 д.а., полягає в обґрунтуванні доцільності інвестування ризикових інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).*

365. Пильнова В. П., Гавриш О. М., Капелюшна Т. В., Лобань О. О. Інтернет-торгівля: особливості реалізації товару за допомогою інтернету. *Економіка. Менеджмент. Бізнес.* 2020. № 1. С. 122–130. URL: http://journals.dut.edu.ua/index.php/e mb/article/view/2394 *(0,51 д.а., авторський внесок 0,19 д.а., полягає в обґрунтуванні доцільності інвестування ризикових*

інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).

366. Капелюшна Т. В. Аналіз та тенденції розвитку фондового ринку в Європейському регіоні та Україні. *Бізнес Інформ.* 2019. Т. 12. № 503. С. 290-296. URL: https://doi.org/10.32983/2222-4459-2019-12-290-296 *(0,41 д.а.).*

367. Panciatici P. Operating in the Fog: Security Management Under Uncertainly. *IEEE Power and Energy Magazine*. 2012. P. 40-49. DOI: 10.1109/MPE.2012.2205318

368. Капелюшна Т. В. Чернявський І. Р. Проблема безпеки даних підприємства при використанні хмарних сервісів. *Актуальні проблеми кібербезпеки* : матеріали всеукр. наук.-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 134-135. URL: https://duikt.edu.ua/uploads/p_2626_52007398.pdf#page=134 *(0,1 д.а., авторський внесок 0,08 д.а., полягає в дослідженні проблематики забезпечення безпеки даних підприємства при їх розміщенні у хмарних сервісах).*

369. Капелюшна Т. В. Врахування впливу інформаційних атак на персонал задля безпеки підприємства. *"Telecommunication: problems and innovation"* : зб. тез всеукр. наук.-практ. конф. Київ, 2022. С.122-123. URL: https://dut.edu.ua/uploads/p_2121_16069800.pdf#page=122 *(0,1 д.а.).*

370. Утенкова К.О. Теоретичні засади формування методики експертної оцінки впливу окремих чинників на стан економічної безпеки анрарних підприємств. *Економіка та держава*. 2020. № 4. С. 133-140. DOI: 10.32702/2306-6806.2020.4.133.

371. Капелюшна Т. В. Проблеми та перспективи розвитку фондового ринку України. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку*: матеріали І міжнар. наук.-практ. конф., м. Київ, 11 лют. 2020 р. Київ : ДУТ, 2020. С. 220-223. *(0,15 д.а., авторський внесок 0,13 д.а. полягає у розгляді проблемних питань для компаній з управління активами на організованих ринках капіталу).*

372. Капелюшна Т. В. Практична підготовка фахівців з використанням програмних продуктів для автоматизації бізнесу в процесі навчання. *Нові інформаційні технології управління бізнесом* : матеріали III всеукр. наук.-практ. конф., м. Київ, 12 лют. 2020 р. Київ, 2020. С. 85-86. *(0,09 д.а.).*

373. Капелюшна Т. В. Аналіз державного боргу та оцінка механізму його управлінням. *Сучасні тенденції розвитку світової економіки* : зб. тез доп. IX міжн. наук.-практ. конф., м. Харків, 26 трав. 2017 р. Харків, 2017. С. 73. *(0,09 д.а.).*

374. Група хакерів здійснює деструктивні кібератаки на українських провайдерів – детальний аналіз інциденту від CERT-UA та рекомендації щодо захисту. *Державної служби спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/news/grupa-khakeriv-zdiisnyuye-destruktivni-kiberataki-na-ukrayinskikh-provaideriv-detalnii-analiz-incidentu-vid-cert-ua-ta-rekomendaciyi-shodo-zakhistu (дата звернення: 28.09.2023)

375. The Global Risks Report 2022. 17th Edition. *World Economic Forum*. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (дата звернення: 28.09.2023).

376. Індекс фінансового стресу. *Національний банк України*. URL: https://bank.gov.ua/ua/stability/fsi

377. Війна Росії проти України: хронологія кібератак. European Parliament. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf

378. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 12.03.2023).

379. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17.01.2018 № 67-р.

URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text. (дата звернення: 14.02.2023).

380. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція № 108 Ради Європи від 28 січня 1981 року. URL: https://www.convention.coe.int/treaty/en/Treaties/Html/108.htm. (дата звернення: 23.01.2023)

381. From electricity grid to broadband Internet: Sustainable and innovative power solutions for rural connectivity. *International Telecommunication Union*. URL: https://www.itu.int/dms_pub/itu-d/opb/tnd/D-TND-09-2023-01-PDF-E.pdf (дата звернення: 28.01.2023).

382. Капелюшна Т. В. Захист та безпека функціонування телекомунікаційних підприємств в умовах цифровізації та невизначеності. *Агросвіт*. 2023. № 7-8 С. 115-123. URL: https://www.nayka.com.ua/index.php/agrosvit/article/view/1351/1361

383. Яковів І. Кібернетична модель APT атаки. *Information technology and security*. 2018. Т. 6, № 1(10), С. 46–58. URL: https://doi.org/10.20535/2411-1031.2018.6.1.153140

384. Капелюшна Т.В. Управління безпекою підприємства в умовах невизначеності: система контролю загроз. Відбудова для розвитку: зарубіжний досвід та українські перспективи : міжнародна колективна монографія. Київ : ДУ "Ін-т екон. та прогнозув. НАН України", 2023. С. 474-486. URL: http://ief.org.ua/wp-content/uploads/2023/08/Reconstruction-for-development.pdf

385. Reference Incident Classification Taxonomy. *The European Union Agency for Cybersecurity*. URL: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

386. Глушко А. Д. Інформаційна політика в системі забезпечення фінансової безпеки держави. *Ефективна економіка,* 2022. № 2. URL: http://www.economy.nayka.com.ua/pdf/2_2022/97.pdf (дата звернення: 04.12.2022)

387. Капелюшна Т. В. Інформаційна складова в управлінні економічною безпекою діяльності підприємства. *Актуальні проблеми кібербезпеки* : матеріали Всеукр. наук.-практ. конф., м. Київ, 27 жовтня 2022 р. Київ : ДУТ, 2022. С. 171-172. URL: https://dut.edu.ua/uploads/p_2121_20358827.pdf#page=171. (дата звернення: 29.11.2022)

388. Індекс цін комунікаційних послуг за роками. *Міністерство фінансів.* URL: https://index.minfin.com.ua/ua/economy/index/serviceprice/

389. Reference Incident Classification Taxonomy. *The European Union Agency for Cybersecurity.* URL: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

390. Капелюшна Т.В. Врахування впливу загроз соціальної інженерії при управлінні безпекою підприємства. *Інвестиції: практика та досвід*. 2023. № 8. С.125-130.

391. Cost of a data breach 2023. *IBM*. URL: https://www.ibm.com/reports/data-breach (date of access: 14.11.2023).

392. Global Security as a Service market forecast 2022. *Statista*. URL: https://www.statista.com/statistics/595164/worldwide-security-as-a-service-market-size (date of access: 08.10.2023).

393. Quantum Economy Blueprint. Insight report January 2024. *World Economic Forum.* URL: https://www3.weforum.org/docs/WEF_Quantum_Economy_Blueprint_2024.pdf

394. NIST Announces First Four Quantum-Resistant Cryptographic Algorithms. *National Institute of Standards and Technology (NIST)*. URL: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-fourquantum-resistant-cryptographic-algorithms.

395. Cost of a data breach 2023. *IBM*. URL: https://www.ibm.com/reports/data-breach (date of access: 14.11.2023)

396. Global Security as a Service market forecast 2022. *Statista*. URL: https://www.statista.com/statistics/595164/worldwide-security-as-a-service-market-size (date of access: 08.10.2023).

397. Рибак А. П. Азарова. І.Б. Управління зацікавленими сторонами в проектному менеджменті : монографія. Одеса : ОДАБА, 2017. 145 с. ISBN 978-617-7195-42-8

398. Про затвердження Показників якості послуг із передачі даних, доступу до Інтернету та їх рівнів : Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 28.12.2012 №803. URL: https://zakon.rada.gov.ua/laws/show/z0135-13#Text (Дата звернення 30.06.2021)

399. ISO 8402:1994. Quality management and quality assurance. Vocabulary. 1994. URL: https://www.iso.org/ru/standard/20115.html

400. Капелюшна Т. В., Дименко Р. А. Експертна оцінка щодо надання телекомунікаційних послуг. *Ефективна економіка*. 2021. № 8. URL: http://www.economy.nayka.com.ua/?op=1&z=8811

401. Quantum Economy Network. *World Economik Forum.* URL: https://initiatives.weforum.org/quantum/home

402. Про компанію. Datagroup. https://www.datagroup.ua/pro-kompaniyu

403. Окрема фінансова звітність відповідно до Міжнародних стандартів фінансової звітності та звіт незалежного аудитора. *Київстар*. URL: https://cdn.kyivstar.ua/nkw/b2c/docs_about/2022/FS_Kyivstar_Stand_Alone_2022_UKR_NOT_signed.pdf?_gl=1*1wvdckf*_ga*MTIyMjY0ODQ3My4xNzExOTA0NjYx*_ga_T1JSNGQ6S4*MTcxNTY2OTMxNi41Mi4wLjE3MTU2NjkzMTYuNjAuMC4w*_gcl_au*MzYwNDg3MzU1LjE3MTE5MDQ2NjA.

404. Окрема фінансова звітність відповідно до Міжнародних стандартів фінансової звітності та звіт незалежного аудитора. *Київстар*. URL: https://cdn.kyivstar.ua/nkw/b2c/docs_about/2022/FS_Kyivstar_Stand_Alone_2022_UKR_NOT_signed.pdf?_gl=1*1wvdckf*_ga*MTIyMjY0ODQ3My4xNzExOTA0NjYx*_ga_T1JSNGQ6S4*MTcxNTY2OTMxNi41Mi4wLjE3MTU2NjkzMTYuNjAuMC4w*_gcl_au*MzYwNDg3MzU1LjE3MTE5MDQ2NjA

405. Фінансові результати. *Vodafone*. URL: https://www.vodafone.ua/company/investors/zvity-ta-rezultaty/finansovi-rezultaty

406. Фінансові результати. *Vodafone*. URL: https://www.vodafone.ua/company/investors/zvity-ta-rezultaty/finansovi-rezultaty

407. Консолідована фінансова звітність станом на і за рік, який закінчився 31 грудня 2019 р. *Vodafone*. URL: https://www.vodafone.ua/storage/editor/files/vf-ukraine-consolidated-19fsu-with-signatures_1609778813.pdf

408. Річні звіти за МСФЗ. *Lifecell*. URL: https://www.lifecell.ua/uk/pro_lifecell/finansovi-ta-operacijni-dani/richni-zviti/

409. Квартальні результати. *Lifecell*. URL: https://www.lifecell.ua/uk/pro_lifecell/finansovi-ta-operacijni-dani/kvartalni-rezultati/

410. Статистичний збірник. Міністерство Фінансів України. URL: https://mof.gov.ua/uk/statistichnij-zbirnik

411. An official website of the European Union. European Union. URL: https://european-union.europa.eu/contact-eu_uk

412. Sukhorukov A, Sukhorukova O. Structural Entropy of Economic System. *ELER2021* : The First International Conference on Economics, Law and Education Research. Kyiv, 2021. P. 30-34. URL: https://ela.kpi.ua/handle/123456789/41489

413. Wankhade L., Dabade B. Quality Uncertainty and Perception Information Asymmetry and Management of Quality Uncertainty and Quality Perception. *Springer*. Heidelberg Dordrecht London New York. 2010. P.137 DOI 10.1007/978-3-7908-2195-6

414. Stiglitz, J. E. Information and the Change in the Paradigm in Economics. Part 1. *The American Economist*. 2003. № 47(2), 6-26. https://doi.org/10.1177/056943450304700202

415. Claire Smith. Economics, ecology and entropy: The second law of thermodynamics and the limits to growth Human Sciences Press, Inc. Volume 17. № 4.1996. P.309-320.

416. Luciano De Castro, Nicholas C. Yannelis, Uncertainty, efficiency and incentive compatibility: Ambiguity solves the conflict between efficiency and incentive compatibility. *Journal of Economic Theory. Volume* 177. 2018. P. 678-707, https://doi.org/10.1016/j.jet.2018.02.008

417. Chen J. An Entropy Theory of Value. *SSRN Electronic Journal*. 2002. URL: https://doi.org/10.2139/ssrn.307442.

418. Chowdhury, S. N., Ray, A., Dana, S. K., & Ghosh, D. (2022). Extreme events in dynamical systems and random walkers: A review. Physics Reports, № *966*, 2022. P. 1-52.

ДОДАТКИ

ДОДАТОК А

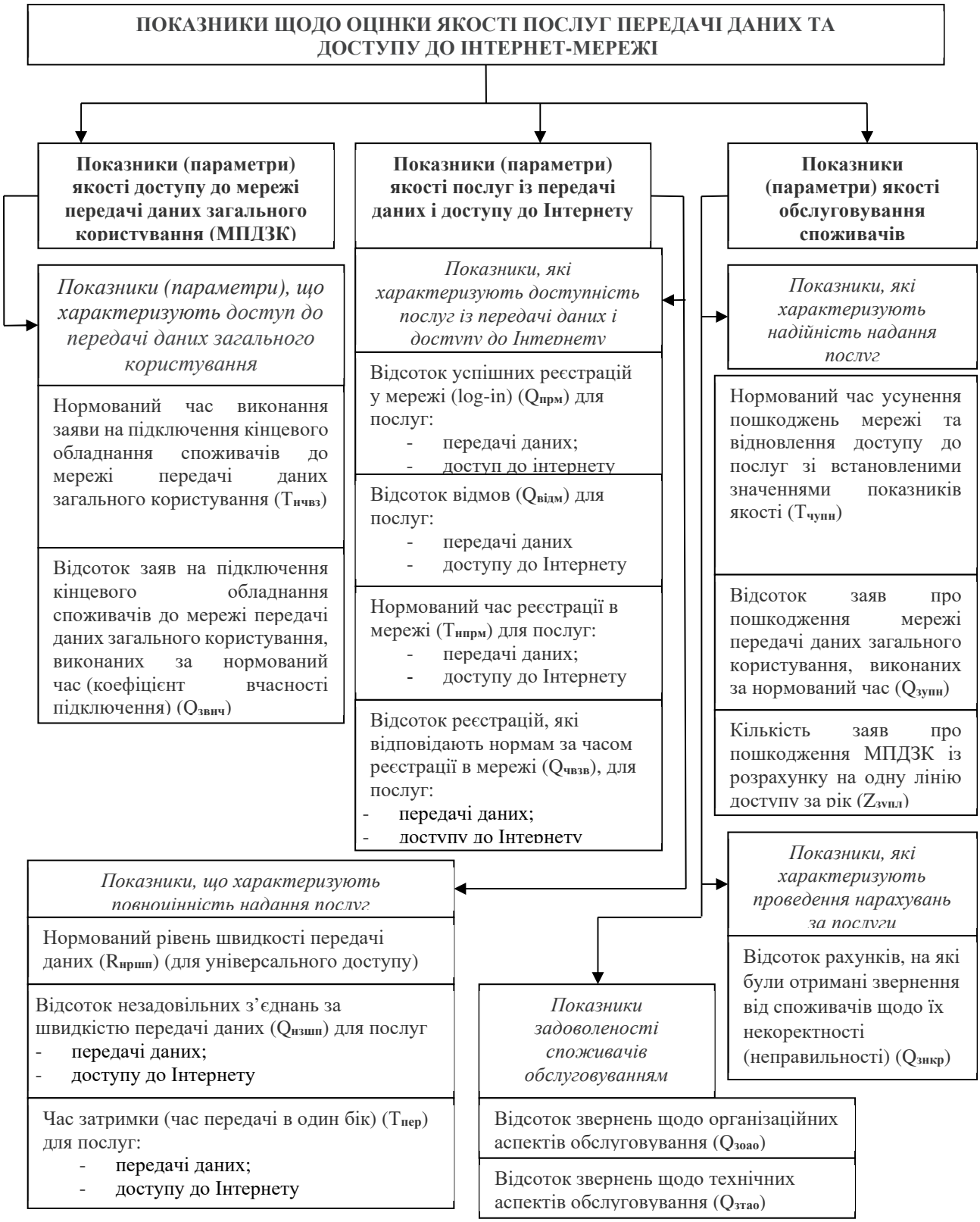


Рис. А. Схематичне представлення показників оцінки якості послуг передачі даних та доступу до глобальної мережі
(9складено автором [398;399; 400])

ДОДАТОК Б

Таблиця Б.1

Динаміка індикаторів ринкової складової безпеки ПрАТ “Київстар” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	K_R витрат на маркетинг ROMI, %	0,17	0,21	0,15	0,12	0,09	0,05-0,09; 0,1-0,25; 0,26-0,37; 0,38-0,45
2	K_{NPS} задов над. посл	0,24	0,27	0,55	0,61	0,63	0,3-0,49; 0,5-0,74; 0,75 – 0,84; 0,85 – 0,93.
3	К проник	0,51	0,74	0,86	0,89	0,9	0,55-0,65 0,66-0,75 0,76-0,86 0,87-0,94
4	К присут по віднош до найб конк (рин част)	1	1	1	1	1	1
5	К затр пер дан *серед 8 ms фактично - 0,98, встанов постач*	0,015	0,014	0,013	0,012	0,017	0,021-0,017 0,015-0,016 0,015-0,013 0,012-0,01
6	$K_{нр}$ (отримн зверен по неправ рахункам) *Не > 1% Встан 0,5 Отримано 0,01*	0,02	0,02	0,01	0,01	0,01	0,05-0,045 0,044-0,031 0,03-0,0221 0,02-0,01
7	$K_{як посл}$ (відповідності нормам за як передачі інфор)	1	1	1	1	1	0,81-0,82 0,83-0,85 0,86-0,87 0,88-0,90
8	$K_{н викл}$ (неуспіш. викликів)	0,024	0,022	0,02	0,019	0,036	0,05-0,04 0,03-0,025 0,024-0,2 0,019-0,01

Таблиця Б.2

Динаміка індикаторів: виробничої, інноваційно-інвестиційної, техніко-технологічної, енергетичної складових безпеки ПрАТ “Київстар” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	$K_{фв}$ ОЗ (фондовіддачі)	2,35	1,84	1,71	1,75	1,6	0,1-0,35 0,36-0,65 0,66-0,88 0,89-0,99
2	$K_{зн}$ (зносу)	0,62	0,56	0,55	0,53	0,5	0,88-0,74 0,73-0,67 0,66-0,50 0,49-0,35
3	$K_{прид}$ (придатності)	0,38	0,44	0,45	0,47	0,5	0,35-0,49 0,50-0,66 0,67-0,73 0,74-0,88
4	$K_{онов}$ (оновлення)	0,115	0,155	0,151	0,162	0,203	0,05-0,09 0,1-0,14 0,15-0,19 0,2-0,22
5	$K_{іннов}$ (інноваційності) лок. рег, маг мереж, комут, радіоустат., моб.мережі.	0,110	0,110	0,108	0, 089	0,203	0,02-0,04 0,05-0,08 0,09-0,1 0,11-0,12
6	$K_{R\ кап\ вклад}$ (рент кап вклад)	0,13	0,05	0,07	0,21	0,17	0,12-0,15 0,16-0,19 0,2-0,25 0,26-0,3 збільшення
7	$K_{R\ іннов\ витр}$ (іннов витр)	0,11	0,03	0,04	0,19	0,17	0,06-0,075 0,076-0,089 0,09-0,12 0,13-0,15
8	$K_{ефект\ оброб\ дан}$ (ен/еф-ті оброб даних)	0,56	0,61	0,625	0,64	0,65	0,35-0,46 0,47-0,57 0,58-0,69 0,7-0,8
9	$K_{енергозб}$ (енергозбереж)	0,26	0,27	0,31	0,315	0,34	0,25-0,3 0,31-0,33 0,34-0,38 0,39-0,43
10	$K_{прогрес\ технол}$ (прогресив технолог)	0,6	0,63	0,7	0,81	0,85	0,5-0,55 0,56-0,6 0,6-0,65 0,66-0,7

Таблиця Б.3

Динаміка індикатора фінансової складової безпеки ПрАТ “Київстар” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	$К_{авт}$	0,67	0,56	0,42	0,42	0,54	0,1-0,2 0,3-0,4 0,41-0,49 0,5-0,6 0,4 - 0,6, більше не використ пт, нижче - банкр
2	$К_{вк/зал\ кап}$	2,05	1,27	0,73	0,72	1,2	0,65-0,77 0,78-0,84 0,85-0,9 0,91-0,99
3	$К_{фін\ стійк}$	0,68	0,66	0,68	0,79	0,74	0,5-0,55 0,56-0,59 0,6-0,66 0,67-0,71 *0,7-0,9., нижче недост фін стій*
4	$К_{ман\ ВК}$	-0,08	-0,46	-0,56	-0,27	-0,43	0,03-0,04 0,05-0,06 0,07-0,089 *0,09-0,099* *0,1 і вище, позит - достатн ВК*
5	$К_{заб\ ВОК}$	-0,21	-3,3	-2,86	-1,09	-1,2	0,049-0,058 0,059-0,078 0,079-0,088 0,089-0,099 *0,1 і вище.*
6	$К_{чист\ заборг}$ (важіль)	0,28	0,67	0,85	0,48	0,75	0,2-0,3 0,31-0,38 0,39-0,42 0,43-0,49 норм за ранг риз. , більше 0,5
7	$К_{покрит}$	0,82	0,23	0,26	0,48	0,83	0,72-0,8 0,81-0,83 0,84-0,94 0,95-1
8	$К_{шв\ ліквід}$	0,82	0,22	0,25	0,47	0,82	0,2-0,29 0,3-0,39 0,4-0,44 0,45-0,5 *0,5-1 і вище*
9	$К_{абсол\ лікв}$	0,67	0,11	0,14	0,27	0,45	0,05-0,1 0,11-0,14 0,15-0,2 *від 0,1 до 0,2.*
10	$К\ R_{кап}$	0,28	0,09	0,1	0,32	0,27	Більше 0,1
11	$К\ R_{вк}$	0,45	0,15	0,21	0,65	0,55	0,27-0,34 0,35-0,4 0,41-0,45 0,46-0,5 *зростання коеф означає підвищення здатності комп генерувати приб власникам.*

продовження таблиці Б.3

12	K R прод, роб, посл	1,48	1,88	1,95	1,91	1,36	0,27-0,34 0,35-0,4 0,41-0,45 0,46-0,5 *порівн із конкур*
13	K R продажів	0,36	0,4	0,41	0,39	0,31	порівн із конкур
14	K R госп дія-ті	0,52	0,65	0,74	0,63	0,48	порівн із конкур

Таблиця Б.4.

Динаміка індикатора електронно-комунікаційної складової безпеки ПрАТ “Київстар” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	K від станд МСЕ (відпов станд)	0,83	0,96	0,97	0,98	0,98	
2	K конверг ІКМ(об’єдн мереж ауд тел комп)	0,51	0,52	0,55	0,59	0,69	0,5-0,65 0,76-0,86 0,85-0,89 0,09-0,95
3	K заб xPON						0,7
4	K MAU	0,07	0,10	0,13	0,14	0,16	0,11-0,26 0,27-0,31 0,32-0,36 0,37-0,42
5	K кіберсвід культ (кіберсвідчення культури)	0,56	0,58	0,63	0,69	0,78	0,65-0,79 0,8-0,84 0,85-0,9 0,91-0,99
6	K сис-ми зах інф та кіберб	0,59	0,61	0,69	0,71	0,71	0-0,24 0,25-0,49 0,5-0,74 0,75-,09

Таблиця Б.5

Динаміка індикатора екологічної складової безпеки ПрАТ “Київстар” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	K R стал розв (стал розвитку)	0,25	0,28	0,32	0,32	0,32	0,15-0,19 0,2-0,26 0,27-0,34 0,35-0,45

продовження таблиці Б.5

2	$K_{впров\ еко\text{-}техн}$ (впровадження екотехнологій)	0,02	0,02	0,12	0,13	0,15	0,09-0,11 0,12-0,14 0,15-0,17 0,18-0,19
3	$K_{екол\ вплив}$ (еколог впливу на навк середовище)	0,56	0,58	0,67	0,67	0,68	0,23-0,21 0,20-0,18 0,17-0,15 0,14-0,12
4	$K_{екол\ серт}$ (екол сертифікації послуг)	0,33	0,36	0,39	0,45	0,51	0,5-0,62 0,63-0,7 0,71-0,94 0,95-0,99
5	$K_{поруш\ нор\ екол}$ (порушення норм екол зак-ва)	0,05	0,05	0,05	0,04	0,03	0,19-0,17 0,16-0,13 0,12-0,06 0,05-0

Таблиця Б.6

Динаміка індикатора фізичної складової безпеки ПрАТ “Київстар” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа (біфуркація)
1	$K_{відв\ прон}$ (відвернутих проникнень)	1	1	1	1	1	1
2	$K_{відверн\ комп\ крадіж}$ (спроб комп крадіжок)	1	1	1	1	1	1
3	$K_{відв\ нанес\ шкоди\ персон}$ (відвер спроб фіз шкоди)	1	1	1	1	1	1
4	$K_{над\ персон}$ (надійності персоналу)	0,95	0,97	0,97	0,98	0,98	1

Таблиця Б.7

Динаміка індикаторів інтелектуального потенціалу (персонал-інтелектуальної) безпеки ПрАТ “Київстар” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	$K_{задов\ ум\ праці}$ (задоволеності умовами праці)	0,71	0,72	0,75	0,79	0,8	0,45-0,65 0,66-0,74 0,75-0,87 0,88-0,95

продовження таблиці Б.7

2	$К_{дотрим норм-умов}$ (дотримання норм праці (випром))	0,85	0,87	0,89	0,89	0,9	0,75-0,84 0,85-0,89 0,9-0,97 0,96-0,99
3	$К_{плин персон вис кв}$ (плин персон високої кваліфік)	0,075	0,065	0,083	0,077	0,085	0,096-0,091 0,09-0,085 0,084-0,082 0,081-0,079
5	$К_{винах акт}$ (винахідницької (раціоналізаторської) активності)	0,34	0,45	0,55	0,63	0,71	0,69-0,76 0,77-0,82 0,83-0,88 0,89-0,93
6	$К_{заб осв перс}$ (забезп освітченим персоналом)	0,45	0,51	0,49	0,51	0,55	0,52-0,58 0,59-0,64 0,65-0,7 0,71-0,75
7	$К_{плин персон}$ (плинності)	0,22	0,25	0,27	0,21	0,35	0,25-0,16 0,15-0,11 0,12-0,1 0,09-0,03
8	$К_{R ор}$ еф пер (рентаб організ ефект-ті персоналу)	0,76	0,65	0,69	0,68	0,7	0,79-0,81 0,82-0,88 0,89-0,93 0,94-0,97
9	$К_{Фехнера}$ (відповід цілей персон цілям підпр)	0,35	0,34	0,37	0,44	0,61	-1; 0; 1

Таблиця Б.8

Динаміка індикаторів інформаційної, інтерфейсної, політико-правової безпеки ПрАТ “Київстар” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа **= біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	$К_{повн інф}$	0,88	0,89	0,81	0,85	0,79	Більше 0,91
2	$К_{точ інф}$ (точності інформації)	0,84	0,84	0,71	0,74	0,69	Більше 0,82
4	$К_{рівн гот до кіберінц}$	0,76	0,78	0,83	0,88	0,74	Більше 0,8
5	$К_{вияв втор}$ (вияв вторгнень)	0,77	0,86	0,89	0,89	0,79	Більше 0,85
7	$К_{поруш догов}$	0,13	0,12	0,11	0,06	0,05	Менше 0,05
8	$К_{судов справ за дог}$ (порушення конт договорів)	0,11	0,1	0,09	0,05	0,03	Менше 0,1
11	$К_{репут}$ (репутації)	0,91	0,93	0,94	0,95	0,79	Більше 0,9
12	К достр прип дог (дострокового припинення договорі)	0,05	0,04	0,04	0,03	0,12	Менше 0,05
13	$К_{компл}$ (комплаєнс-дисципліни)	0,93	0,95	0,95	0,96	0,95	Більше 0,91

Рівень інформаційної безпеки може бути визначений на основі добутку трьох згаданих коефіцієнтів:
Кі = Кпі*Кті*Ксі. *При цьому, якщо:*
Кі ≥ *0,7 – рівень безпеки високий;*
0,3 ≤ Кі <*0,7 – рівень безпеки середній;*
Кі<*0,3 – рівень безпеки низький.*

Таблиця Б.9.

Динаміка індикаторів ринкової складової безпеки ПрАТ “ВФ Україна” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа **= біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	K_R продажів	0,37	0,37	0,37	0,38	0,32	
2	K_R витрат на маркетинг ROMI, %	0,21	0,19	0,18	0,11	0,07	0,05-0,09; 0,1-0,25; 0,26-0,37; 0,38-0,45
4	K_{NPS} задов над. посл	0,27	0,32	0,78	0,67	0,71	Сер - 35 Медіан - 40 Верх квар – більше 64 Нижн кварт - менше 11 0, 11-0,49; 0,5-0,74; 0,75 – 0,84; 0,85 – 0,93.
5	К проник	0,43	0,73	0,86	0,86	0,86	0,55-0,65 0,66-0,75 0,76-0,86 0,87-0,94
6	К присут по віднош до найб конк (рин част)	0,54	0,55	0,58	0,64	0,59	1
7	К затр пер дан *серед 8 ms фактично - 0,98, встанов постач*	0,017	0,015	0,014	0,012	0,019	0,021-0,017 0,015-0,016 0,015-0,013 0,012-0,01
8	$K_{нр}$ (отримн зверен по неправ рахункам) *Не > 1%* *Встан 0,5* *Отримано 0,01*	0,02	0,03	0,02	0,02	0,01	0,05-0,045 0,044-0,031 0,03-0,0221 0,02-0,01
9	$K_{як\ посл}$ (відповідності нормам за як передачі інфор)	1	1	1	1	1	0,81-0,82 0,83-0,85 0,86-0,87 0,88-0,90
10	$K_{н\ викл}$ (неуспіш. викликів)	0,025	0,021	0,013	0,014	0,029	0,05-0,04 0,03-0,025 0,024-0,2 0,019-0,01

Таблиця Б.10

Динаміка індикаторів: виробничої, інноваційно-інвестиційної, техніко-технологічної, енергетичної складових безпеки ПрАТ “ВФ Україна” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$K_{фв}$ ОЗ (фондовіддачі)	1,1	1,3	1,46	1,62	1,61	0,1-0,35 0,36-0,65 0,66-0,88 0,89-0,99
2	$K_{зн}$ (зносу)	0,56	0,5	0,52	0,56	0,594	0,88-0,74 0,73-0,67 0,66-0,50 0,49-0,35
3	$K_{прид}$ (придатності)	0,44	0,5	0,48	0,44	0,406	0,35-0,49 0,50-0,66 0,67-0,73 0,74-0,88
4	$K_{онов}$ (оновлення)	0,12	0,21	0,2	0,19	0,19	0,05-0,09 0,1-0,14 0,15-0,19 0,2-0,22
5	$K_{іннов}$ (інноваційності) лок. рег, маг мереж, комут, радіоустат., моб.мережі.	0,13	0,19	0,21	0,23	0,23	0,02-0,04 0,05-0,08 0,09-0,1 0,11-0,12
6	$K_{R\ кап\ вклад}$ (рент кап вклад)	0,15	0,17	0,22	0,19	0,15	0,12-0,15 0,16-0,19 0,2-0,25 0,26-0,3 збільшення
7	$K_{R\ іннов\ витр}$ (іннов витр)	0,09	0,09	0,08	0,21	0,15	0,06-0,075 0,076-0,089 0,09-0,12 0,13-0,15
8	$K_{ефект\ оброб\ дан}$ (ен/еф-ті оброб даних)	0,59	0,6	0,67	0,68	0,61	0,35-0,46 0,47-0,57 0,58-0,69 0,7-0,8
9	$K_{енергозб}$ (енергозбереж)	0,19	0,28	0,35	0,36	0,36	0,25-0,3 0,31-0,33 0,34-0,38 0,39-0,43
10	$K_{прогрес\ технол}$ (прогресив технолог)	0,65	0,69	0,71	0,83	0,85	0,5-0,55 0,56-0,6 0,6-0,65 0,66-0,7

Таблиця Б.11

Динаміка індикатора фінансової складової безпеки ПрАТ “ВФ Україна” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$К_{авт}$	0,47	0,57	0,412	0,436	0,418	0,1-0,2 0,3-0,4 0,41-0,49 0,5-0,6 0,4 - 0,6, більше не використ пт, нижче - банкр
2	$К_{вк/зал\ кап}$	0,899	1,36	0,702	0,773	0,718	0,65-0,77 0,78-0,84 0,85-0,9 0,91-0,99
3	$К_{фін\ стійк}$	0,71	0,73	0,862	0,862	0,857	0,5-0,55 0,56-0,59 0,6-0,66 0,67-0,71 *0,7-0,9., нижче недост фін стій*
4	$К_{ман\ ВК}$	-0,27	-0,25	0,706	0,685	0,902	0,03-0,04 0,05-0,06 0,07-0,089 *0,09-0,099* *0,1 і вище, позит - достатн ВК*
5	$К_{заб\ ВОК}$	-0,8	-1,16	0,678	0,683	0,726	0,049-0,058 0,059-0,078 0,079-0,088 0,089-0,099 *0,1 і вище.*
6	$К_{чист\ заборг}$ (важіль)	1,49	1,068	2,457	1,558	2,616	0,2-0,3 0,31-0,38 0,39-0,42 0,43-0,49 норм за ранг риз. , більше 0,5
7	$К_{покрит}$	0,55	0,46	3,109	3,152	3,644	0,72-0,8 0,81-0,83 0,84-0,94 0,95-1 *норм 1-3, оптимальним є значення 2-3. Показник нижче нормативного свідчить про проблемний стан платоспроможності*
8	$К_{шв\ ліквід}$	0,53	0,42	3,078	3,12	3,618	0,2-0,29 0,3-0,39 0,4-0,44 0,45-0,5 *0,5-1 і вище*
9	$К_{абсол\ лікв}$	0,4	0,28	2,872	2,879	3,1202	0,05-0,1 0,11-0,14 0,15-0,2 *від 0,1 до 0,2.*
10	$К_{R\ кап}$	0,07	0,1	0,03	0,103	0,014	

продовження таблиці Б.11

11	K $_{Rвк}$	0,13	0,19	0,076	0,24	0,067	0,27-0,34 0,35-0,4 0,41-0,45 0,46-0,5 *зростання коеф означає підвищення здатності комп генерувати приб власникам.*
12	K $_{R\ прод,\ роб,\ посл}$	0,81	0,92	0,989	1,19	1,371	0,27-0,34 0,35-0,4 0,41-0,45 0,46-0,5 *порівн із конкур*
13	K $_{R\ продажів}$	0,16	0,14	0,066	0,190	0,056	порівн із конкур
14	K $_{R\ госп\ дія-ті}$	0,16	0,184	0,069	0,24	0,052	порівн із конкур

Таблиця Б.12.

Динаміка індикатора електронно-комунікаційної складової безпеки ПрАТ “ВФ Україна” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	K$_{від\ станд\ МСЕ}$ (відпов станд)	0,81	0,95	0,97	0,98	0,98	
2	K $_{конверг\ ІКМ}$(об’єдн мереж ауд тел комп)	0,49	0,51	0,53	0,55	0,57	0,5-0,65 0,76-0,86 0,85-0,89 0,09-0,95
3	K$_{заб\ xPON}$						0,7
4	K $_{MAU}$	0,06	0,8	0,11	0,12	0,14	0,11-0,26 0,27-0,31 0,32-0,36 0,37-0,42
5	K $_{кіберсвід\ культ}$ (кіберсвідчення культури)	0,54	0,55	0,61	0,65	0,74	0,65-0,79 0,8-0,84 0,85-0,9 0,91-0,99
6	K $_{сис-ми\ зах\ інф\ та\ кіберб}$	0,55	0,59	0,6	0,63	0,63	0-0,24 0,25-0,49 0,5-0,74 0,75-,09

Таблиця Б.13

Динаміка індикатора екологічної складової безпеки ПрАТ “ВФ Україна” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$K_{R\ стал\ розв}$ (стал розвитку)	0,2	0,23	0,27	0,29	0,3	0,15-0,19 0,2-0,26 0,27-0,34 0,35-0,45
2	$K_{впров\ еко\text{-}техн}$ (впровадження екотехнологій)	0,025	0,03	0,12	0,14	0,17	0,09-0,11 0,12-0,14 0,15-0,17 0,18-0,19
3	$K_{екол\ вплив}$ (еколог впливу на навк середовище)	0,56	0,58	0,67	0,67	0,68	0,23-0,21 0,20-0,18 0,17-0,15 0,14-0,12
4	$K_{екол\ серт}$ (екол сертифікації послуг)	0,3	0,3	0,32	0,35	0,4	0,5-0,62 0,63-0,7 0,71-0,94 0,95-0,99
5	$K_{поруш\ нор\ екол}$ (порушення норм екол зак-ва)	0,04	0,03	0,03	0,04	0,02	0,19-0,17 0,16-0,13 0,12-0,06 0,05-0

Таблиця Б.14

Динаміка індикатора фізичної (силової) складової безпеки ПрАТ “ВФ Україна” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа (біфуркація)
1	$K_{відв\ прон}$ (відвернутих проникнень)	1	1	1	1	1	1
2	$K_{відверн\ комп\ крадіж}$ (спроб комп крадіжок)	1	1	1	1	1	1
3	$K_{відв\ нанес\ шкоди\ персон}$ (відвер спроб фіз шкоди)	1	1	1	1	1	1
4	$K_{над\ персон}$ (надійності персоналу)	0,91	0,93	0,95	0,93	0,95	1

Таблиця Б.15

Динаміка індикаторів інтелектуального потенціалу (персонал-інтелектуальної) безпеки ПрАТ “ВФ Україна” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$K_{\text{задов ум праці}}$ (задоволеності умовами праці)	0,74	0,74	0,76	0,8	0,83	0,45-0,65 0,66-0,74 0,75-0,87 0,88-0,95
2	$K_{\text{дотрим норм-умов}}$ (дотримання норм праці (випром))	0,87	0,89	0,89	0,9	0,92	0,75-0,84 0,85-0,89 0,9-0,97 0,96-0,99
3	$K_{\text{плин персон вис кв}}$ (плин персон високої кваліфік)	0,081	0,077	0,088	0,072	0,08	0,096-0,091 0,09-0,085 0,084-0,082 0,081-0,079
5	$K_{\text{винах акт}}$ (винахідницької (раціоналізаторської) активності)	0,29	0,39	0,51	0,61	0,63	0,69-0,76 0,77-0,82 0,83-0,88 0,89-0,93
6	$K_{\text{заб осв перс}}$ (забезп освітченим персоналом)	0,43	0,49	0,49	0,5	0,51	0,52-0,58 0,59-0,64 0,65-0,7 0,71-0,75
7	$K_{\text{плин персон}}$ (плинності)	0,2	0,2	0,25	0,19	0,31	0,25-0,16 0,15-0,11 0,12-0,1 0,09-0,03
9	$K_{R\ op}$ еф пер (рентаб організ ефект-ті персоналу)	0,69	0,65	0,67	0,65	0,67	0,79-0,81 0,82-0,88 0,89-0,93 0,94-0,97
	$K_{\text{Фехнера}}$ (відповід цілей персон цілям підпр)	0,37	0,41	0,42	0,42	0,65	-1; 0; 1

Таблиця Б.16

Динаміка індикаторів інформаційної, інтерфейсної, політико-правової безпеки ПрАТ “ВФ Україна” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$K_{\text{повн інф}}$	0,89	0,87	0,83	0,81	0,77	Більше 0,91
2	$K_{\text{точ інф}}$ (точності інформації)	0,85	0,83	0,69	0,71	0,73	Більше 0,82
4	$K_{\text{рівн гот до кіберінц}}$	0,74	0,75	0,81	0,85	0,71	Більше 0,8
5	$K_{\text{вияв втор}}$ (вияв вторгнень)	0,79	0,87	0,89	0,89	0,81	Більше 0,85
7	$K_{\text{поруш догов}}$	0,11	0,11	0,09	0,07	0,05	Менше 0,05

продовження таблиці Б.16

8	К судов справ за дог (порушення конт договорів)	0,09	0,08	0,07	0,02	0,02	Менше 0,1
11	К репут (репутації)	0,92	0,94	0,94	0,95	0,91	Більше 0,9
12	К достр прип дог (дострокового припинення договорі)	0,04	0,03	0,04	0,02	0,12	Менше 0,05
13	К компл (комплаєнс-дисципліни)	0,91	0,92	0,94	0,94	0,93	Більше 0,91

Рівень інформаційної безпеки може бути визначений на основі добутку трьох згаданих коефіцієнтів: *Ki = Kni*Kmi*Kci.* При цьому, якщо:

Ki ≥ 0,7 – рівень безпеки високий;

0,3 ≤ *Ki*<0,7 – рівень безпеки середній;

Ki<0,3 – рівень безпеки низький.

Таблиця Б.17.

Динаміка індикаторів ринкової складової безпеки ТОВ “Лайфселл” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
2	K_R витрат на маркетинг ROMI, %	0,17	0,21	0,15	0,12	0,09	0,05-0,09; 0,1-0,25; 0,26-0,37; 0,38-0,45
3	K_{NPS} задов над. посл	0,41	0,46	0,56	0,55	0,63	0, 01-0,49; 0,5-0,74; 0,75 – 0,84; 0,85 – 0,93.
4	К проник	0,77	0,81	0,83	0,84	0,94	0,55-0,65 0,66-0,75 0,76-0,86 0,87-0,94
5	К присут по віднош до найб конк (рин част)	0,27	0,29	0,3	0,31	0,35	1
6	К затр пер дан серед 8 ms фактично - 0,98, встанов постач	0,016	0,015	0,014	0,013	0,014	0,021-0,017 0,015-0,016 0,015-0,013 0,012-0,01
7	К нр (отримн зверен по неправ рахункам) Не > 1% Встан 0,5 Отримано 0,01	0,04	0,05	0,04	0,03	0,02	0,05-0,045 0,044-0,031 0,03-0,0221 0,02-0,01
8	К як посл (відповідності нормам за як передачі інфор)	1	1	1	1	1	0,81-0,82 0,83-0,85 0,86-0,87 0,88-0,90
9	К н викл (неуспіш. викликів)	0,023	0,023	0,02	0,018	0,034	0,05-0,04 0,03-0,025 0,024-0,2 0,019-0,01

Таблиця Б.18

Динаміка індикаторів: виробничої, інноваційно-інвестиційної, техніко-технологічної, енергетичної складових безпеки ТОВ “Лайфселл” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$К_{фв}$ ОЗ (фондовіддачі)	0,993	1,175	1,343	1,312	1,477	0,1-0,35 0,36-0,65 0,66-0,88 0,89-0,99
2	$К_{зн}$ (зносу)	0,6	0,636	0,647	0,617	0,651	0,88-0,74 0,73-0,67 0,66-0,50 0,49-0,35
3	$К_{прид}$ (придатності)	0,4	0,364	0,353	0,383	0,349	0,35-0,49 0,50-0,66 0,67-0,73 0,74-0,88
4	$К_{онов}$ (оновлення)	0,14	0,16	0,173	0,2	0,19	0,05-0,09 0,1-0,14 0,15-0,19 0,2-0,22
5	$К_{іннов}$ (інноваційності) лок. рег, маг мереж, комут, радіоустат., моб.мережі.	0,09	0,11	0,14	0, 16	0,18	0,02-0,04 0,05-0,08 0,09-0,1 0,11-0,12
6	$К_{R\ кап\ вклад}$ (рент кап вклад)	0,09	0,06	0,07	0,15	0,14	0,12-0,15 0,16-0,19 0,2-0,25 0,26-0,3 збільшення
7	$К_{R\ іннов\ витр}$ (іннов витр)	0,11	0,03	0,04	0,19	0,17	0,06-0,075 0,076-0,089 0,09-0,12 0,13-0,15
8	$К_{ефект\ оброб\ дан}$ (ен/еф-ті оброб даних)	0,43	0,51	0,58	0,58	0,54	0,35-0,46 0,47-0,57 0,58-0,69 0,7-0,8
9	$К_{енергозб}$ (енергозбереж)	0,21	0,23	0,25	0,27	0,29	0,25-0,3 0,31-0,33 0,34-0,38 0,39-0,43
10	$К_{прогрес\ технол}$ (прогресив технолог)	0,52	0,57	0,63	0,79	0,78	0,5-0,55 0,56-0,6 0,6-0,65 0,66-0,7

Таблиця Б.19

Динаміка індикатора фінансової складової безпеки ТОВ “Лайфселл” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$К_{авт}$	0,323	0,327	0,46	0,474	0,489	0,1-0,2 0,3-0,4 0,41-0,49 0,5-0,6 0,4 - 0,6, більше не використ пт, нижче - банкр
2	$К_{вк/зал\ кап}$	0,478	0,318	0,853	0,9	0,957	0,65-0,77 0,78-0,84 0,85-0,9 0,91-0,99
3	$К_{фін\ стійк}$	0,489	0,487	0,671	0,721	0,649	0,5-0,55 0,56-0,59 0,6-0,66 0,67-0,71 *0,7-0,9., нижче недост фін стій*
4	$К_{ман\ ВК}$	-1,421	-1,389	-0,573	-0,38	-0,29	0,03-0,04 0,05-0,06 0,07-0,089 *0,09-0,099* *0,1 і вище, позит - достатн ВК*
5	$К_{заб\ ВОК}$	-9,01	-7,67	-4,052	-1,867	-0,678	0,049-0,058 0,059-0,078 0,079-0,088 0,089-0,099 *0,1 і вище.*
6	$К_{чист\ заборг}$ (важіль)	2,42	1,47	2,39	1,64	1,399	0,2-0,3 0,31-0,38 0,39-0,42 0,43-0,49 норм за ранг риз. , більше 0,5
7	$К_{покрит}$	0,048	0,115	0,198	0,349	0,596	0,72-0,8 0,81-0,83 0,84-0,94 0,95-1 *норм 1-3, оптимальним є значення 2-3. Показник нижче нормативного свідчить про проблемний стан платоспроможності*
8	$К_{шв\ ліквід}$	0,097	0,113	0,195	0,344	0,585	0,2-0,29 0,3-0,39 0,4-0,44 0,45-0,5 *0,5-1 і вище*
9	$К_{абсол\ лікв}$	0,048	0,063	0,138	0,277	0,483	0,05-0,1 0,11-0,14 0,15-0,2 *від 0,1 до 0,2.*

продовження таблиці Б.19

10	K $_{R\ кап}$	-0,044	-0,082	0,152	0,036	0,053	
11	K $_{Rвк}$	-0,135	-0,251	0,162	0,038	0,111	0,27-0,34 0,35-0,4 0,41-0,45 0,46-0,5 *зростання коеф означає підвищення здатності комп генерувати приб власникам.*
12	K $_{R\ прод,\ роб,\ посл}$	0,218	0,287	0,347	0,475	0,497	0,27-0,34 0,35-0,4 0,41-0,45 0,46-0,5 *порівн із конкур*
13	K $_{R\ продажів}$	-0,115	-0,199	0,379	0,072	0,103	порівн із конкур
14	K $_{R\ госп\ дія-ті}$	-0,095	-0,158	0,271	0,077	0,111	порівн із конкур

Таблиця Б.20

Динаміка індикатора електронно-комунікаційної складової безпеки ТОВ “Лайфселл” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	K$_{від\ станд\ МСЕ}$ (відпов станд)	0,84	0,88	0,88	0,89	0,91	
2	K $_{конверг\ ІКМ}$(об’єдн мереж ауд тел комп)	0,59	0,61	0,61	0,62	0,63	0,5-0,65 0,76-0,86 0,85-0,89 0,09-0,95
3	K$_{заб\ xPON}$						
4	K $_{MAU}$	0,06	0,07	0,08	0,11	0,12	0,11-0,26 0,27-0,31 0,32-0,36 0,37-0,42
5	K $_{кіберсвід\ культ}$ (кіберсвідчення культури)	0,61	0,64	0,65	0,65	0,71	0,65-0,79 0,8-0,84 0,85-0,9 0,91-0,99
6	K $_{сис-ми\ зах\ інф\ та\ кіберб}$	0,65	0,68	0,71	0,73	0,74	0-0,24 0,25-0,49 0,5-0,74 0,75-,09

Таблиця Б.21

Динаміка індикатора екологічної складової безпеки ТОВ “Лайфселл” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$K_{R\ стал\ розв}$ (стал розвитку)	0,2	0,21	0,23	0,26	0,26	0,15-0,19 0,2-0,26 0,27-0,34 0,35-0,45
2	$K_{впров\ еко-техн}$ (впровадження екотехнологій)	0,03	0,05	0,1	0,1	0,15	0,09-0,11 0,12-0,14 0,15-0,17 0,18-0,19
3	$K_{екол\ вплив}$ (еколог впливу на навк середовище)	0,61	0,62	0,61	0,62	0,61	0,23-0,21 0,20-0,18 0,17-0,15 0,14-0,12
4	$K_{екол\ серт\ (екол\ сертифікації\ послуг)}$	0,33	0,36	0,39	0,45	0,51	0,5-0,62 0,63-0,7 0,71-0,94 0,95-0,99
5	$K_{поруш\ нор\ екол}$ (порушення норм екол зак-ва)	-	-	-	-	-	0,19-0,17 0,16-0,13 0,12-0,06 0,05-0

Таблиця Б.22

Динаміка індикатора фізичної (силової) складової безпеки ТОВ “Лайфселл” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа (біфуркація)
1	$K_{відв\ прон}$ (відвернутих проникнень)	1	1	1	1	1	1
2	$K_{відверн\ комп\ крадіж}$ (спроб комп крадіжок)	1	1	1	1	1	1
3	$K_{відв\ нанес\ шкоди\ персон}$ (відвер спроб фіз шкоди)	1	1	1	1	1	1
4	$K_{над\ персон}$ (надійності персоналу)	0,95	0,97	0,97	0,98	0,98	1

Таблиця Б.23

Динаміка індикаторів інтелектуально-кадрової (персонал-інтелектуальної) безпеки ТОВ “Лайфселл” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$K_{\text{задов ум праці}}$ (задоволеності умовами праці)	0,74	0,76	0,78	0,78	0,82	0,45-0,65 0,66-0,74 0,75-0,87 0,88-0,95
2	$K_{\text{дотрим норм-умов}}$ (дотримання норм праці (випром))	0,86	0,86	0,87	0,86	0,86	0,75-0,84 0,85-0,89 0,9-0,97 0,96-0,99
3	$K_{\text{плин персон вис кв}}$ (плин персон високої кваліфік)	0,065	0,061	0,063	0,071	0,13	0,096-0,091 0,09-0,085 0,084-0,082 0,081-0,079
5	$K_{\text{винах акт}}$ (винахідницької (раціоналізаторської) активності)	0,43	0,43	0,46	0,45	0,49	0,69-0,76 0,77-0,82 0,83-0,88 0,89-0,93
6	$K_{\text{заб осв перс}}$ (забезп освітченим персоналом)	0,55	0,54	0,49	0,53	0,51	0,52-0,58 0,59-0,64 0,65-0,7 0,71-0,75
7	$K_{\text{плин персон}}$ (плинності)	0,23	0,26	0,28	0,21	0,38	0,25-0,16 0,15-0,11 0,12-0,1 0,09-0,03
8	$K_{R\ \text{ор}}$ еф пер (рентаб організ ефект-ті персоналу)	0,74	0,76	0,78	0,81	0,8	0,79-0,81 0,82-0,88 0,89-0,93 0,94-0,97
	$K_{\text{Фехнера}}$ (відповід цілей персон цілям підпр)	0,41	0,56	0,45	0,43	0,5	-1; 0; 1

Таблиця Б.24

Динаміка індикаторів інформаційної, інтерфейсної, політико-правової безпеки ТОВ “Лайфселл” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$K_{\text{повн інф}}$	0,88	0,89	0,81	0,85	0,79	Більше 0,91
2	$K_{\text{точ інф}}$ (точності інформації)	0,84	0,84	0,71	0,74	0,69	Більше 0,82
4	$K_{\text{рівн гот до кіберінц}}$	0,76	0,78	0,83	0,88	0,74	Більше 0,8
5	$K_{\text{вияв втор}}$ (вияв вторгнень)	0,77	0,86	0,89	0,89	0,79	Більше 0,85
7	$K_{\text{поруш догов}}$	0,13	0,12	0,11	0,06	0,05	Менше 0,05

продовження таблиці Б.24

8	К судов справ за дог (порушення конт договорів)	0,11	0,1	0,09	0,05	0,03	Менше 0,1
11	К репут (репутації)	0,91	0,93	0,94	0,95	0,79	Більше 0,9
12	К достр прип дог (дострокового припинення договорі)	0,05	0,04	0,04	0,03	0,12	Менше 0,05
13	К компл (комплаєнс-дисципліни)	0,95	0,95	0,95	0,95	0,95	Більше 0,91

Рівень інформаційної безпеки може бути визначений на основі добутку трьох згаданих коефіцієнтів: *Кі = Кпі*Кті*Ксі.* При цьому, якщо: *Кі* ≥ 0,7 – рівень безпеки високий; 0,3 ≤ *Кі*<0,7 – рівень безпеки середній; *Кі*<0,3 – рівень безпеки низький.

Таблиця Б. 25

Динаміка індикаторів ринкової складової безпеки ТОВ “Укртелеком” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	K_R продажів	0, 02	-0,14	0,37	0,1	-0,45	
2	K_R витрат на маркетинг ROMI, %	0,17	0,21	0,15	0,12	0,09	0,05-0,09; 0,1-0,25; 0,26-0,37; 0,38-0,45
3	CR (відтік клієнтів)	0,0069355	0,00757576	0,01145038	-0,01158301	0,05343511	0,062-0,056 0,055-0,049 0,048-0,043 0,042-0,039
4	K_{NPS} задов над. посл	0,24	0,27	0,55	0,61	0,63	0, 01-0,49; 0,5-0,74; 0,75 – 0,84; 0,85 – 0,93.
5	К проник	0,51	0,74	0,86	0,89	0,9	0,55-0,65 0,66-0,75 0,76-0,86 0,87-0,94
6	К присут по віднош до найб конк (рин част)	1	1	1	1	1	1
7	К затр пер дан *серед 8 ms фактично - 0,98, встанов постач*	0,015	0,014	0,013	0,012	0,017	0,021-0,017 0,015-0,016 0,015-0,013 0,012-0,01
8	К нр (отримн зверен по неправ рахункам) *Не > 1% Встан 0,5 Отримано 0,01*	0,02	0,02	0,01	0,01	0,01	0,05-0,045 0,044-0,031 0,03-0,0221 0,02-0,01
9	К як посл (відповідності нормам за як передачі інфор)	1	1	1	1	1	0,81-0,82 0,83-0,85 0,86-0,87 0,88-0,90
10	К н викл (неуспіш. викликів)	0,024	0,022	0,02	0,019	0,036	0,05-0,04 0,03-0,025 0,024-0,2 0,019-0,01

Таблиця Б. 26

Динаміка індикаторів: виробничої, інноваційно-інвестиційної, техніко-технологічної, енергетичної складових безпеки ТОВ “Укртелеком” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$K_{фв}$ ОЗ (фондовіддачі)	2,35	1,84	1,71	1,75	1,6	0,1-0,35 0,36-0,65 0,66-0,88 0,89-0,99
2	$K_{зн}$ (зносу)	0,62	0,56	0,55	0,53	0,5	0,88-0,74 0,73-0,67 0,66-0,50 0,49-0,35
3	$K_{прид}$ (придатності)	0,38	0,44	0,45	0,47	0,5	0,35-0,49 0,50-0,66 0,67-0,73 0,74-0,88
4	$K_{онов}$ (оновлення)	0,115	0,155	0,151	0,162	0,203	0,05-0,09 0,1-0,14 0,15-0,19 0,2-0,22
5	$K_{іннов}$ (інноваційності) лок. рег, маг мереж, комут, радіоустат., моб.мережі.	0,110	0,110	0,108	0, 089	0,203	0,02-0,04 0,05-0,08 0,09-0,1 0,11-0,12
6	$K_{R\ кап\ вклад}$ (рент кап вклад)	0,13	0,05	0,07	0,21	0,17	0,12-0,15 0,16-0,19 0,2-0,25 0,26-0,3 збільшення
7	$K_{R\ іннов\ витр}$ (іннов витр)	0,11	0,03	0,04	0,19	0,17	0,06-0,075 0,076-0,089 0,09-0,12 0,13-0,15
8	$K_{ефект\ оброб\ дан}$ (ен/еф-ті оброб даних)	0,56	0,61	0,625	0,64	0,65	0,35-0,46 0,47-0,57 0,58-0,69 0,7-0,8
9	$K_{енергозб}$ (енергозбереж)	0,26	0,27	0,31	0,315	0,34	0,25-0,3 0,31-0,33 0,34-0,38 0,39-0,43
10	$K_{прогрес\ технол}$ (прогресив технолог)	0,6	0,63	0,7	0,81	0,85	0,5-0,55 0,56-0,6 0,6-0,65 0,66-0,7
11	$K_{енергоощадл}$ (енергоощадл)	0,32	0,32	0,34	0,34	0,43	

Таблиця Б.27

Динаміка індикатора фінансової складової безпеки ТОВ “Укртелеком” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	$К_{авт}$	0,24	0,21	0,22	0,23	0,45	0,1-0,2 0,3-0,4 0,41-0,49 0,5-0,6 0,4 - 0,6, більше не використ пт, нижче - банкр
2	$К_{вк/зал кап}$	0,67	-0,68	0.36	0,56	-0,98	0,65-0,77 0,78-0,84 0,85-0,9 0,91-0,99
3	$К_{фін стійк}$	0,68	0,66	0,68	0,79	0,74	0,5-0,55 0,56-0,59 0,6-0,66 0,67-0,71 *0,7-0,9., нижче недост фін стій*
4	$К_{ман ВК}$	-0,08	-0,46	-0,56	-0,27	-0,43	0,03-0,04 0,05-0,06 0,07-0,089 *0,09-0,099* *0,1 і вище, позит - достатн ВК*
5	$К_{заб ВОК}$	-0,33	-2,1	-0,9	0,25	-1,33	0,049-0,058 0,059-0,078 0,079-0,088 0,089-0,099 *0,1 і вище.*
6	$К_{чист заборг}$ (важіль)	0,28	0,67	0,85	0,48	0,75	0,2-0,3 0,31-0,38 0,39-0,42 0,43-0,49 норм за ранг риз. , більше 0,5
7	$К_{покрит}$	0,33	-0,21	0,31	0,38	-0,46	0,72-0,8 0,81-0,83 0,84-0,94 0,95-1 *норм 1-3, оптимальним є значення 2-3. Показник нижче нормативного свідчить про проблемний стан платоспроможності*

продовження таблиці Б.27

8	К шв ліквід	0,22	0,12	0,1	0,33	0,3	0,2-0,29 0,3-0,39 0,4-0,44 0,45-0,5 *0,5-1 і вище*
9	К абсол лікв	0,06	0,09	0,02	0,09	0,01	0,05-0,1 0,11-0,14 0,15-0,2 *від 0,1 до 0,2.*
10	К R кап	-0,011	-0,076	0,14	0,028	-0,19	> 0,1
11	К Rвк	0,019	-0,12	0,2	0,038	-0.27	0,27-0,34 0,35-0,4 0,41-0,45 0,46-0,5 *зростання коеф означає підвищення здатності комп генерувати приб власникам.*
12	К R прод, роб, посл	0,54	0,48	0,49	0,26	0,15	0,27-0,34 0,35-0,4 0,41-0,45 0,46-0,5 *порівн із конкур*
13	К R продажів	0, 02	-0,14	0,37	0,1	-0,45	порівн із конкур
14	К R госп дія-ті	0,42	0,48	0,52	0,51	0,41	порівн із конкур

Таблиця Б.28

Динаміка індикатора електронно-комунікаційної складової безпеки ТОВ “Укртелеком” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	Квід станд МСЕ (відпов станд)	0,5	0,56	0,46	0,43	0,46	
2	К конверг ІКМ(об’єдн мереж ауд тел комп)	0,3	0,31	0,29	0,29	0,28	0,5-0,65 0,76-0,86 0,85-0,89 0,09-0,95
4	К MAU	-	-	-	-	-	0,11-0,26 0,27-0,31 0,32-0,36 0,37-0,42
5	К кіберсвід культ (кіберсвідчення культури)	0,32	0,29	0,31	0,29	0,27	0,65-0,79 0,8-0,84 0,85-0,9 0,91-0,99
6	К сис-ми зах інф та кіберб	0,4	0,42	0,31	0,34	0,39	0-0,24 0,25-0,49 0,5-0,74 0,75-,09

Оцінки показників ЕП(СЗІКБ) рекомендуємо застосовувати наступні критерії

Критерій	Рівень
Рівень 0 ≤ ЕП(СЗІКБ) ≤0,25	незадовільний
0,25< ЕП(СЗІКБ) ≤0,5	низький
0,5< ЕП(СЗІКБ)≤0,75	середній
0,75< ЕП(СЗІКБ) ≤0,9	високий
0,9< ЕП(СЗІКБ) ≤1	найвищий

Критерії оцінювання показників ЕП(СЗІКБ) Критерій ЕП(СЗІКБ) (НЗ) (Н) (С) високий (В) 0,9< ЕП(СЗІКБ) ≤1 найвищий (НВ) Система захисту інформації і кібербезпеки (СЗІКБ) – це складний комплекс програмних, криптографічних, організаційних та інших засобів, методів і заходів призначених для захисту інформації та кібербезпеки.

Таблиця Б.29

Динаміка індикатора екологічної складової безпеки ТОВ “Укртелеком” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	$K_{R\ стал\ розв}$ (стал розвитку)	0,12	0,13	0,14	0,13	0,17	0,15-0,19 0,2-0,26 0,27-0,34 0,35-0,45
2	$K_{впров\ еко-техн}$ (впровадження екотехнологій)	0,01	0,02	0,02	0,02	0,02	0,09-0,11 0,12-0,14 0,15-0,17 0,18-0,19
3	$K_{екол\ вплив}$ (еколог впливу на навк середовище)	0,42	0,44	0,45	0,43	0,41	0,23-0,21 0,20-0,18 0,17-0,15 0,14-0,12
5	$K_{поруш\ нор\ екол}$ (порушення норм екол зак-ва)	0,1	0,05	0,05	0,04	0,03	0,19-0,17 0,16-0,13 0,12-0,06 0,05-0

Таблиця Б.30

Динаміка індикатора фізичної (силової) складової безпеки ТОВ “Укртелеком” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа (біфуркація)
1	$K_{відв\ прон}$ (відвернутих проникнень)	1	1	1	1	1	1
2	$K_{відверн\ комп\ крадіж}$ (спроб комп крадіжок)	1	1	1	1	1	1
3	$K_{відв\ нанес\ шкоди\ персон}$ (відвер спроб фіз шкоди)	1	1	1	1	1	1
4	$K_{над\ персон}$ (надійності персоналу)	0,95	0,97	0,97	0,98	0,98	1

Таблиця Б.31

Динаміка індикаторів інтелектуально-кадрової (персонал-інтелектуальної) безпеки ТОВ “Укртелеком” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	$K_{\text{задов ум праці}}$ (задоволеності умовами праці)	0,71	0,72	0,75	0,79	0,8	0,45-0,65 0,66-0,74 0,75-0,87 0,88-0,95
2	$K_{\text{дотрим норм-умов}}$ (дотримання норм праці (випром))	0,85	0,87	0,89	0,89	0,9	0,75-0,84 0,85-0,89 0,9-0,97 0,96-0,99
3	$K_{\text{плин персон вис кв}}$ (плин персон високої кваліфік)	0,075	0,065	0,083	0,077	0,085	0,096-0,091 0,09-0,085 0,084-0,082 0,081-0,079
4	$K_{\text{заб інж-техн кад і наук}}$ забезп інж-техн персоналу і науковців						
5	$K_{\text{винах акт}}$ (винахідницької (раціоналізаторської) активності)	0,11	0,15	0,15	0,14	0,15	0,69-0,76 0,77-0,82 0,83-0,88 0,89-0,93
6	$K_{\text{заб осв перс}}$ (забезп освітченим персоналом)	0,5	0,47	0,41	0,43	0,43	0,52-0,58 0,59-0,64 0,65-0,7 0,71-0,75
7	$K_{\text{плин персон}}$ (плинності)	0,18	0,19	0,25	0,2	0,39	0,25-0,16 0,15-0,11 0,12-0,1 0,09-0,03
9	$K_{R\ \text{ор}}$ еф пер (рентаб організ ефект-ті персоналу)	0,3	0,35	0,44	0,41	0,43	0,79-0,81 0,82-0,88 0,89-0,93 0,94-0,97
	$K_{\text{Фехнера}}$ (відповід цілей персон цілям підпр)	0,3	0,3	0,3	0,3	0,32	-1; 0; 1

Таблиця Б.32

Динаміка індикаторів інформаційної, інтерфейсної, політико-правової безпеки ТОВ “Укртелеком” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	$K_{повн\ інф}$	0,88	0,89	0,81	0,85	0,79	Більше 0,91
2	$K_{точ\ інф}$ (точності інформації)	0,84	0,84	0,71	0,74	0,69	Більше 0,82
4	$K_{рівн\ гот\ до\ кіберінц}$	0,76	0,78	0,83	0,88	0,74	Більше 0,8
5	$K_{вияв\ втор}$ (вияв вторгнень)	0,77	0,86	0,89	0,89	0,79	Більше 0,85
7	$K_{поруш\ догов}$	0,13	0,12	0,11	0,06	0,05	Менше 0,05
8	$K_{судов\ справ\ за\ дог}$ (порушення конт договорів)	0,11	0,1	0,09	0,05	0,03	Менше 0,1
11	$K_{репут}$ (репутації)	0,91	0,93	0,94	0,95	0,79	Більше 0,9
12	K достр прип дог (дострокового припинення договорі)	0,05	0,04	0,04	0,03	0,12	Менше 0,05
13	$K_{компл}$ (комплаєнс-дисципліни)	0,93	0,95	0,95	0,96	0,95	Більше 0,91

Рівень інформаційної безпеки може бути визначений на основі добутку трьох згаданих коефіцієнтів:
$Ki = Kni*Kmi*Kci.$ При цьому, якщо:
$Ki \geq 0,7$ – рівень безпеки високий;
$0,3 \leq Ki < 0,7$ – рівень безпеки середній;
$Ki < 0,3$ – рівень безпеки низький.

Таблиця Б.33

Динаміка індикаторів ринкової складової безпеки ТОВ “Датагруп” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
2	K_R витрат на маркетинг ROMI, %	0,17	0,21	0,15	0,12	0,09	0,05-0,09; 0,1-0,25; 0,26-0,37; 0,38-0,45
3	K_{NPS} задов над. посл	0,41	0,46	0,56	0,55	0,63	0, 01-0,49; 0,5-0,74; 0,75 – 0,84; 0,85 – 0,93.
4	K проник	0,77	0,81	0,83	0,84	0,94	0,55-0,65 0,66-0,75 0,76-0,86 0,87-0,94

продовження таблиці Б.33

5	К присут по віднош до найб конк (рин част)	0,27	0,29	0,3	0,31	0,35	1
6	К затр пер дан серед 8 ms фактично - 0,98, встанов постач	0,016	0,015	0,014	0,013	0,014	0,021-0,017 0,015-0,016 0,015-0,013 0,012-0,01
7	$К_{нр}$ (отримн зверен по неправ рахункам) Не > 1% Встан 0,5 Отримано 0,01	0,04	0,05	0,04	0,03	0,02	0,05-0,045 0,044-0,031 0,03-0,0221 0,02-0,01
8	$К_{як\ посл}$ (відповідності нормам за як передачі інфор)	1	1	1	1	1	0,81-0,82 0,83-0,85 0,86-0,87 0,88-0,90
9	$К_{н\ викл}$ (неуспіш. викликів)	0,023	0,023	0,02	0,018	0,034	0,05-0,04 0,03-0,025 0,024-0,2 0,019-0,01

Таблиця Б.34

Динаміка індикаторів: виробничої, інноваційно-інвестиційної, техніко-технологічної, енергетичної складових безпеки ТОВ “Датагруп” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$К_{фв}$ ОЗ (фондовіддачі)	0,993	1,175	1,343	1,312	1,477	0,1-0,35 0,36-0,65 0,66-0,88 0,89-0,99
2	$К_{зн}$ (зносу)	0,6	0,636	0,647	0,617	0,651	0,88-0,74 0,73-0,67 0,66-0,50 0,49-0,35
3	$К_{прид}$ (придатності)	0,4	0,364	0,353	0,383	0,349	0,35-0,49 0,50-0,66 0,67-0,73 0,74-0,88
4	$К_{онов}$ (оновлення)	0,14	0,16	0,173	0,2	0,19	0,05-0,09 0,1-0,14 0,15-0,19 0,2-0,22
5	$К_{іннов}$ (інноваційності) лок. рег, маг мереж, комут, радіоустат., моб.мережі.	0,09	0,11	0,14	0, 16	0,18	0,02-0,04 0,05-0,08 0,09-0,1 0,11-0,12
6	$К_{R\ кап\ вклад}$ (рент кап вклад)	0,09	0,06	0,07	0,15	0,14	0,12-0,15 0,16-0,19 0,2-0,25 0,26-0,3 збільшення

продовження таблиці Б.34

7	$К_{\text{к іннов витр}}$ (іннов витр)	0,11	0,03	0,04	0,19	0,17	0,06-0,075 0,076-0,089 0,09-0,12 0,13-0,15
8	$К_{\text{ефект оброб дан}}$ (ен/еф-ті оброб даних)	0,43	0,51	0,58	0,58	0,54	0,35-0,46 0,47-0,57 0,58-0,69 0,7-0,8
9	$К_{\text{енергозб}}$ (енергозбереж)	0,21	0,23	0,25	0,27	0,29	0,25-0,3 0,31-0,33 0,34-0,38 0,39-0,43
10	$К_{\text{прогрес технол}}$ (прогресив технолог)	0,52	0,57	0,63	0,79	0,78	0,5-0,55 0,56-0,6 0,6-0,65 0,66-0,7

Таблиця Б.35

Динаміка індикатора фінансової складової безпеки ТОВ “Датагруп” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = біфуркація нижня межа; прийнятна верхня межа = репелер
1	$К_{\text{авт}}$	0,323	0,327	0,46	0,474	0,489	0,1-0,2 0,3-0,4 0,41-0,49 0,5-0,6 0,4 - 0,6, більше не використ пт, нижче - банкр
2	$К_{\text{вк/зал кап}}$	0,478	0,318	0,853	0,9	0,957	0,65-0,77 0,78-0,84 0,85-0,9 0,91-0,99
3	$К_{\text{фін стійк}}$	0,489	0,487	0,671	0,721	0,649	0,5-0,55 0,56-0,59 0,6-0,66 0,67-0,71 *0,7-0,9., нижче недост фін стій*
4	$К_{\text{ман ВК}}$	-1,421	-1,389	-0,573	-0,38	-0,29	0,03-0,04 0,05-0,06 0,07-0,089 *0,09-0,099* *0,1 і вище, позит - достатн ВК*
5	$К_{\text{заб ВОК}}$	-9,01	-7,67	-4,052	-1,867	-0,678	0,049-0,058 0,059-0,078 0,079-0,088 0,089-0,099 *0,1 і вище.*
6	$К_{\text{чист заборг}}$ (важіль)	2,42	1,47	2,39	1,64	1,399	0,2-0,3 0,31-0,38 0,39-0,42 0,43-0,49 норм за ранг риз. , більше 0,5

продовження таблиці Б.35

7	К покрит	0,048	0,115	0,198	0,349	0,596	0,72-0,8 0,81-0,83 0,84-0,94 0,95-1 *норм 1-3, оптимальним є значення 2-3. Показник нижче нормативного свідчить про проблемний стан платоспроможності*
8	К шв ліквід	0,097	0,113	0,195	0,344	0,585	0,2-0,29 0,3-0,39 0,4-0,44 0,45-0,5 *0,5-1 і вище*
9	К абсол лікв	0,048	0,063	0,138	0,277	0,483	0,05-0,1 0,11-0,14 0,15-0,2 *від 0,1 до 0,2.*
10	К R кап	0,01	0,1	0,12	0,05	-0,28	> 0, 46 (ереднє за конкурентами галузі)
11	К Rвк	0,05	0,26	0,25	0,23	-0,1	0,27-0,34 0,35-0,4 0,41-0,45 0,46-0,5 *зростання коеф означає підвищення здатності комп генерувати приб власникам.*
12	К R прод, роб, посл	0,53	0,76	0,49	0,83	0,59	0,27-0,34 0,35-0,4 0,41-0,45 0,46-0,5 *порівн із конкур*
13	К R продажів	0,02	0,11	0,15	0,12	-0,09	>0,05
14	К R госп дія-ті	0,03	0,21	0,27	0,23	0,15	порівн із конкур

Таблиця Б.36

Динаміка індикатора електронно-комунікаційної складової безпеки ТОВ “Датагруп” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа **= біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	Квід станд МСЕ (відпов станд)	0,84	0,88	0,88	0,89	0,91	
2	К конверг ІКМ(об’єдн мереж ауд тел комп)	0,59	0,61	0,61	0,62	0,63	0,5-0,65 0,76-0,86 0,85-0,89 0,09-0,95
3	Кзаб хPON						

продовження таблиці Б.36

4	K MAU	0,06	0,07	0,08	0,11	0,12	0,11-0,26 0,27-0,31 0,32-0,36 0,37-0,42
5	K кіберсвід культ (кіберсвідчення культури)	0,61	0,64	0,65	0,65	0,71	0,65-0,79 0,8-0,84 0,85-0,9 0,91-0,99
6	K сис-ми зах інф та кіберб	0,65	0,68	0,71	0,73	0,74	0-0,24 0,25-0,49 0,5-0,74 0,75-,09

Таблиця Б.37

Динаміка індикатора екологічної складової безпеки ТОВ “Датагруп” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	$K_{R\ стал\ розв}$ (стал розвитку)	0,2	0,21	0,23	0,26	0,26	0,15-0,19 0,2-0,26 0,27-0,34 0,35-0,45
2	K впров еко-техн (впровадження екотехнологій)	0,03	0,05	0,1	0,1	0,15	0,09-0,11 0,12-0,14 0,15-0,17 0,18-0,19
3	$K_{екол\ вплив}$ (еколог впливу на навк середовище)	0,61	0,62	0,61	0,62	0,61	0,23-0,21 0,20-0,18 0,17-0,15 0,14-0,12
4	K екол серт (екол сертифікації послуг)	0,33	0,36	0,39	0,45	0,51	0,5-0,62 0,63-0,7 0,71-0,94 0,95-0,99
5	K поруш нор екол (порушення норм екол зак-ва)	-	-	-	-	-	0,19-0,17 0,16-0,13 0,12-0,06 0,05-0

Таблиця Б.38

Динаміка індикатора фізичної (силової) складової безпеки ТОВ “Датагруп” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа (біфуркація)
1	K відв прон (відвернутих проникнень)	1	1	1	1	1	1

продовження таблиці Б.38

2	$К_{відверн комп крадіж}$ (спроб комп крадіжок)	1	1	1	1	1	1
3	$К_{відв нанес шкоди персон}$ (відвер спроб фіз шкоди)	1	1	1	1	1	1
4	$К_{над персон}$ (надійності персоналу)	0,95	0,97	0,97	0,98	0,98	1

Таблиця Б.39

Динаміка індикаторів інтелектуально-кадрової (персонал-інтелектуальної) безпеки ТОВ “Датагруп” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	$К_{задов ум праці}$ (задоволеності умовами праці)	0,74	0,76	0,78	0,78	0,82	0,45-0,65 0,66-0,74 0,75-0,87 0,88-0,95
2	$К_{дотрим норм-умов}$ (дотримання норм праці (випром))	0,86	0,86	0,87	0,86	0,86	0,75-0,84 0,85-0,89 0,9-0,97 0,96-0,99
3	$К_{плин персон вис кв}$ (плин персон високої кваліфік)	0,065	0,061	0,063	0,071	0,13	0,096-0,091 0,09-0,085 0,084-0,082 0,081-0,079
5	$К_{винах акт}$ (винахідницької (раціоналізаторської) активності)	0,43	0,43	0,46	0,45	0,49	0,69-0,76 0,77-0,82 0,83-0,88 0,89-0,93
6	$К_{заб осв перс}$ (забезп освітченим персоналом)	0,55	0,54	0,49	0,53	0,51	0,52-0,58 0,59-0,64 0,65-0,7 0,71-0,75
7	$К_{плин персон}$ (плинності)	0,23	0,26	0,28	0,21	0,38	0,25-0,16 0,15-0,11 0,12-0,1 0,09-0,03
8	$К_{R ор}$ еф пер (рентаб організ ефект-ті персоналу)	0,74	0,76	0,78	0,81	0,8	0,79-0,81 0,82-0,88 0,89-0,93 0,94-0,97
	$К_{Фехнера}$ (відповід цілей персон цілям підпр)	0,41	0,56	0,45	0,43	0,5	-1; 0; 1

Таблиця Б.40

Динаміка індикаторів інформаційної, інтерфейсної, політико-правової безпеки ТОВ “Датагруп” за 2018-2022 рр.

№ з/п	Індикатор	Роки					Критерій
		2018	2019	2020	2021	2022	критична нижня межа; нижня межа = **біфуркація** нижня межа; прийнятна верхня межа = **репелер**
1	$K_{повн\ інф}$	0,88	0,89	0,81	0,85	0,79	Більше 0,91
2	$K_{точ\ інф}$ (точності інформації)	0,84	0,84	0,71	0,74	0,69	Більше 0,82
4	$K_{рівн\ гот\ до\ кіберінц}$	0,76	0,78	0,83	0,88	0,74	Більше 0,8
5	$K_{вияв\ втор}$ (вияв вторгнень)	0,77	0,86	0,89	0,89	0,79	Більше 0,85
7	$K_{поруш\ догов}$	0,13	0,12	0,11	0,06	0,05	Менше 0,05
8	$K_{судов\ справ\ за\ дог}$ (порушення конт договорів)	0,11	0,1	0,09	0,05	0,03	Менше 0,1
11	$K_{репут}$ (репутації)	0,91	0,93	0,94	0,95	0,79	Більше 0,9
12	K достр прип дог (дострокового припинення договорі)	0,05	0,04	0,04	0,03	0,12	Менше 0,05
13	$K_{компл}$ (комплаєнс-дисципліни)	0,95	0,95	0,95	0,95	0,95	Більше 0,91

Рівень інформаційної безпеки може бути визначений на основі добутку трьох згаданих коефіцієнтів: $Ki = Kni*Kmi*Kci$. При цьому, якщо:

$Ki \geq 0,7$ – рівень безпеки високий;

$0,3 \leq Ki < 0,7$ – рівень безпеки середній;

$Ki < 0,3$ – рівень безпеки низький.

ДОДАТОК В

№ 259-24
від 15.05.2024 р.

Про впровадження результатів дисертаційної роботи

До спеціалізованої вченої ради Д 26.861.03

ДОВІДКА

про впровадження результатів дисертаційного дослідження

Капелюшної Тетяни Вікторівни

«Управління безпекою підприємства: теорія та методологія»

представленого на здобуття наукового ступеня доктора економічних наук.

Основні положення, рекомендації дисертаційного дослідження на здобуття наукового ступеня доктора економічних наук Капелюшної Тетяни Вікторівни можуть використовуватись в аналітичній роботі компанії ТОВ «НВО «Інформаційні технології».

Слід відмітити, що тематика дослідження актуалізована умовами невизначеності, в яких на сьогодні функціонують підприємства, тому питання безпеки на підприємствах та управління нею вартують розгляду та досліджень. Заслуговує уваги запропонована концепт-методологія управління безпекою підприємства в частині ідентифікації площини безпеки за рахунок побудови її за стійкими та нестійкими точками, які визначаються відхиленнями показників від критеріальних значень (порогових та критичних) за попередньо означеними групами складових, що вказуватимуть на перебування значення показника у зоні ризику або загрози й, відповідних площинах безпеки, що сприятиме пошуку прийнятного для кожного конкретного стану підходу до управління безпекою, що і значиться у дослідженні, й дозволяє зробити висновок про доцільність до використання у практичній діяльності постачальниками електронних комунікаційних послуг.

Генеральний директор — Фесенко С.Д.

Посада — ПІБ

Про впровадження результатів
дисертаційної роботи

До спеціалізованої вченої
ради Д 26.861.03

АКТ

про впровадження результатів дисертаційного дослідження

Капелюшної Тетяни Вікторівни

на тему "**Управління безпекою підприємства: теорія та методологія**"

Основні положення та рекомендації дисертаційного дослідження на здобуття наукового ступеня доктора економічних наук Капелюшної Т.В. можуть використовуватись в аналітичній діяльності ДП "ЕС ЕНД ТІ УКРАЇНА".

Практична цінність представленої роботи полягає у запропонованій диференціації підходів до управління безпекою підприємства, в залежності від порушень стану безпеки, які визначаються відхиленнями цільових показників від заздалегідь сформованих індикаторів за складовими безпеки, зокрема: фінансової, техніко-технологічної, виробничої, енергетичної, ринкової, інтелектуального капіталу, інтерфейсної, інформаційної, силової, політико-правової, екологічної, інвестиційно-інноваційної, електронно-комунікаційної складових безпеки підприємства.

Відзначається запропонована у роботі електронно-комунікаційна складова, вплив якої на безпеку підприємства актуалізований умовами цифровізації суспільства, держави, і, як результат, зростанням кібер- та інформаційних інцидентів, що порушують безпеку підприємства та загрожують інформаційним активам й, відповідно, результатам діяльності.

Генеральний директор
ДП «ЕС ЕНД ТІ УКРАЇНА»,
доктор технічних наук, доцент,
член Вченої ради Інституту проблем
математичних машин і систем
Національної академії наук України

Лисецький Ю.М.

Паперова копія електронного документа

НАЦІОНАЛЬНА КОМІСІЯ, ЩО ЗДІЙСНЮЄ ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРАХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ, РАДІОЧАСТОТНОГО СПЕКТРА ТА НАДАННЯ ПОСЛУГ ПОШТОВОГО ЗВ'ЯЗКУ

вул. Солом'янська, 3, м. Київ, 03110, тел./факс. (044) 202-00-43 тел. (044) 202-00-10, (044) 202-00-22,
E-mail: kabmin_doc@nkrzi.gov.ua, сайт: www.nkrzi.gov.ua
код згідно з ЄДРПОУ 37994258

від 12.06.2024 р. № 06-4065/103

На № _____ від _____ р.

Державний університет інформаційно-комунікаційних технологій (спеціалізована вчена рада Д 26.861.03)
вул. Солом'янська, 7,
м. Київ, 03110

ДОВІДКА
про впровадження результатів дисертаційного дослідження Капелюшної Тетяни Вікторівни

«Управління безпекою підприємства: теорія та методологія»
представленого на здобуття наукового ступеня доктора економічних наук

Основні положення, рекомендації дисертаційного дослідження на здобуття наукового ступеня доктора економічних наук Капелюшної Тетяни Вікторівни можуть використовуватись в аналітичній роботі ТОВ «НВО «Інформаційні технології».

Слід відмітити, що тематика дослідження актуалізована умовами невизначеності, в яких на сьогодні функціонують підприємства, тому питання безпеки на підприємствах та управління нею вартують розгляду та досліджень. Заслуговує уваги запропонована концепт-методологія управління безпекою підприємства в частині ідентифікації площини безпеки за рахунок побудови її за стійкими та нестійкими точками, які визначаються відхиленнями показників від критеріальних значень (порогових та критичних) за попередньо означеними групами складових, що вказуватимуть на перебування значення показника у зоні ризику або загрози й, відповідних площинах безпеки, що сприятиме пошуку прийнятного для кожного конкретного стану підходу до управління безпекою, що і значиться у дослідженні, й дозволяє зробити висновок про доцільність до використання у практичній діяльності постачальниками електронних комунікаційних мереж та послуг.

Член Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку — Микола ТКАЧЕНКО

Братіца М.С. 202-00-80
bratitsa@nkrzi.gov.ua

UB
НКЕК
№06-4065/103 від 12.06.2024
КЕП: Ткаченко М. М. 12.06.2024 11:37
26B2648ADD3032E1040000007 65E3200BE81AE00

Паперова копія електронного документа

**НАЦІОНАЛЬНА КОМІСІЯ,
ЩО ЗДІЙСНЮЄ ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРАХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ, РАДІОЧАСТОТНОГО СПЕКТРА ТА НАДАННЯ ПОСЛУГ ПОШТОВОГО ЗВ'ЯЗКУ**

вул. Солом'янська, 3, м. Київ, 03110, тел./факс. (044) 202-00-43 тел. (044) 202-00-10, (044) 202-00-22,
E-mail: kabmin_doc@nkrzi.gov.ua, сайт: www.nkrzi.gov.ua
код згідно з ЄДРПОУ 37994258

від 17.06.2024 р. № 06-4169/103

На № _____ від _____ р.

Державний університет
інформаційно-комунікаційних
технологій
(спеціалізована вчена рада
Д 26.861.03)
вул. Солом'янська, 7,
м. Київ, 03110

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Капелюшної Тетяни Вікторівни
«Управління безпекою підприємства: теорія та методологія»
представленого на здобуття наукового ступеня доктора економічних наук

У межах рішень НКЕК від 06.03.2024 № 105 «Про схвалення проекту розпорядження Кабінету Міністрів України «Про затвердження плану заходів із забезпечення стійкості електронних комунікаційних мереж» та від 29.05.2024 № 296 «Про розгляд проекту постанови Кабінету Міністрів України «Деякі питання оперативно-технічного управління електронними комунікаційними мережами в умовах надзвичайної ситуації, надзвичайного або воєнного стану» основні положення, рекомендації дисертаційного дослідження на здобуття наукового ступеня доктора економічних наук Капелюшної Тетяни Вікторівни можуть використовуватись в аналітичній роботі Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку.

Слід відмітити, що тематика безпеки підприємств особливо актуальна за нинішніх умов при низькій поінформованості щодо функціонування підприємств на найближчу перспективу, саме тому питання управління безпекою підприємств потребують досліджень та вирішення для завчасного упередження загрозливих ситуацій й реакції на виклики, динамічність середовища.

Відзначається грунтовно проведений у роботі теоретичний огляд проблематики безпеки з подальшим аналізом ринку постачання електронних

UB
НКЕК
№06-4169/103 від 17.06.2024
КЕП: Ткаченко М. М. 17.06.2024 17:26
26B2648ADD3032E104000000765E3200BE81AE00

комунікаційних мереж та послуг для внесення рекомендацій та пропозицій щодо управління безпекою підприємства грунтуючись на теоретичних та методологічних результатах дослідження. Вважається доцільним управління безпекою підприємствами-постачальниками електронних комунікаційних мереж та послуг за пропонованими чотирма сценаріями розвитку, які сформовані, зважаючи на сьогоднішню безпекову невизначеність та враховують вірогідні наслідки викликів, з подальшим розглядом стратегічних можливостей розвитку підприємств, пошуком заходів безпеки за наявних можливостей використання ресурсів.

Член Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку Микола ТКАЧЕНКО

ТОВ «IT Спеціаліст», 03124, Україна, м.Київ
бул. Вацлава Гавела, 6, корпус 3
ЄДРПОУ 39230764, +38 044 390 81 90

№ 965 від 28.05.2024 р.

До спеціалізованої вченої ради
Д 26.861.03

Про впровадження
результатів дисертаційної роботи

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Капелюшної Тетяни Вікторівни
на тему: "Управління безпекою підприємства: теорія та методологія"

ТОВ "IT СПЕЦІАЛІСТ" прийняло до розгляду та використання методичні положення та рекомендації щодо управління безпекою підприємства, в частині виокремлення традиційних та адаптованих до мінливих умов функціонування підприємства підходів до управління, що пристосовані до умов, в яких функціонує підприємство, а саме: процесно-структурований, ситуаційно-функціональний, ресурсно-функціональний, структурно-функціональний, ризик-орієнтований, в основі яких залягають традиційні підходи: функціональний, процесний, системний, ситуаційний та комбінований підходи. Більшою мірою, зважаючи на сьогоднішні умови функціонування підприємств, значиться запропонований у науково-дослідній роботі резистентно-ситуаційний підхід, за яким визначається стан безпеки (небезпеки) в залежності від ризику, як вірогідності впливу на функціонування підприємства, та загрози, як похідної від ризику, якими провокуються зміни різної інтенсивності у функціонуванні підприємства й відхилення від цільових результатів діяльності, тож даний запропонований підхід сприятиме керованості та об'єктивності управлінських рішень в сьогоднішніх невизначених умовах.

Директор

ТОВ "IT СПЕЦІАЛІСТ" **Олексій Морозов**

ТОВ "ПРОКОМ", ЄДРПОУ 13605118
м. Запоріжжя, вул. Перемоги, 97а
IBAN 153133990000026002055710692
ІПН 136051106299, Св.№11820043
тел. (099) 30 099 50
office@procom.zp.ua
csoprocom.zp.ua

До спеціалізованої вченої ради Д 26.861.03

Вих.№ 3345 від 05 червня 2024 р.

Про впровадження результатів дисертаційної роботи

ДОВІДКА
про впровадження результатів отриманих при виконанні дисертаційного дослідження Капелюшною Тетяною Вікторівною
на тему: «Управління безпекою підприємства: теорія та методологія»

Основні положення, рекомендації дисертаційного дослідження на здобуття наукового ступеня доктора економічних наук Капелюшної Тетяни Вікторівни можуть використовуватись в аналітичній роботі ТОВ «Проком».

Відзначається актуальність теми дослідження у контексті пошуку шляхів розвитку та потреби в адаптації підприємств до безпекової ситуації з урахуванням умов, в яких на сьогодні функціонують підприємства. Заслуговує уваги пропозиція перегляду підходів до управління підприємством під впливом ризиків та загроз, а також дослідження викликів перед якими нині постають підприємства. Доцільним є запропонований у роботі якісний аналіз середовища господарюючих суб'єктів та визначення ентропії (ступеня невизначеності ситуації) для формування висновків щодо стану безпеки й прогнозування цільових результатів діяльності, а також обрання на їх основі стратегії управління підприємством у повоєнний період, що вказує на значимість отриманих результатів дослідження та можливість їх використання у роботі підприємства на практиці.

З повагою,
Директор ТОВ «ПРОКОМ» **Сергій БУТЕНКО**

"ПРОКОМ" №13605118

Про впровадження результатів дисертаційної роботи

До спеціалізованої вченої ради Д 26.861.03

АКТ

про впровадження результатів дисертаційного дослідження

Капелюшної Тетяни Вікторівни

на тему «**Управління безпекою підприємств: теорія та методологія**»

представленого на здобуття наукового ступеня доктора економічних наук

Основні положення та рекомендації дисертаційного дослідження на здобуття наукового ступеня доктора економічних наук Капелюшної Т.В. можуть використовуватись в аналітичній діяльності підприємства ТОВ «ЄВРОСТРАТОС»

На сьогодні умови та середовище, в яких господарюють суб'єкти характеризується, як зовнішньою нестабільністю, так і коливаннями всередині організацій, тому питання безпеки особливо актуальні та потребують вирішення, що підтверджує доцільність теми дослідження й своєчасність.

Практична цінність представленої роботи полягає у пропозиції прогнозування прибутків, грунтуючись на вирахованій ентропії невизначеності середовища функціонування суб'єктів господарювання, що дозволяє розглядати можливі варіанти перспектив розвитку підприємств та планувати діяльність.

Директор

ТОВ «ЄВРОСТРАТОС» С.В. Дмитроца

Про впровадження результатів
дисертаційної роботи

№57 від 18.05.2024 р.

До спеціалізованої вченої
ради Д 26.861.03

ДОВІДКА

про впровадження результатів отриманих при виконанні дисертаційного дослідження Капелюшною Тетяною Вікторівною на тему: «Управління безпекою підприємств: теорія та методологія»

Зважаючи на безпекову ситуацію, що склалася нині, підприємства мають упереджувати загрози для розвитку та функціонування підприємств, моніторити спроможність протидії невизначеності середовища, проводити оцінку безпеки фінансово-економічних показників діяльності, тому тема актуальна та доречна для дослідження. Відзначаються запропоновані у дисертаційному дослідженні метрики результатів безпеки, що є показовими для стейкхолдерів та дозволяють проводити оцінку безпеки функціонування підприємств, слугують підґрунтям для прийняття рішень щодо управління безпекою.

Вартує уваги запропонована у роботі електронно-комунікаційна складова, вплив якої на безпеку підприємства актуалізований умовами цифровізації суспільства, держави, і, як результат, зростанням кібер- та інформаційних інцидентів, що порушують безпеку підприємства та загрожують інформаційним активам й, відповідно, результатам діяльності підприємства.

Вважаємо прийнятними до використання у практичній діяльності ТОВ «АМ «АРТ-ПРОЄКТ»» запропоновані метрики безпеки, що слугуватимуть підґрунтям для прийняття рішень щодо управління підприємством та забезпечення безпечного функціонування.

Директор
ТОВ«АМ «АРТ-ПРОЄКТ»

Б.А. Тодуа

ЗАТВЕРДЖУЮ
Перший проректор
Державного університету
інформаційно-комунікаційних
технологій

_____ Олександр КОРЧЕНКО
«07» 06 2024 р.

АКТ

впровадження в освітній процес Державного університету інформаційно-комунікаційних технологій наукових результатів **Капелюшної Тетяни Вікторівни**, одержаних під час проведення дисертаційного дослідження на тему «Управління безпекою підприємств: теорія та методологія» на здобуття наукового ступеня доктора економічних наук
зі спеціальності 08.00.04 – економіка та управління підприємствами
(за видами економічної діяльності)

Комісія у складі:

голови комісії – директора Навчально-наукового інституту захисту інформації, д.т.н., професора Савченка В.А.;

членів комісії:

професора кафедри Підприємництва, торгівлі та біржової діяльності, д.е.н., професора Сьомкіної Т.В.; завідувача кафедри Інформаційної та кібернетичної безпеки, д.т.н., професора Гайдур Г.І.; професора кафедри економіки Голобородько А.Ю., д.е.н., професора провела роботу щодо визначення фактичного впровадження результатів наукового дослідження здобувача наукового ступеня доктора наук кафедри управління інформаційною та кібернетичною безпекою в освітній процес Державного університету інформаційно-комунікаційних технологій.

У результаті проведеної роботи комісія встановила:

1. Нові наукові результати, одержані Капелюшною Т.В., використовуються під час навчальних занять зі здобувачами вищої освіти за спеціальністю 125 Кібербезпека та захист інформації освітніх рівнів Бакалавр та Магістр у наступних дисциплінах:

математична модель Ляпунова для визначення безпекової площини підприємством, визначення нестійких точок, що впливають на цільові результати безпеки - під час проведення занять з дисципліни «Економічна безпека діяльності підприємства»;

визначення стану безпеки управління безпекою підприємств за репелер та біфуркаційними точками – під час проведення занять з дисциплін «Економічна безпека діяльності підприємства»;

визначення інформаційної складової безпеки підприємства (за пропонованими індикаторами) - під час проведення занять з дисципліни «Управління інформаційною безпекою банків»;

методологія управління безпекою підприємства - під час проведення занять з дисципліни «Організація проведення наукових досліджень».

2. Зазначені наукові результати Капелюшної Т.В. представлені у формі окремих навчальних питань і включені до методичних розробок для лекційних та практичних занять, які проводяться у Державному університеті інформаційно-комунікаційних технологій.

Голова комісії:

Директор Навчально-наукового інституту захисту інформації
д.т.н., професор — Віталій САВЧЕНКО

Члени комісії:

Завідувач кафедри Інформаційної та кібернетичної безпеки
д.т.н., професор — Галина ГАЙДУР

Професор кафедри Підприємництва, торгівлі та біржової діяльності
д.е.н., професор — Тетяна СЬОМКІНА

Професор кафедри Економіки
д.е.н., професор — Альона ГОЛОБОРОДЬКО

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Kapeliushna T., Lehominova S., Goloborodko A., Lysetskyi Yu., Nosova T. Methodological approaches to enterprise security management: traditional and transformed to the conditions of functioning. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024. No. 3. P. 204-209. URL: https://doi.org/10.33271/nvngu/2024-3/204. *(0,99 д.а., авторський внесок 0,2 д.а., полягає в аналізі методичних підходів до управління безпекою підприємства).*

2. Kapeliushna T., Goloborodko A., Nesterenko S. Bezhenar I., Matviichuk B. Analysis of digitalization changes and their impact on enterprise security management under uncertainty. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2023. No. 4. P. 150–156. URL: https://doi.org/10.33271/nvngu/2023-4/150. *(1,01 д.а., авторський внесок 0,21 д.а., полягає в обґрунтуванні врахування трансформаційних змін, що викликані діджиталізацією в управлінні безпекою).*

3. Kapeliushna T., Dymenko R., Safonov Yu. Kachmala V., Borshch V., Sheremet O. Digital tools for effective student learning and training online in conditions of uncertainty. *Financial and Credit Activity Problems of Theory and Practice*. 2022. Vol. 6, No. 47. P. 469–479. URL: https://doi.org/10.55643/fcaptp.6.47.2022.3817. *(0,9 д.а., авторський внесок 0,15 д.а., полягає в означенні електронних комунікаційних послуг та технологій, як основи забезпечення безпечного функціонування господарюючих одиниць за умов невизначеності).*

4. Kryshtal H., Kapeliushna T., Kalina I., Shuliar N., Martynenko M. Trends of development of financial and economic activity of entrepreneurial structures during the period of quarantine restrictions. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2022. No. 1. P. 139–144. URL: https://doi.org/10.33271/nvngu/2022-1/139. *(0,74 д.а., авторський внесок 0,14 д.а., полягає в аналізі трендів безпеки та можливостей забезпечення безперебійної роботи підприємства в умовах пандемії).*

5. Zghurska O., Dymenko R., Semkina T., Kapeliushna T. Diversification Strategy of Entrepreneurial Activity in Conditions of European Integration. *International Journal of Innovative Technology and Exploring Engineering*. 2019. Vol. 9, no. 1. P. 4809–4815. URL: https://doi.org/10.35940/ijitee.j9443.119119. *(0,7 д.а., авторський внесок 0,14 д.а., полягає в формуванні безпекових орієнтирів у функціонуванні підприємств в умовах євроінтеграції).*

6. Капелюшна Т. В. Управління безпекою підприємства в умовах невизначеності: система контролю загроз. Відбудова для розвитку: зарубіжний досвід та українські перспективи: міжнародна колективна монографія. Київ : ДУ "Ін-т екон. та прогнозув. НАН України", 2023. С. 474-486. URL: http://ief.org.ua/wp-content/uploads/2023/08/Reconstruction-for-development.pdf *(0,69 д.а.).*

7. Yakymenko Yu., Rabchun D., Kapeliushna T. Use of methodological approaches of system analysis to ensure information security of critical infrastructure objects. *Challenges and threats to critical infrastructure : Collective monograph.*. Detroit : NGO Institute for Cyberspace Research, 2023. P. 46-51. URL: https://conference.cyberspace.org.ua/wp-content/uploads/2023/06/Monograph-09-06-2023.pdf#page=46 *(0,36 д.а., авторський внесок 0,12 д.а., в частині пропозицій проведення системного аналізу безпеки функціонування підприємств).*

8. Капелюшна Т. В. Методологічний концепт управління безпекою підприємства. *Інвестиції: практика та досвід.* 2024. № 10. С. 69-74. URL: https://doi.org/10.32702/2306-6814.2024.10.69 *(0,4 д.а.)*

9. Капелюшна Т. В. Формування площини безпеки підприємства під дією ризиків і загроз. *Бізнес інформ.* 2024. Т. 3, № 554. С. 255–262. URL: 10. https://doi.org/10.32983/2222-4459-2024-3-255-262 *(0,42 д.а.)*

10. Капелюшна Т. В. Безпека даних підприємства у хмарному середовищі: аналіз загроз. *Облік і фінанси*. 2023. № 4(102). С. 97-104. URL: https://afj.org.ua/ua/journals/2023/4/ *(0,49 д.а.)*

11. Капелюшна Т. В., Голобородько А. Ю. Врахування інформаційних викликів при управлінні безпекою підприємств у сьогоденних невизначених

умовах. *European Journal of Economics and Management.* 2023. Т. 9, № 1. С. 12-21. URL: https://doi.org/10.46340/eujem.2023.9.1.2 *(0,61 д.а., авторський внесок 0,31 д.а. полягає в обґрунтуванні врахування інформаційних викликів в управлінні безпекою підприємства).*

12. Капелюшна Т. В. Врахування впливу загроз соціальної інженерії при управлінні безпекою підприємства. *Інвестиції: практика та досвід*. 2023. № 8. С. 125-130. URL: https://www.nayka.com.ua/index.php/investplan/article/view/1374/1384 *(0,36 д.а.)*

13. Капелюшна Т. В. Захист безпечного функціонування телекомунікаційних підприємств в умовах цифровізації та невизначеності. *Агросвіт*. 2023. No 7-8. С. 115-123. URL: https://www.nayka.com.ua/index.php/agrosvit/article/view/1351/1361 *(0,42 д.а.)*

14. Голобородько А. Ю., Капелюшна Т. В. Формування цифровізації інтегративного розвитку економіки та підприємств, як її елементів. *European Journal of Economics and Management.* 2022. Т. 8, № 6. С.5-13. URL: https://doi.org/10.46340/eujem.2022.8.6.1 *(0,88 д.а., авторський внесок 0,08 д.а., полягає в обґрунтуванні імперативів цифровізації економіки та розвитку підприємств).*

15. Капелюшна Т. В. Розширення базових складових економічної безпеки підприємства з урахуванням умов невизначеності. *Ефективна економіка*. 2022. № 10. URL: https://www.nayka.com.ua/index.php/ee/article/view/675/683 *(0,42 д.а.)*

16. Капелюшна Т. В., Пильнова В. П., Полякова А. О., Купрієнко Є. О. Роль електронної комерції в умовах формування цифрової держави та інформатизації суспільства. *Економіка. Менеджмент. Бізнес.* 2021. № 4. С. 68-75. URL: http://nbuv.gov.ua/UJRN/ecmebi_2021_4_13 *(0,45 д.а., авторський внесок 0,18 д.а., полягає в відзначенні потреби посилення захисту та безпеки підприємств, що представляють товари та послуги на електронних комерційних платформах).*

17. Капелюшна Т. В., Дименко Р. А. Експертна оцінка щодо надання телекомунікаційних послуг. *Ефективна економіка*. 2021. № 8. URL: http://www.economy.nayka.com.ua/?op=1&z=8811 *(0,7 д.а., авторський внесок 0,36 д.а., полягає в пропозиції визначення ключових показників якості для формування позитивного сприйняття постачальника послуг та захисту від втрати економічних вигід).*

18. Капелюшна Т. В., Кришталь Г. О., Ващенко О. О. Огляд та аналіз розвитку ринку державних боргових цінних паперів в Україні. *Ефективна економіка*. 2021. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=8811 *(0,7 д.а., авторський внесок 0,24 д.а., полягає в визначенні пріоритетних напрямів вкладення коштів в державні боргові цінні як найбільш безпечні з точки зору ризиків фінансових втрат).*

19. Капелюшна Т. В., Пильнована В. П., Овсійчук В. Я., Красник О. А. Місце інноваційних ризиків у системі економічної безпеки підприємства. *Економіка. Менеджмент. Бізнес.* 2021. № 4. С. 61-68. URL: http://nbuv.gov.ua/UJRN/ecmebi_2021_4_12 *(0,41 д.а., авторський внесок 0,19 д.а., полягає в дослідженні ризиків та визначенні їх місця в системі економічної безпеки підприємства).*

20. Капелюшна Т. В., Гавриш О. М. Проблеми неформального інвестування інноваційного підприємництва в Україні. *Ефективна економіка.* 2020. № 12. URL: http://nbuv.gov.ua/UJRN/efek_2020_12_69 *(0,68 д.а., авторський внесок 0,36 д.а., полягає в обґрунтуванні доцільності інвестування ризикових інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).*

21. Пильнова В. П., Гавриш О. М., Капелюшна Т. В. Організація експорту товарів суб'єктами малого та середнього бізнесу. *Агросвіт.* 2020. № 24. С. 29–36. URL: http://www.agrosvit.info/pdf/24_2020/5.pdf *(0,8 д.а., авторський внесок 0,26 д.а., полягає в обґрунтуванні доцільності експорту як заходу захисту та убезпечення підприємства від зменшення продажів на внутрішньому ринку).*

22. Пильнова В. П., Гавриш О. М., Капелюшна Т. В. Формування системи управління підприємницькими ризиками. *Інвестиції: практика та досвід.* 2020. № 24. С. 51-57. URL: http://www.investplan.com.ua/?op=1&z=7258&i=6 *(0,38 д.а., авторський внесок 0,13 д.а., полягає в обґрунтуванні доцільності інвестування ризикових інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).*

23. Гавриш О. М, Згурська О. М., Капелюшна Т. В., Мартиненко М. О. IT-послуги як об'єкт міжнародної торгівлі. *Міжнародний науковий журнал "Інтернаука". Серія:"Економічні науки".* 2020. № 11. URL: https://www.inter-nauka.com/ua/issues/economic2020/11/6585 *(0,7 д.а., авторський внесок 0,16 д.а., полягає в формуванні безпекових засад надання IT послуг на зовнішніх ринках).*

24. Капелюшна Т. В., Гавриш О. М., Пильнова В. П. Діагностика та тенденції розвитку міжнародної торгівлі в Україні. *Ефективна економіка.* 2020. № 11. URL: http://www.economy.nayka.com.ua/?op=1&z=8379 *(0,65 д.а., авторський внесок 0,23 д.а., полягає в означення загроз безпеці підприємств з урахуванням тенденцій розвитку міжнародної торгівлі).*

25. Капелюшна Т. В., Гавриш О. М., Дименко Р. А. Новації оподаткування підприємницької діяльності. *Інфраструктура ринку*. 2020. № 49. URL: http://www.market-infr.od.ua/uk/49-2020 *(0,75 д.а., авторський внесок 0,27 д.а., полягає в визначенні перспектив та ризиків в оподаткуванні для підприємств).*

26. Гавриш О. М., Пильнова В. П., Капелюшна Т. В. Планування торговельної діяльності підприємств на міжнародних ринках. *Підприємництво і торгівля*. 2020. № 27. С. 21-25. URL: http://journals- lute.lviv.ua/index.php/pidpr-torgi/article/view/699/664. *(0,68 д.а., авторський внесок 0,23 д.а., полягає в обґрунтуванні доцільності інвестування ризикових інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).*

27. Пильнова В. П., Гавриш О. М., Капелюшна Т. В., Лобань О. О. Інтернет-торгівля: особливості реалізації товару за допомогою інтернету. *Економіка. Менеджмент. Бізнес.* 2020. № 1. С. 122–130. URL:

http://journals.dut.edu.ua/index.php/e_mb/article/view/2394 *(0,51 д.а., авторський внесок 0,19 д.а., полягає в обґрунтуванні доцільності інвестування ризикових інноваційних проєктів шляхом неформального інвестування, як безпечної форми залучення коштів у разі згортання проєктів).*

28. Kapeliushna T. Organizational Mechanism for the Formation of an Innovative Enterprise in the Conditions of a New Technological Structure. *Science and Education a New Dimension.* 2019. Vol. VII, Is. 213, №. 35. P. 16-19. URL: https://doi.org/10.31174/send-hs2019-213vii35-03 *(0,42 д.а.)*

29. Капелюшна Т. В. Аналіз та тенденції розвитку фондового ринку в Європейському регіоні та Україні. *Бізнес Інформ.* 2019. Т. 12. № 503. С. 290-296. URL: https://doi.org/10.32983/2222-4459-2019-12-290-296 *(0,41 д.а.)*

30. Капелюшна Т. В. Роль інноваційного підприємства в умовах нового технологічного укладу. *Економіка. Менеджмент. Бізнес.* 2019. № 3(29). С. 71-77. URL: https://doi.org/10.31673/2415-8089.2019.037177 *(0,42 д.а.)*

31. Kryshtal H., Kapeliushna T. Synergy of the banking sector and socio-economic under the influence of the state regulator. *Підприємництво та інновації.* 2019. № 9. С.147-152. URL: https://doi.org/10.37320/2415-3583/9.24 *(0,63 д.а., авторський внесок 0,31 д.а., полягає в обґрунтуванні доцільності синергії фінансового сектора із соціально-економічним для безпечного функціонування та стабільності роботи підприємницьких структур під наглядом регулятора).*

32. Дименко Р. А., Капелюшна Т. В., Лобань О. О. Ризики впровадження та проблеми правового регулювання цифрової валюти в Україні. *Економіка. Менеджмент. Бізнес.* 2019. № 2(28). С. 72-79. URL: https://journals.dut.edu.ua/index.php/emb/article/view/2153 *(0,68 д.а., авторський внесок 0,22 д.а., полягає в аналізі ризиків впровадження та безпеки цифрової валюти).*

33. Капелюшна Т. В., Згурська О. М. Динаміка розвитку інтернет-речей та їх вплив на управління підприємствами. *Економіка. Менеджмент. Бізнес.* 2018. № 3(25). С. 79-86. URL: https://journals.dut.edu.ua/index.php/emb/article/view/1943 *(0,41 д.а., авторський*

внесок 0,21 д.а., полягає в дослідженні ризиків, додаткових можливостей та безпеки використання інтернет-речей в управлінні підприємствами).

34. Капелюшна Т. В. Оцінювання ефективності механізму управління сталим розвитком підприємства з використанням статико-динамічного підходу. *Економіка. Менеджмент. Бізнес.* 2016. № 3(17). С. 69-74. URL: https://journals.dut.edu.ua/index.php/emb/article/view/758 *(0,36 д.а.).*

35. Капелюшна Т. В. Підхід до оцінки ефективності механізму управління підприємством в контексті сталого розвитку. *Економіка. Менеджмент. Бізнес*. 2016. № 2(16). С. 62-68. URL: https://journals.dut.edu.ua/index.php/emb/article/view/650 *(0,37 д.а.).*

Опубліковані праці апробаційного характеру:

36. Капелюшна Т. В. Пропозиції щодо упередження ризиків інформаційних активів задля захисту репутації підприємства. *Перспективи та проблематика інтелектуальних систем* : зб. наук.-практ. конф., м. Київ, 31 трав. 2024 р. Київ, 2024. С. 54-55. *(0,1 д.а.).*

37. Капелюшна Т. В. Заходи щодо захисту інформаційного середовища підприємства. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу* : матеріали IV всеукр. наук.-практ. конф., м. Київ, 28 лют. 2024 р. Київ, 2024. С.105-108. *(0,15 д.а.).*

38. Капелюшна Т. В., Стріканов Д. О. Інформаційна безпека підприємства: важливість дотримання міжнародних стандартів безпеки. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу* : матеріали IV всеукр. наук.-практ. конф., м. Київ, 28 лют. 2024 р. Київ, 2024. С. 277-280. *(0,16 д.а., авторський внесок 0,12 д.а., полягає в дослідженні стандартів управління інформаційною безпекою підприємства).*

39. Капелюшна Т. В. Актуалізація питань інформаційної та кібернетичної безпеки підприємства в діджитал-умовах. *Глобалізаційні процеси та їх вплив на соціально-економічний та правовий розвиток України* : зб. матеріалів II всеукр. наук.-теор. конф., Київ 20 груд. 2023 р. Київ, 2023. С.92-93. *(0,1 д.а.).*

40. Капелюшна Т. В. Іванов Д. А. Врахування репутаційних ризиків при управлінні інформаційною безпекою компанії. *Актуальні проблеми кібербезпеки* : матеріали всеукр. наук.-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 125-127. URL: https://duikt.edu.ua/uploads/p_2626_52007398.pdf#page=125. *(0,16 д.а., авторський внесок 0,12 д.а., полягає в дослідженні впливу репутаційних ризиків на безпеку підприємства).*

41. Капелюшна Т. В. Чернявський І. Р. Проблема безпеки даних підприємства при використанні хмарних сервісів. *Актуальні проблеми кібербезпеки* : матеріали всеукр. наук.-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 134-135. URL: https://duikt.edu.ua/uploads/p_2626_52007398.pdf#page=134 *(0,1 д.а., авторський внесок 0,08 д.а., полягає в дослідженні проблематики забезпечення безпеки даних підприємства при їх розміщенні у хмарних сервісах).*

42. Капелюшна Т. В. Багаторівневий захист даних підприємств критичної інфраструктури задля зменшення поверхонь атак. *"Забезпечення кібероборони держави" Національного університету оборони України:* матеріали IV наук.-практ. вебінару, *м. Київ,* 10 лист. 2023 р. Київ, 2023. С. 62-65. URL: https://drive.google.com/file/d/1VpULkcweKcyZ-KR8EvxtxQSGYbyS1JSq/view *(0,16 д.а.).*

43. Kapeliushna T. Enterprise security management under uncertainty: a threat control system. *Міжнародний історичний досвід повоєнної реконструкції економіки: уроки для України* : матеріали міжнар. наук.-практ. конф., м. Київ, 27 квіт. 2023 р. Київ, 2023. С. 90. URL: Mizhnar-istor-dosvid-povojen-reconstrukcii-uroky-dla-Ukrainy.pdf (ief.org.ua) *(0,06 д.а.).*

44. Капелюшна Т. В., Голобородько С. О. Безпека функціонуючих господарюючих суб'єктів в сучасних умовах за систематизованого управління ризиками. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу :* матеріали всеукр. наук.-практ. Інтернет-конф., м. Київ, 23 лют. 2023 р.

Київ, 2023. С. 40-42. *(0,13 д.а. авторський внесок 0,09 д.а., полягає в дослідженні стандартів управління інформаційною безпекою підприємства).*

45. Капелюшна Т. В. Упередження від кібернетичних загроз підприємств критичної інфраструктури за використання систем їх контролю. *Шкідливі програми як загроза об'єктам критичної інфраструктури в умовах кібервійни* : зб. матеріалів міжвідомчого круглого столу, м. Київ, 21 лют. 2023 р. Київ, 2023. С. 63-66. URL: https://drive.google.com/file/d/1VpULkcweKcyZ-KR8EvxtxQSGYbyS1JSq/view *(0,17 д.а).*

46. Капелюшна Т. В. Забезпечення безпечного функціонування підприємств за сьогочасних викликів. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку :* матеріали IV міжнар. наук.-практ. конф., м. Київ, 17 лют. 2023 р. Київ, 2023. С. 97-99. *(0,15 д.а.).*

47. Капелюшна Т. В. Інформаційна складова в управлінні економічною безпекою діяльності підприємства. *Актуальні проблеми кібербезпеки :* матеріали всеукр. наук.-практ. конф., м. Київ, 27 жовт. 2022 р. Київ, 2022. С.171-172 –URL: https://dut.edu.ua/uploads/p_2121_20358827.pdf#page=171 *(0,1 д.а.).*

48. Капелюшна Т. В. Врахування впливу інформаційних атак на персонал задля безпеки підприємства. "*Telecommunication: problems and innovation"* : зб. тез всеукр. наук.-практ. конф. Київ, 2022. С.122-123. URL: https://dut.edu.ua/uploads/p_2121_16069800.pdf#page=122 *(0,1 д.а.).*

49. Капелюшна Т. В. Системи управління бізнесом – невід'ємна складова оптимізації бізнес-процесів. *Нові інформаційні технології управління бізнесом* : матеріали VI всеукр. наук.-практ. конф., м. Київ, 16 лют. 2022 р. Київ, 2022. С. 113-116. URL: http://unionba.com.ua/osvita *(0,15 д.а.).*

50. Капелюшна Т. В., Хуторна А. В. Формування товарного асортименту на підприємствах. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку :* матеріали III міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 37- 40. *(0,17 д.а., авторський внесок 0,12 д.а., полягає в дослідженні конкрентоспроможності як*

орієнтиру безпеки підприємства за рахунок клієнтоорієнтованого асортименту).

51. Капелюшна Т. В., Сіненко А. О. Формування соціально-психологічних компетенцій підприємця для досягнення ефективних результатів діяльності. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку:* матеріали ІІІ міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 35-37. *(0,12 д.а., авторський внесок 0,08 д.а., полягає в дослідженні впливу соціально-психологічних компетенцій підприємця на результати діяльності підприємства).*

52. Капелюшна Т. В., Берегова В. О. Переваги ведення підприємницької діяльності в інтернет за сучасних невизначених умов. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку:* матеріали ІІІ міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 132-139. *(0,28 д.а., авторський внесок 0,2 д.а., полягає в дослідженні переваг провадження підприємством своєї діяльності у глобальній мережі за невизначених умов функціонування).*

53. Капелюшна Т. В., Воробей К. О. Метрики визначення оптимізації управління запасами на підприємствах. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали ІІІ міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 32-35. *(0,18 д.а., авторський внесок 0,14 д.а. полягає у деталізації метрик оптимізації управління запасами підприємства для гарантування безпеки постачання й забезпечення безперебійного функціонування підприємств).*

54. Капелюшна Т. В., Дерев'янко Б. О. Дієві методи реклами в сучасних умовах функціонування підприємств. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку :* матеріали ІІІ міжнар. наук.-практ. конф., м. Київ, 15–16 лют. 2022 р. Київ, 2022. С. 177-180. *(0,13 д.а. авторський внесок 0,1 д.а. полягає у моніторингу впливу реклами на результати діяльності підприємства та обґрунтування доцільності вкладень у рекламу).*

55. Капелюшна Т. В. Інноваційні інструменти інтернет-реклами в умовах інформатизації та цифровізації суспільства. *Розвиток економіки та бізнес-адміністрування: наукові течії та рішення* : матеріали III міжнар. наук.-практ. конф., м. Київ, 20–25 трав. 2022 р. Київ, 2022. С. 55-57. *(0,14 д.а.).*

56. Капелюшна Т. В., Новикова І.В. Умови ефективного провадження е-торгівлі. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку:* матеріали II міжнар. наук.-практ. конф., м. Київ, 11–12 лют. 2021 р. Київ, 2021. С. 35- 40. *(0,14 д.а., авторський внесок 0,09 д.а. полягає у дослідженні податкових новацій та їх впливу на результати діяльності підприємства).*

57. Капелюшна Т. В., Мізецький М. М. Підхід до забезпечення економічної стійкості у бізнес-процесах підприємства. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали II міжнар. наук.-практ. конф., м. Київ, 11–12 лют. 2021 р. Київ, 2021. С. 28- 31. *(0,13 д.а., авторський внесок 0,1 д.а. полягає у дослідженні підходів до забезпечення економічної стійкості підприємств як гарантій безпеки функціонування підприємства та його розвитку).*

58. Капелюшна Т. В., Ткаченко І. С. Private label як дієвий захід формування товарного асортименту. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали II міжнар. наук.-практ. конф., м. Київ, 11–12 лют. 2021 р. Київ, 2021. С. 189-193. *(0,17 д.а, авторський внесок 0,13 д.а. полягає у формуванні власної товарної марки для гарантування й забезпечення інтересів споживачів).*

59. Капелюшна Т. В. Податкові новації в умовах сьогоднішньої невизначеності. *Модернізація економіки: сучасні реалії, прогнозні сценарії та перспективи розвитку* : матеріали II міжнар. наук.-практ. конф., м. Херсон, 28 квіт. 2020 р. Херсон, 2020. С.701-703 *(0,12 д.а.).*

60. Капелюшна Т. В., Лисогор М. Л., Купрієнко Є. О. Фінансовий механізм забезпечення розвитку та конкурентоспроможності торговельного підприємства. *Підприємницька, торговельна, біржова діяльність: тенденції,*

проблеми та перспективи розвитку : матеріали І міжнар. наук.-практ. конф., м. Київ, 11 лют. 2020 р. Київ, 2020. С. 32-35. *(0,13 д.а., авторський внесок 0,1 д.а. полягає у дослідженні дієвих механізмів забезпечення розвитку та конкурентоспроможності підприємств).*

61. Капелюшна Т. В., Татаринський Г. О. Фіскальні інструменти як стимул для розвитку підприємств. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку* : матеріали І міжнар. наук.-практ. конф., м. Київ, 11 лют. 2020 р. Київ, 2020. С. 35-36. *(0,08 д.а., авторський внесок 0,06 д.а. полягає у дослідженні стимулювання розвитку підприємства за рахунок фіскальних інструментів).*

62. Капелюшна Т. В. Проблеми та перспективи розвитку фондового ринку України. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку*: матеріали І міжнар. наук.-практ. конф., м. Київ, 11 лют. 2020 р. Київ : ДУТ, 2020. С. 220-223. *(0,15 д.а., авторський внесок 0,13 д.а. полягає у розгляді проблемних питань для компаній з управління активами на організованих ринках капіталу).*

63. Капелюшна Т. В. Практична підготовка фахівців з використанням програмних продуктів для автоматизації бізнесу в процесі навчання. *Нові інформаційні технології управління бізнесом* : матеріали ІІІ всеукр. наук.-практ. конф., м. Київ, 12 лют. 2020 р. Київ, 2020. С. 85-86. *(0,09 д.а.).*

64. Капелюшна Т. В. Роль технологій у розбудові фондового ринку. *Телекомунікаційний простір XXI сторіччя: ринок, держава, бізнес* : матеріали І міжнар. наук.-прак. конф., м. Київ, 18-19 груд. 2019 р. Київ, 2019. С. 33-38. *(0,2 д.а.).*

65. Капелюшна Т. В. Концепція міжнародного управління в сучасних умовах. *Сучасні тенденції розвитку світової економіки* : зб. тез доп. Х міжн. наук.-практ. конф., м. Харків, 18 трав. 2018 р. Харків, 2018. С. 130. *(0,09 д.а.).*

66. Капелюшна Т. В. Аналіз державного боргу та оцінка механізму його управлінням. *Сучасні тенденції розвитку світової економіки* : зб. тез доп. ІХ

міжн. наук.-практ. конф., м. Харків, 26 трав. 2017 р. Харків, 2017. С. 73. *(0,09 д.а.)*

67. Капелюшна Т. В. Оцінювання динаміки рівня сталості розвитку підприємств. *Актуальні проблеми управління та економічного розвитку в умовах інформатизації суспільства*: матеріали наук.-практ. конф., м. Київ, 20 груд. 2016 р. Київ, 2016. С. 48-49. *(0,1 д.а.).*