МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

КАПЕЛЮШНА ТЕТЯНА ВІКТОРІВНА

УДК 330.34:004.89:005.4:621.39(043.3)

УПРАВЛІННЯ БЕЗПЕКОЮ ПІДПРИЄМСТВ: ТЕОРІЯ ТА МЕТОДОЛОГІЯ

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

РЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора економічних наук

Київ – 2024

Дисертацією є рукопис.

Роботу виконано у Державному університеті інформаційно-комунікаційних технологій Міністерства освіти і науки України, м. Київ.

Науковий консультант: доктор економічних наук, професор
Легомінова Світлана Володимирівна,
завідувач кафедри управління інформаційною та кібернетичною безпекою,
Державний університет інформаційно-комунікаційних технологій, м. Київ.

Опоненти:

доктор економічних наук, професор
Васильців Тарас Григорович,
ДУ "Інститут регіональних досліджень імені М.І. Долішнього НАН України",
завідувач відділу проблем соціально-гуманітарного розвитку регіонів, м. Львів;

доктор економічних наук, професор
Жадько Костянтин Степанович,
Університет митної справи та фінансів,
завідувач кафедри підприємництва та економіки підприємства, м. Дніпро;

доктор економічних наук, професор
Охріменко Ігор Віталійович,
Київський кооперативний інститут бізнесу і права Київської регіональної спілки споживчої кооперації,
ректор, м. Київ.

Захист відбудеться "06" вересня 2024 р. о 14^{00} годині на засіданні спеціалізованої вченої ради Д 26.861.03 у Державному університеті інформаційно-комунікаційних технологій Міністерства освіти і науки України за адресою: 03110, м. Київ, вул. Солом'янська, 7, конференц-зала.

З дисертацією можна ознайомитись на офіційному сайті https: //duikt.edu.ua/ua/1537-arhiv-disertaciy-diyalnist-specializovanoi-vchenoi-radi-d-2686103 та у бібліотеці Державного університету інформаційно-комунікаційних технологій Міністерства освіти і науки України за адресою: 03110, м. Київ, вул. Солом'янська, 7.

Учений секретар
спеціалізованої вченої ради Д 26.861.03 Ольга РОМАЩЕНКО

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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 потенціальної спроможності його розвитку за умови відсутності небезпек (викликів, ризиків, загроз), а у разі їх появи – захищеності, що гарантує досягнення цільових безпекових 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 такими проявами, 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 безпекові 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 і 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 із 418 найменувань, 4 додатків. Загальний обсяг роботи – 485 сторінок комп'ютерного тексту, з них 365 сторінок основного тексту, містить 111 рисунків, 46 таблиць (10 сторінок – рисунки і таблиці, які повністю займають площу сторінки).

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЙНОЇ РОБОТИ

У **вступі** обґрунтовано вибір теми дисертаційної роботи, сформульовано мету відповідно до предмета та об'єкта дослідження, методологічні засади, методи дослідження, відображено наукову новизну та практичне значення отриманих результатів, наведено відомості про особистий внесок здобувача та апробацію основних положень.

У першому розділі **"Теоретичні засади управління безпекою підприємства"** розглянуто термінологічний базис в управлінні безпекою підприємства; проаналізовано понятійно-категоріальну площину елементів управління безпекою підприємства; визначено складові безпеки підприємства та множину чинників впливу на безпеку підприємства.

Досліджено сутність поняття "безпека" та особливостей управління безпекою підприємства за змістовною, об'єктною, територіальною архітектурою небезпеки й вимірністю вразливості підприємства під дією ризиків та загроз, що дозволило вибудувати послідовність станів безпеки із рухом уздовж ланцюга "виклик – ризик – загроза" й дало змогу охарактеризувати економічну безпеку підприємства як складну комбіновану цілісність із взаємопов'язаних між собою підсистем, окремих елементів, які існують окремо, але формують єдине ціле, а також представити критеріальні параметри вимог безпеки підприємства (рис. 1). Розвинутий у дисертаційній роботі понятійно-категоріальний апарат дефініцій "безпека", "безпека підприємства" став базисом теоретичного обґрунтування розуміння 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.

Відзначено, що у конкурентному середовищі безпека підприємства пов'язана з інтересами стейкхолдерів, при чому об'єктом економічних інтересів для власників та інвесторів виступають результати діяльності підприємства (доходи, прибуток), для споживачів, у частині задоволення їх потреб, – результати операційної діяльності у вигляді наданої послуги.

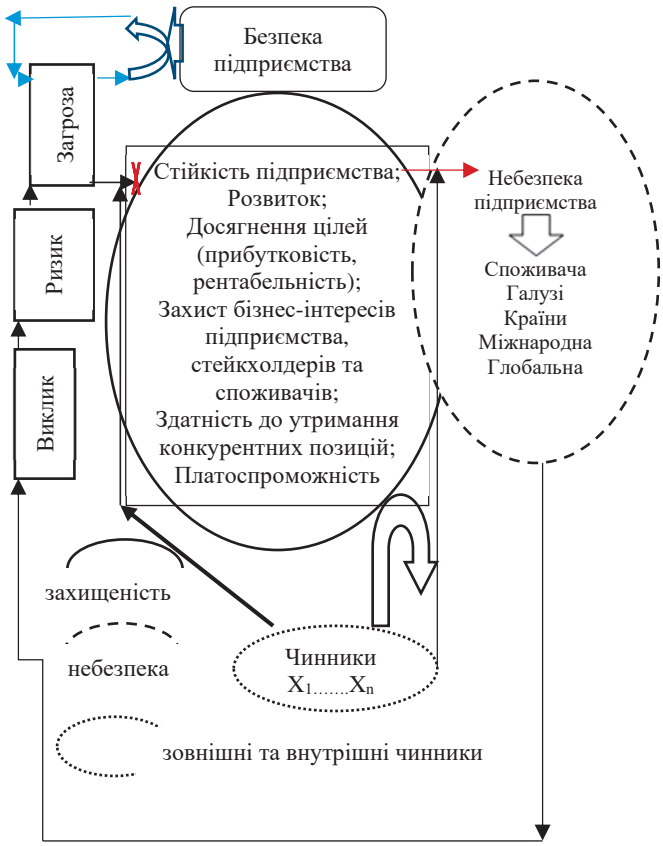


Рис. 1. Критеріальні параметри вимог безпеки підприємства
(авторська розробка)

Рис. 2. Концепт цільових безпекових орієнтирів підприємства
(авторська розробка)

Дослідження ґенези поняття “безпека”, аналіз праць науковців щодо визначення понять “безпека підприємства” слугували підґрунтям для побудови концепту цільових безпекових орієнтирів підприємства (рис. 2), які є базовими для безпеки підприємства з економічної точки зору та з огляду мети створення підприємства (забезпечення прибутку), на яких фокусується проблематика дослідження управління безпекою підприємств. Цільовими безпековими орієнтирами визначено: здатність до розвитку; стійкість, конкуренто-спроможність; платоспроможність; прибутковість та рентабельність; врахування інтересів стейкхолдерів у взаємозв’язку з ризиками і загрозами в умовах викликів сьогодення. Запропоноване розмежування ризиків та загроз слугувало базисом для подальшого розвитку в частині диференціації безпекової площини управління підприємством за рівнями безпеки та небезпеки у відповідності до ймовірності появи ризиків та реальної дії загроз, як окремих елементів впливу на цільові орієнтири, за якої традиційно визначені стани безпеки пропонується доповнити станами небезпеки в залежності від перебування підприємства на конкретній небезпечній ділянці за зональною градацією (передкризовий стан небезпеки; кризовий стан небезпеки; критичний стан).

У другому розділі **“Наукова еволюція поглядів щодо управління безпекою підприємства”** розглянуто ризики та загрози як рушії небезпеки в управлінні підприємством у визначеному та невизначеному середовищі; проаналізовано трансформаційні зміни управління безпекою підприємств в умовах невизначеності та втрати прогностичності; розглянуто еволюцію поглядів щодо управління безпекою підприємств, обумовленою змінами підходів до виробництва.

Відзначено, що окрім спроможності підприємства чинити опір чинникам, явищам, подіям без суттєвих втрат та відхилень від запланованих результатів, так званої “толерантності” до ризику управління безпекою підприємств, прийняття рішень залежить від рівня поінформованості щодо стану безпеки, який нині значиться як низький через невизначені умови функціонування суб’єктів господарювання (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). З’ясовано, що ризик існує завжди, починаючи з генерування підприємницької ідеї, є вимірним, передбачає прийняття рішення із множини варіантів, за попередньо відомою ймовірністю отриманого результату, чого неможливо досягти за невизначених умов, в яких існує поліваріантність прийняття рішень внаслідок дії певних процесів, явищ, чинників з невідомою ймовірністю їх настання.

У результаті досліджень доведено доцільність введення поняття резистентності, яким описується протидія ризикам та загрозам, невизначеностям, викликам в оточенні підприємства (резистентність (стійкість, несприйняття, здатність чинити опір) підприємства, яка знижується у міру невизначеності середовища) з фрагментацією виразності розгалуження ризиків та загроз у безпековій площині за визначеного та невизначеного середовища функціонування підприємства (рис. 3).

Доведено, що за неспроможності підприємством усувати ризики резистентність знижується, гіпотетичний ризик переходить у реальні загрози, які безпосередньо чинять деструктивний вплив на результати діяльності підприємства. Зміни негативного характеру, що наражають підприємство на небезпеку, можуть призвести до його ліквідації, актуалізується питання безпекозабезпечувальної діяльності підприємства та розгляду прийнятних заходів безпеки із захисту активів задля протидії негативним змінам і повернення спроможності підприємством провадити свою операційну діяльність, відновлення функціонування. Зазначено, що чіткість окреслення викликів, ризиків та загроз, розуміння їх природи, класифікація та характеристика сприяє більш точному та адекватному реагуванню на них, розробці, як оперативних, так і превентивних заходів управління безпекою підприємства із встановлення резистентності підприємства за визначених та невизначених умов функціонування. Аналітично доведено вплив промислових революцій на стрімкість розвитку технологій: впродовж останніх 40 років індустрію 3.0 змінила 4.0, що враховує невизначеності, стейкхолдер-орієнтованість, динамічне ситуативне управління безпекою.

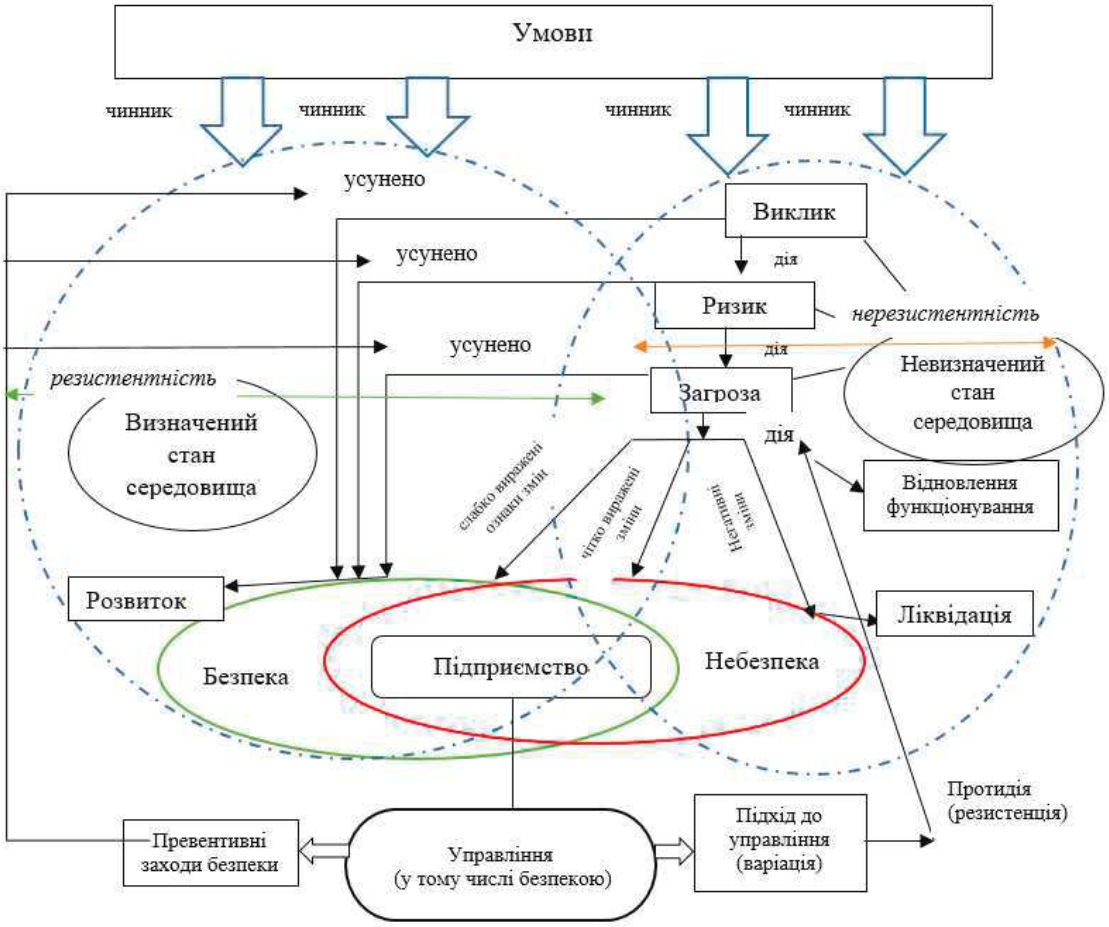


Рис. 3. Фрагментація виразності розгалуження ризиків та загроз у безпековій площині за визначеного та невизначеного середовища функціонування підприємства *(авторська розробка)*

Відмічено передумови розгортання квантових технологій, наголошено, що квантова епоха зумовлює захист екосистеми, керованої квантовими технологіями, безпеку Великих даних, квантових обчислень та квантових комунікацій на підприємствах, що засвідчує та обґрунтовує динамічно-ситуативну спрямованість управління безпекою підприємства.

У третьому розділі **“Методологічні засади управління безпекою підприємств”** сформовано науково-онтологічний базис методології управління безпекою підприємств, запропоновано концепт траєкторії площин станів безпеки підприємства, розроблено методологію управління безпекою підприємств.

Методологічне забезпечення дослідження проблематики управління безпекою підприємств включає онтологічний базис, тобто понятійно-категоріальний апарат навколо безпекового об’єкта дослідження, та гносеологічній – пошук та виокремлення зв’язків у структурі категорій з описом та аналізом існуючих методів оцінки та управління безпекою підприємства. Зазначено, що процес управління безпекою підприємства доволі складний, методологія збагачується з урахуванням нових поглядів, знань, умов, розвитку суспільства та трансформаційних змін. Доведено, що управління є комплементарним поняттям, що поєднує складові елементи, функціональні цеглини, оточення, загрози та невизначеності, формуючи вміст площини безпеки

– цільові безпекові орієнтири підприємства, що підлягають захисту, на яких зосереджене управління безпекою підприємства.

Ґрунтовний аналіз теоретичних напрацювань дозволив окреслити площину безпеки (стійкість, платоспроможність, прибутковість й рентабельність, розвиток, конкурентоспроможність, гармонізація інтересів стейкхолдерів), які розглядатимуться як результати безпеки та забезпечуватимуться у процесі управління, що дозволило сформувати науково-онтологічний базис методології управління безпекою підприємства (рис. 4).

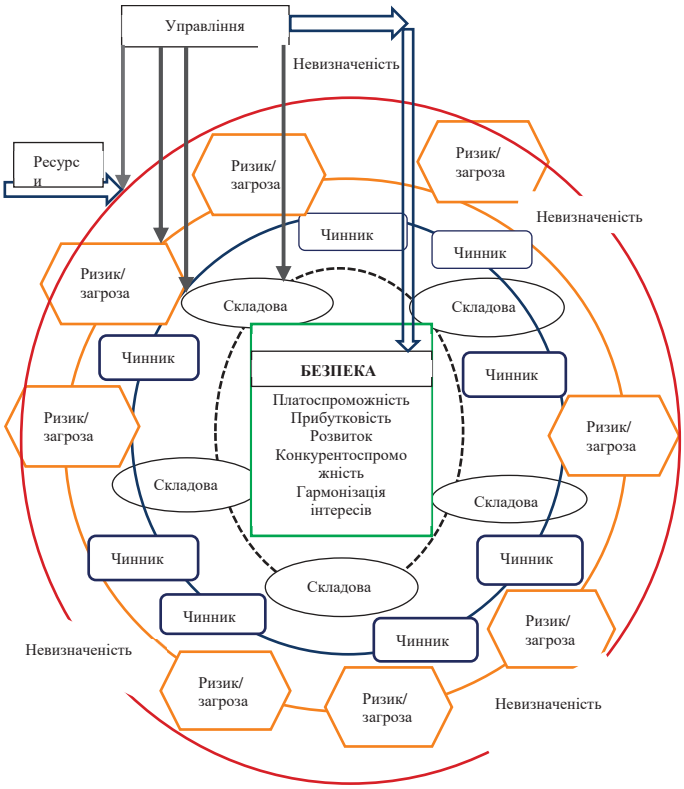
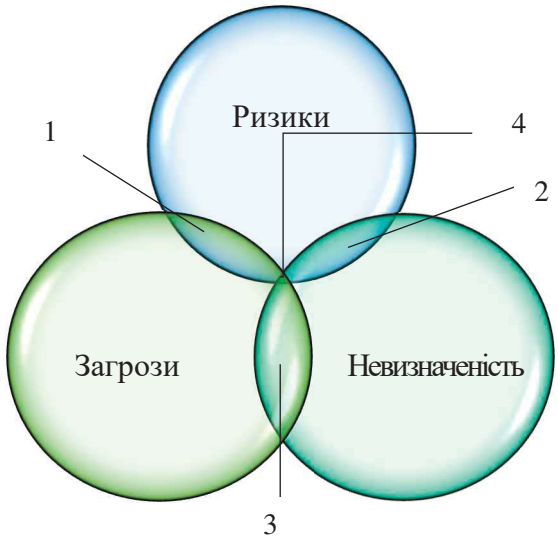


Рис. 4. Науково-онтологічний базис методології управління безпекою підприємства *(авторська розробка)*



1, 2, 3, 4 – перетин "ризиків – загроз – невизначеностей"

Рис. 5. Синергетизм турбулентності середовища на перетині "ризиків – загроз – невизначеностей" *(авторська розробка)*

Відзначено, що мінливість та непередбачуваність середовища окреслює такі елементи в площині безпеки, як: невизначеність, виклики, загрози, які сукупно посилюють дію один одного, синергетично поєднуючись, здійснюють потужніший вплив на безпеку підприємств, змінюючи стан безпеки підприємства в залежності від зони перебування на перетині "ризик-загроза-невизначеність" (рис. 5): перетин 1 (ризик і загроза), перетин 2 (ризик і невизначеність), перетин 3 (загроза та невизначеність), перетин 4 (загроза, ризик, невизначеність). Результатом дослідження підходів до управління є фокус зосередження уваги на адаптації традиційних управлінських підходів до умов невизначеності, аргументація їх взаємної інтегрованості, зв'язку із об'єктом управління (рис. 6).

За результатом онтологічного дослідження та окреслених цільових результатів безпеки запропоновано концепт траєкторії площин станів безпеки підприємств, яким передбачається тривекторне управління безпекою підприємства, що включає: ресурсно-діяльнісну спрямованість – захист складових безпеки;

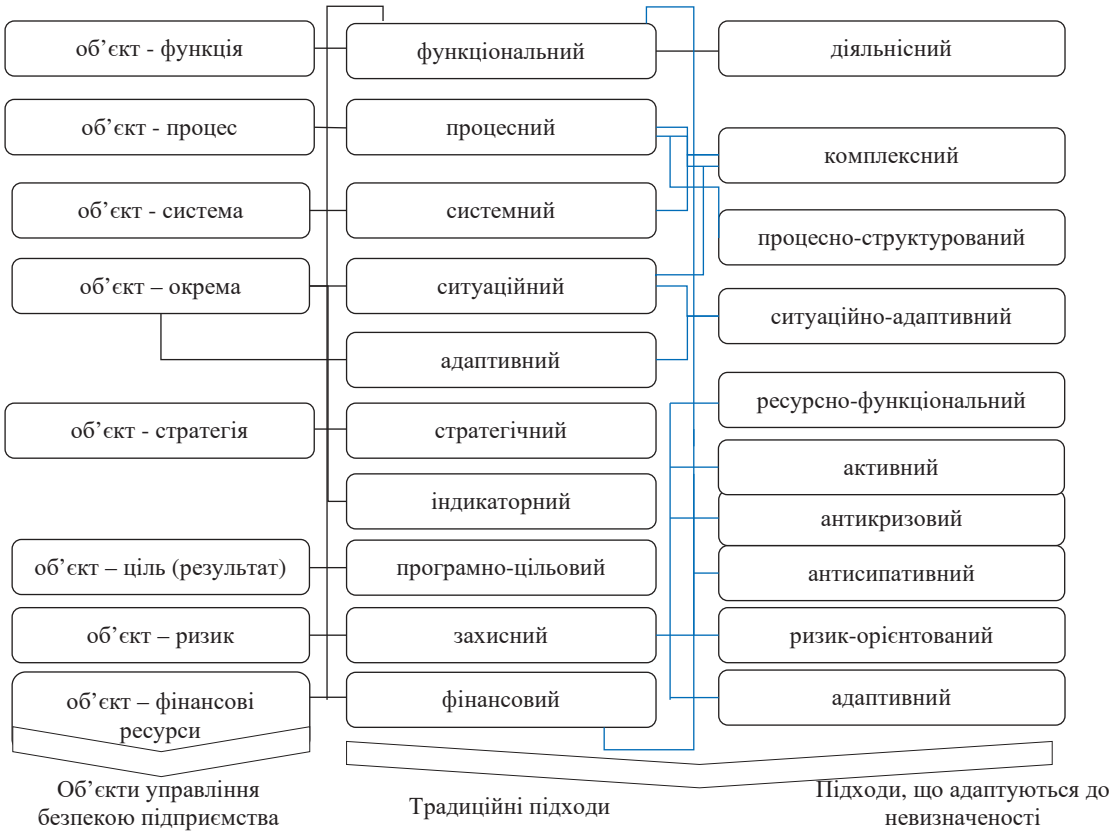


Рис. 6. Адаптація традиційних підходів до управління безпекою підприємства за невизначених умов *(авторська розробка)*

гармонізаційну направленість – захист інтересів стейкхолдерів; захисну направленість від умов функціонування – уникнення, усунення, запобігання (або інші варіанти) ризиків, загроз, невизначеностей. Осередком безпекової площини є цільові результати безпеки, що підлягають управлінню, визначаються метриками, які в залежності від зміни їх параметрів перебувають у діапазоні ризику (із фіксацією репелерної точки) та переходом у діапазон загрози (у біфуркаційній точці) (рис. 7).

Аргументовано, що рівні гармонізації інтересів внутрішнього та зовнішнього оточення доцільно визначати за рівнем гармонізації інтересів (рис. 8): 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%).

На основі проведених досліджень запропоновано визначати репелерні та біфуркаційні точки, які, відповідно, ідентифікуватимуть ризики та загрози, стійкість підприємства до умов функціонування, а також сформовано композитарний зв'язок між складовими безпеки, метриками безпеки та цільовими безпековими результатами, сформовано мережеву складову ємність цільових результатів управління.

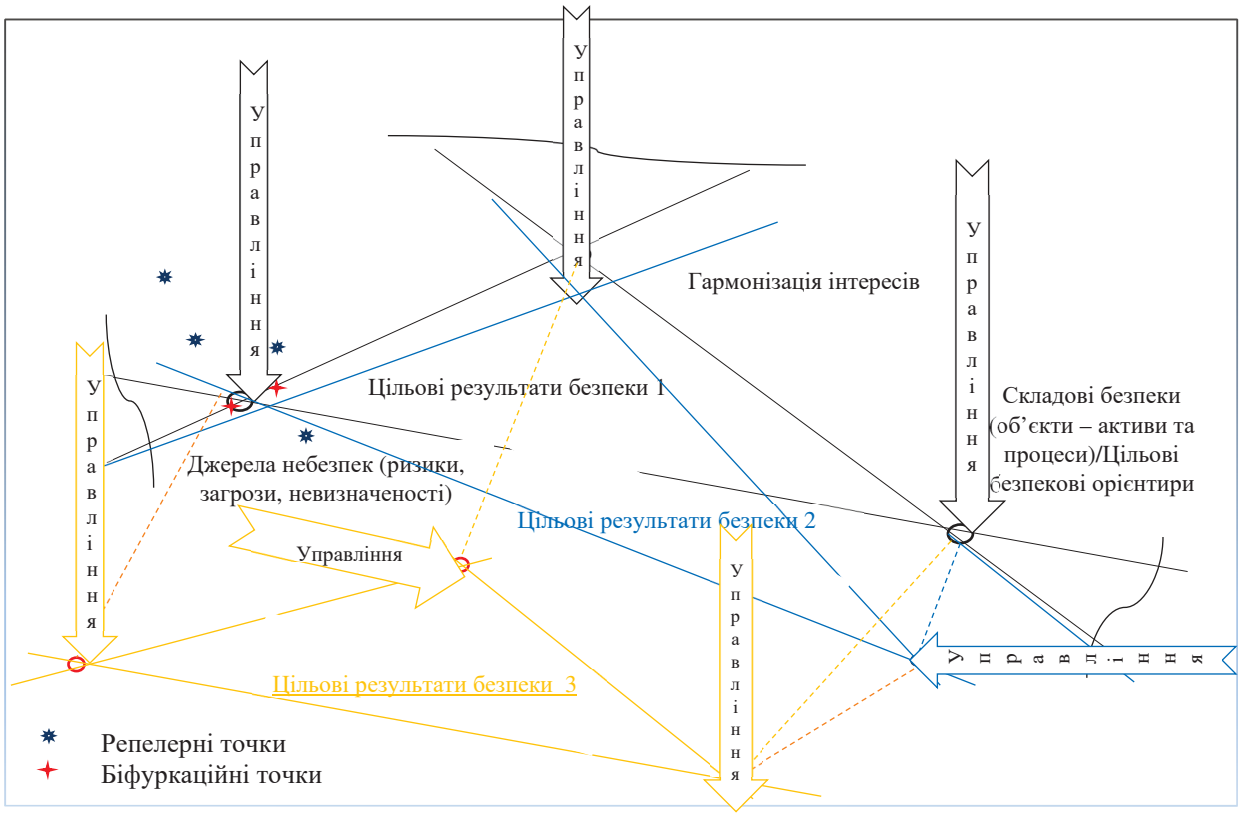


Рис. 7. Концепт траєкторії площин станів безпеки під дією тривекторного синергетичного управління (гармонізація інтересів – захист від небезпек – захист складових) *(авторська розробка)*

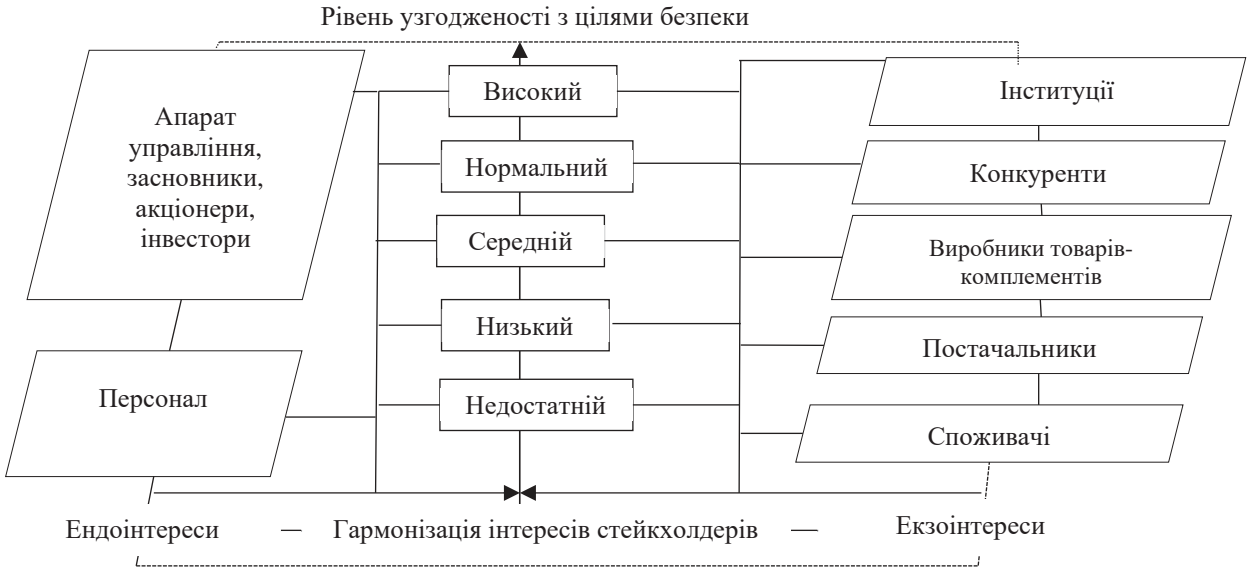


Рис. 8. Вертикалі гармонізації екзо- та ендоінтересів стейкхолдерів підприємств ПЕКМП *(авторська розробка)*

Узагальнення результатів дослідження теоретичних та методологічних засад управління безпекою підприємства слугували базисом для обґрунтування формування теоретико-методологічної концепції управління безпекою підприємств за умов невизначеності (рис. 9), а також формування теоретико-методологічної компонентної площини управління безпекою підприємств (рис. 10).

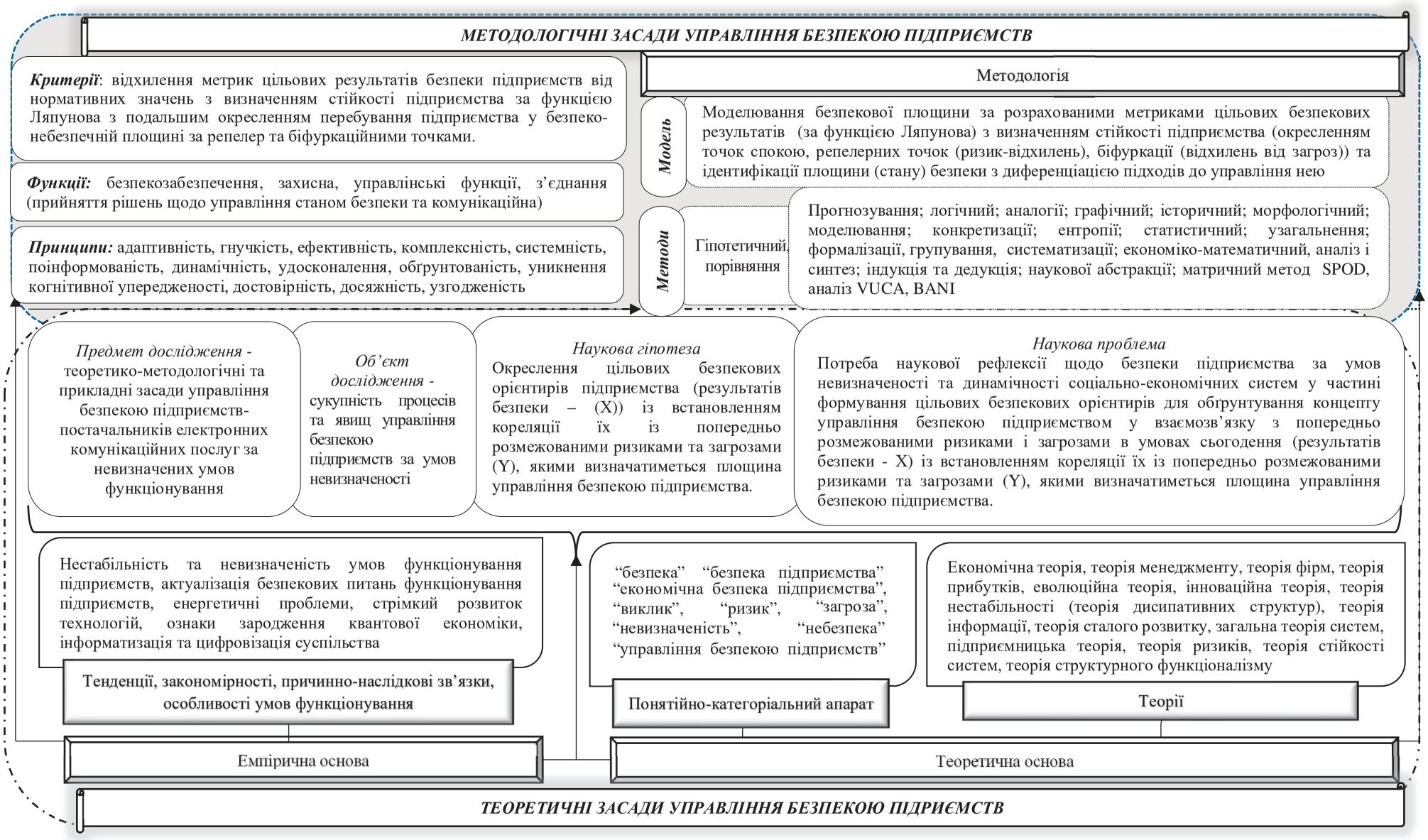


Рис. 9. Теоретико-методологічна концепція управління безпекою підприємств за умов невизначеності *(авторська розробка)*

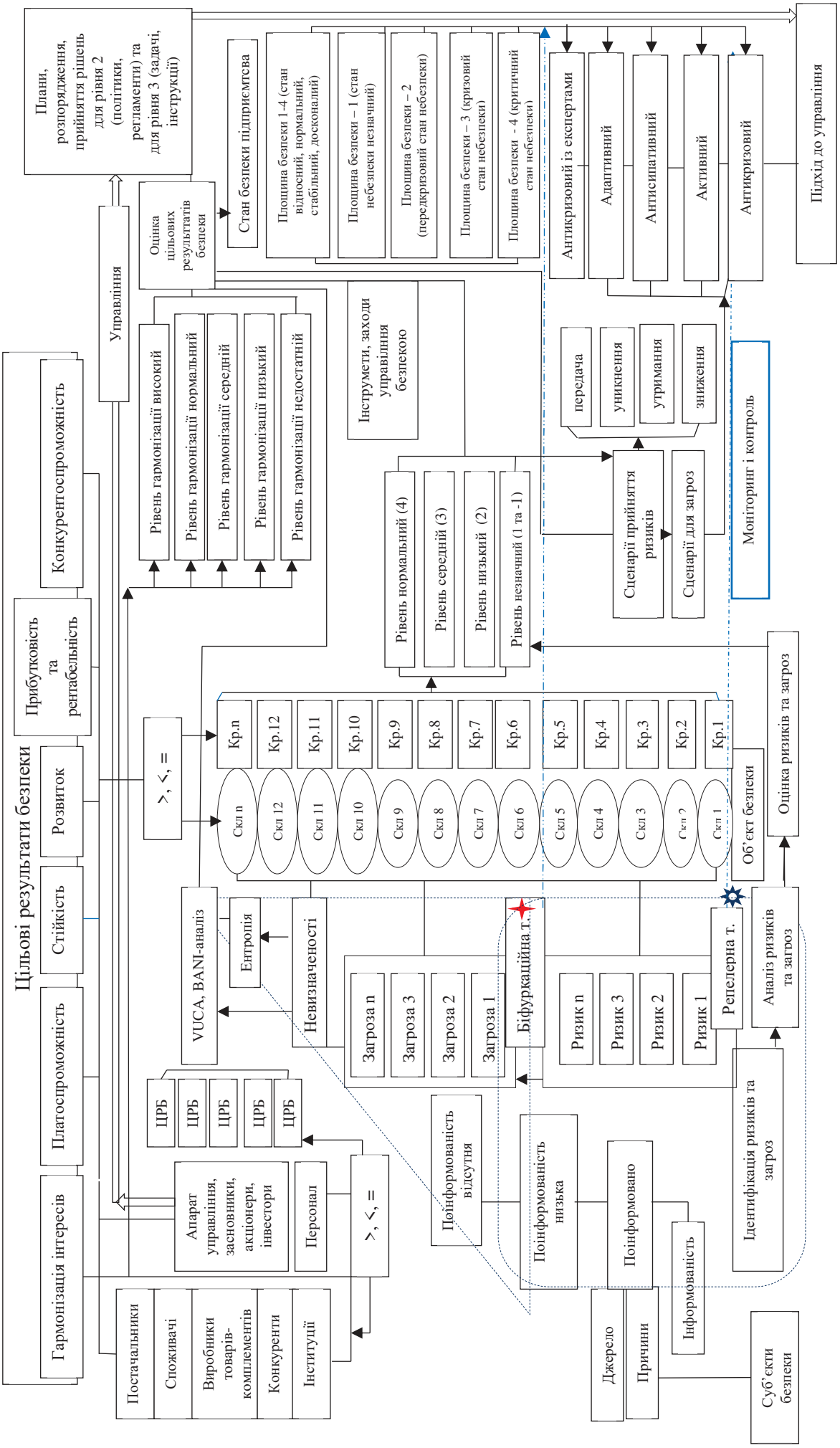


Рис. 10. Теоретико-методологічна компонентна площина управління безпекою підприємств *(авторська розробка)*

У четвертому розділі **“Аналіз середовища функціонування та оцінка стану безпеки підприємств-постачальників електронних комунікаційних послуг”** проаналізовано стан ринку постачання електронних комунікаційних мереж та послуг; проведено моніторинг безпекової площини українських підприємств-постачальників електронних комунікаційних послуг; сконструйовано модель управління безпекою підприємств-постачальників електронних комунікаційних послуг.

Проведений аналіз стану ринку постачання електронних комунікаційних мереж та послуг, дозволив відмітити сприяння функціонуванню підприємств через спрощення реєстрації постачальників даних послуг для розбудови конкурентного ринку електронних комунікаційних мереж та послуг (зростання кількості зареєстрованих суб’єктів-постачальників електронних комунікаційних послуг з 2036 (2022 р.) до 4113 (2023 р.)), а також зростання доходів від електронних комунікаційних послуг із 83,2 до 97,3 млрд грн за рахунок: фіксованого доступу до мережі Інтернет – 21,2 млрд грн у 2023 році (темп росту склав 133,1 % по відношенню до обсягів доходів у 2022 році); послуг 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) (рис. 11).

Рис. 11. Динаміка та структура доходів від надання електронних комунікаційних послуг (за видами) впродовж 2021-2023 рр., млрд грн *(складено автором)*

Встановлено, що найбільш затребуваною споживачами електронних послуг залишається послуга Інтернет, завдяки якій бізнес та населення спроможні залишатися на зв'язку, функціонувати за умов невизначеності. Частки постачальників на ринку надання електронних комунікаційних послуг за обсягами доходів у 2023 р. вказують на домінування на ринку компаній: ПрАТ "Київстар", ПрАТ "ВФ Україна", ТОВ "Лайфселл" (рис. 12).

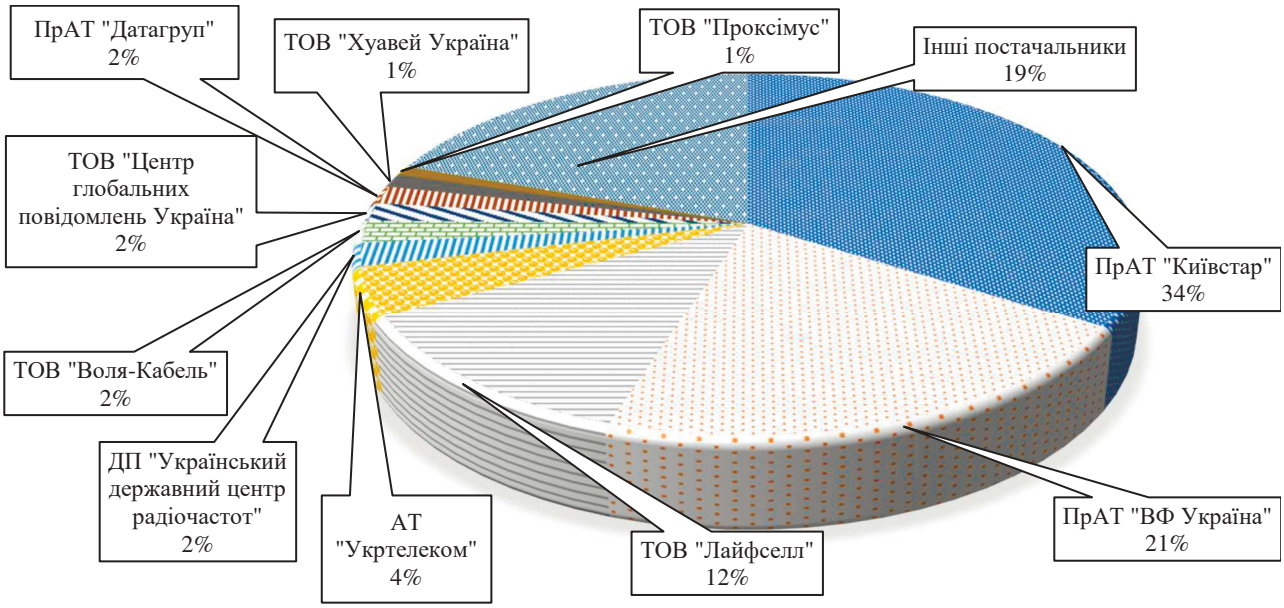


Рис. 12. Структура ринку постачальників електронних комунікаційних послуг за обсягами доходів у 2023 р. *(складено автором)*

Аналіз стану ринку електронних комунікаційних послуг дозволив виявити позитивну динаміку, оскільки загальні доходи у 2023 році зросли на 17% та склали 97,3 млрд грн, що пов'язано із приростом за рахунок: доступу до фіксованої мережі Інтернет (обсяг доходів – 21,2 млрд грн, приріст доходів на 33% по відношенню до 2022 року); 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 у 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 причин руйнувань інфраструктури мережі та довготривалості відновлення ліній зв'язку, які надаються за аналоговими технологіями. Відмічено вагу енергоефективних технологій, зростання попиту на технології PON на 17,7% у порівнянні з 2022 роком через спроможність користування послугою Інтернет у разі відсутності енергопостачання, а також інтеграцією національної енергосистеми з

європейською мережею операторів системи передачі електроенергії (European Network of Transmission System Operators for Electricity).

За результатами проведеного моніторингу безпекової площини українських підприємств-постачальників електронних комунікаційних послуг, за розрахованими на основі фінансово-економічних показників, метриками було визначено цільові результати безпеки ПрАТ "Київстар", ПрАТ "ВФ Україна", ТОВ "Лайфселл", АТ "Укртелеком", ПрАТ "Датагруп".

Запропонована методика розмежування ризиків та загроз, дозволила з'ясувати, 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 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.

Змодельовано управління безпекою підприємств-постачальників електронних комунікаційних послуг з розмежуванням ризиків та загроз і визначенням точок репелер та біфуркації у безпековій площині, через відхилення від нормативних значень, що призводить до зміни станів безпеки, характер стійкості точок описано диференціальним рівнянням:

$$\frac{dx_i}{dt} = f_i(t, x_1, x_2, \dots\dots, x_n), \text{ i = 1, 2, ……., n,} \qquad (1)$$

де $f_i(t, x_1, x_2, \dots\dots, x_n)$ – функція Ляпунова, яка обирається без попереднього знаходження рішень системи;

$x_1, x_2, \dots\dots, x_n$ – метрики безпеки за цільовими результатами безпеки.

Модель апробовано на українських підприємствах-постачальниках електронних комунікаційних мереж та послуг, представлено результати, за якими змодельовано стійкість за цільовими результатами безпеки (рис. 13), визначено безпекові площини й, відповідно, стан безпеки чи небезпеки підприємств (за визначеними безпековими відхиленнями у безпеко-небезпечній площині дотичності репелерних точок впливу ризиків і біфуркаційних точок дії загроз) (табл. 1).

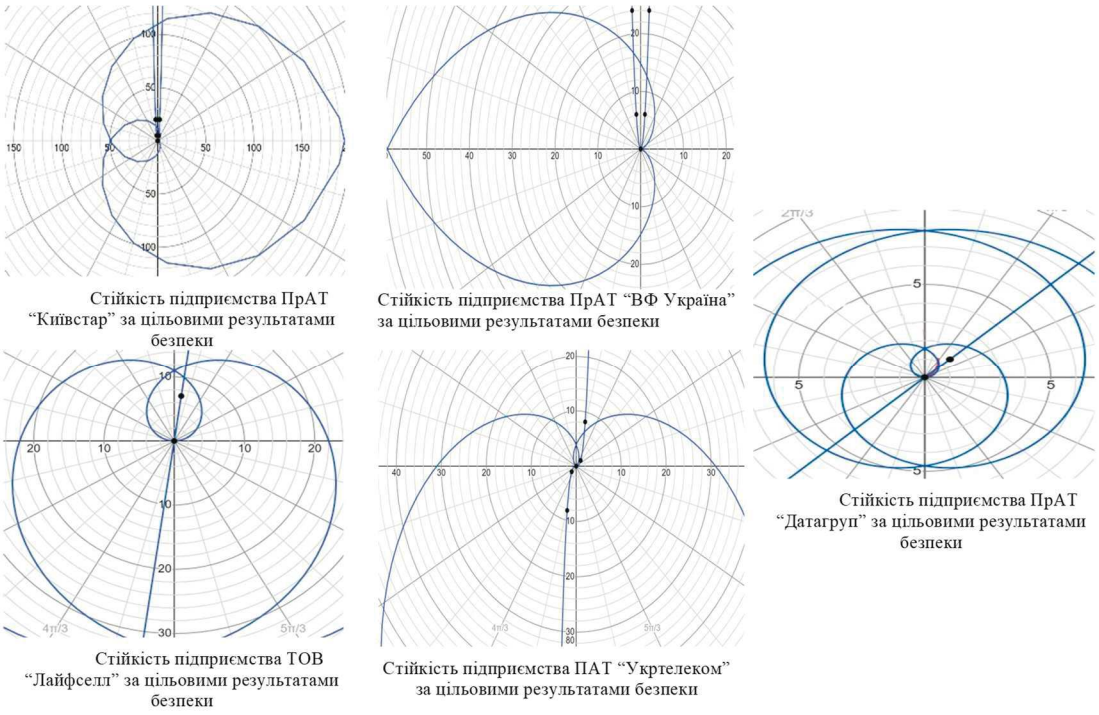


Рис. 13. Моделювання стійкості функціонування українських підприємств ПЕКМП за цільовими результатами безпеки *(авторська розробка)*

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

Таблиця 1

Ідентифікація безпекової площини (стан безпеки/небезпеки) українських підприємств-постачальників електронних комунікацій за цільовими безпековими орієнтирами *(авторська розробка)*

Підприємство-постачальник електронних комунікаційних послуг	Цільові безпекові орієнтири					Рівень ризику/ загрози	Стан безпеки/ небезпеки
	Прибутковість	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)
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

Доведено, що змодельовані відхилення площин безпеки дозволяють диференціювати підходи до управління безпекою підприємства з урахуванням втрат (відхилень) від цільових метрик безпеки (результатів) (рис. 14).

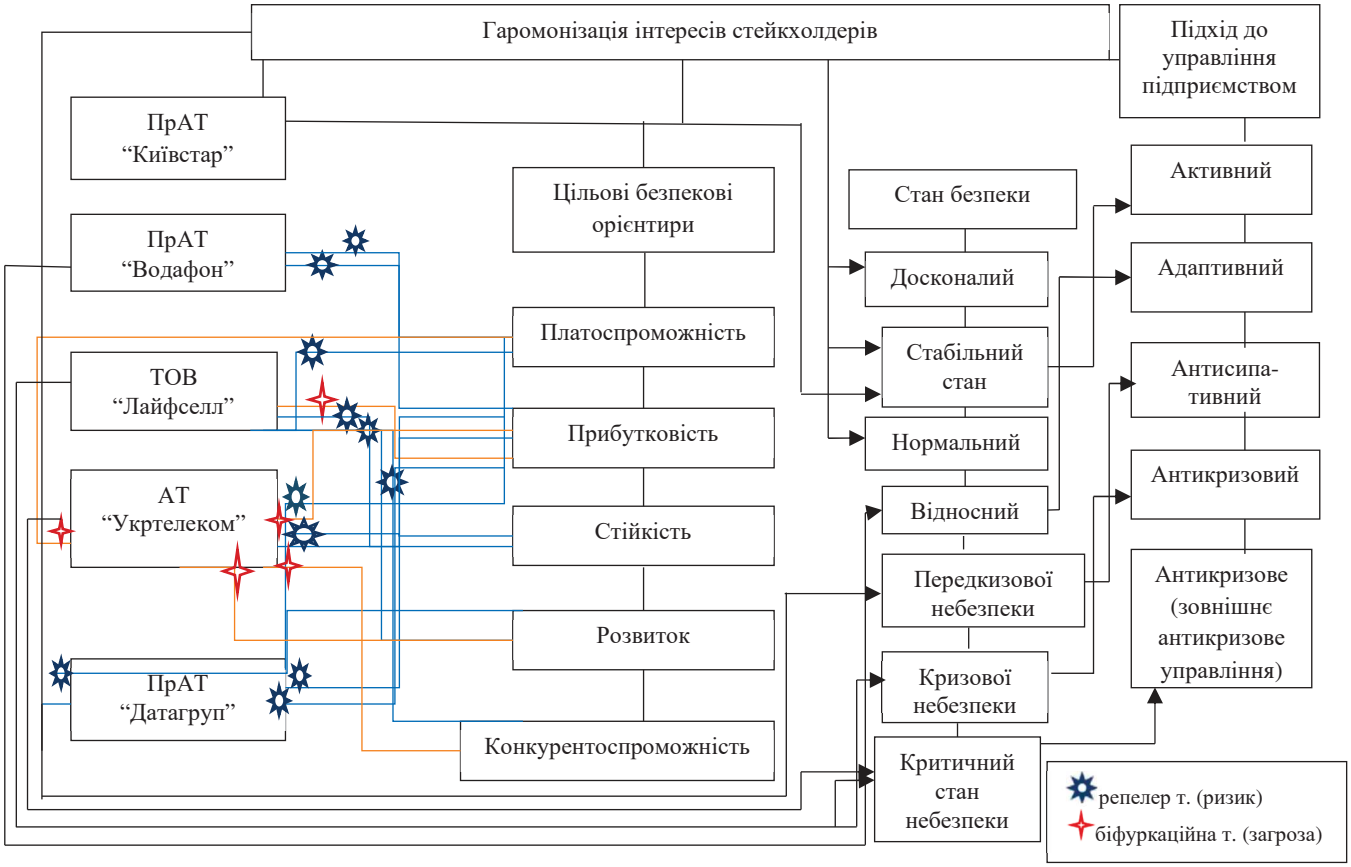


Рис. 14. Управління безпекою підприємств ПЕКМП за результатами оцінки цільових безпекових орієнтирів *(авторська розробка)*

У п'ятому розділі **"Управління безпекою підприємства за умов невизначеності"** проаналізовано та узагальнено виклики управління безпекою підприємства; проведено науково-параметричну діагностику безпеки підприємств за умов невизначеності; запропоновано стратегічні напрями розвитку підприємств, як підґрунтя для управління безпекою підприємства у повоєнний час.

Аналіз глобальних викликів щодо управління безпекою підприємства за невизначених умов дозволив їх структурувати та ранжувати за шкалою небезпечності та загрозливості до функціонування підприємств. Основними викликами визначено: кліматичні зміни (екстремальні погодні явища, посухи, пожежі, втрата біорізноманіття, процеси руйнації екології); стрімкий зростаючий ризик використання штучного інтелекту та Великих даних, активізація використання хмарних технологій та сервісів, які надають позитивні можливості, так, і спричиняють появу негативних наслідків їх використання в сенсі створення можливості втрати конфіденційної інформації підприємства (кіберризик), що підтверджено зростанням кількості кіберінцидентів, спрямованих на порушення безпеки підприємства; геополітична нестабільність (війна, катастрофічні руйнування) (рис. 15).

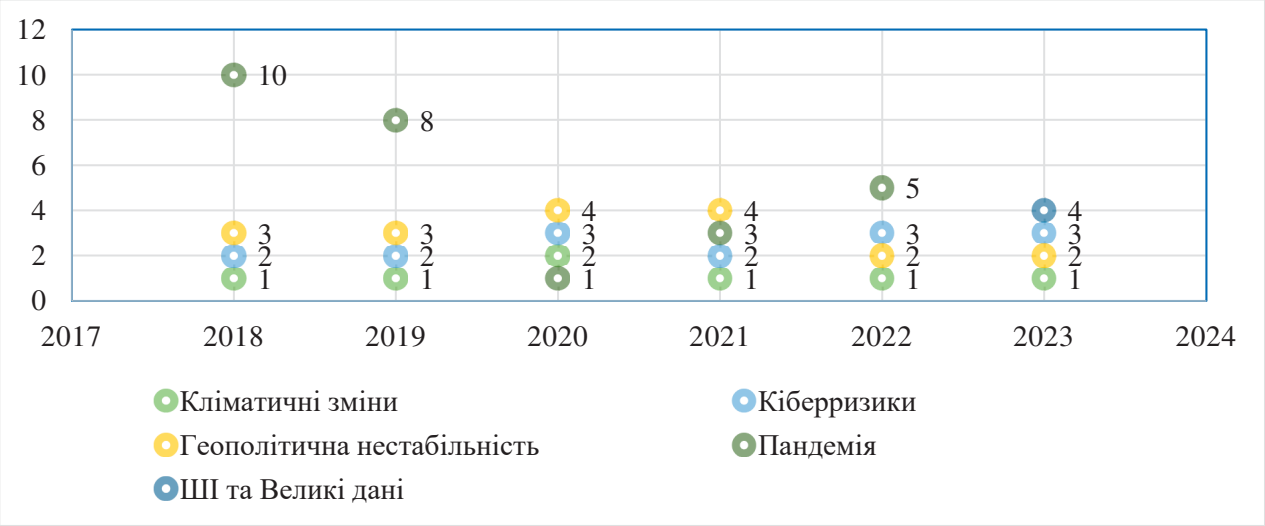


Рис. 15. Ранги глобальних викликів впродовж 2017-2023 рр.
(побудовано автором на основі даних AXA Future Risks Report)

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 (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. 16).

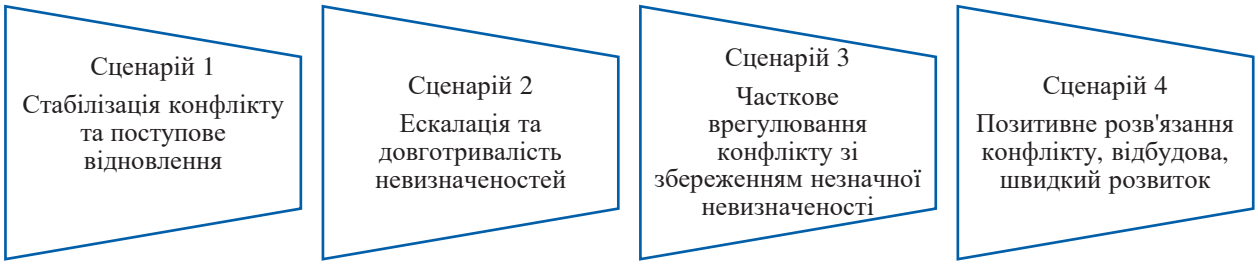


Рис. 16. Сценарії розвитку підприємств сфери електронних комунікацій за невизначених умов функціонування *(авторська розробка)*

Сценарій 1 – стабілізація конфлікту та поступове відновлення, зводиться до наступних аспектів безпекової ситуації й першочергово вказує на потребу в інвестуванні інфокомунікаційної інфраструктури з пріоритезацією відновлення зруйнованої та пошкодженої інфраструктури з використанням новітніх технологій, особливо технологій GPON для підвищення надійності мереж в умовах втрати енергетичних потужностей в енергосистемі країни. Стратегічні партнерства з міжнародними організаціями з метою залучення інвестування, врахування їх регуляторних вимог та відповідність стандартів надання послуг зв’язку.

Сценарій 2 – ескалація та довготривалість невизначеностей, підприємствам-постачальникам електронних комунікацій доцільно 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 адаптивні 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 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 протидія дезінформації щодо роботи підприємства з метою збереження репутації.

Сценарій 4 – позитивне розв'язання конфлікту, відбудова, швидкий розвиток значиться як: прогресивне інвестування в розбудову мережі та переходу на новітні технології надання зв'язку споживачам послуг, модернізація мереж для відповідності вимогам європейського інфокомунікаційного простору; розширення переліку послуг зв'язку, підвищення якості надання послуг для збільшення швидкості передачі даних у роумінгу; залучення іноземних партнерів до проєктів та інноваційних розробок; дотримання принципів сталого розвитку для підтримки концепції розвитку без загрози існуванню майбутнім поколінням, корпоративна відповідальність.

Аналіз викликів сучасності дозволив виділити найсуттєвіші: руйнування та пошкодження інфраструктури; експлуатаційні порушення; загрози кібербезпеці; невизначеність нормативно-правового, інституційного регулювання; а також нестабільність економіки. Запропоновано науково-методичну оцінку викликів, які вимірюються відповідними їм ймовірностями: 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. 17).

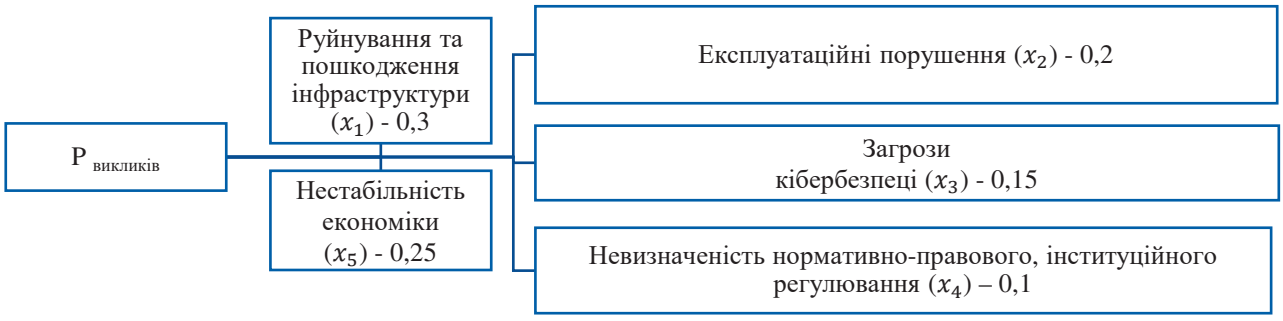


Рис. 17. Ймовірності викликів невизначеності для підприємств-постачальників електронних комунікаційних мереж та послуг *(авторська розробка)*

Проведено науково-параметричну діагностику безпеки підприємства за умов невизначеності шляхом визначення ентропії, що передбачає врахування взаємозв'язку з інформацією щодо оточення підприємства (ймовірностями викликів невизначеності для підприємств-постачальників електронних комунікаційних мереж та послуг):

$$\mathrm{H(X)} = -(p\,(x_1)\log_2 p(x_1) + (p\,(x_2)\log_2 p(x_2) + \ (p\,(x_3)\log_2 p(x_3\,) + \\ + (p\,(x_4)\log_2 p(x_4) + \ (p\,(x_5)\log_2 p(x_5), \qquad (2)$$

де $p(x_i)$ – ймовірність окремого виклику для постачальників електронних комунікаційних мереж та послуг.

Відзначено, що за нормальних умов функціонування, ентропія оцінюється для визначення середовища функціонування підприємств в залежності від приналежності до типу ринкової структури. Ринок електронних комунікацій визначається як конкурентний для постачальників послуг інтернет-зв'язку, однак, в результаті аналізу з'ясовано, що увесь можливий спектр послуг надається трьома основними гравцями: ПрАТ "Київстар", ПрАТ "ВФ Україна", ТОВ "Лайфселл", тобто ринок наближений до олігополістичного, тому ентропія для підприємств, що господарюють за даного типу ринкової структури, коливається в межах до 1,5 біт.

За результатами розрахунків ентропія H(X) викликів сектору електронних комунікацій під час воєнних дій на території України становить приблизно 2,23 біта, що дало змогу стверджувати про значний рівень непередбачуваності та складності в управлінні виявленими викликами.

За результатами проведеної параметричної діагностики безпеки підприємств запропоновано стратегічні напрями подолання викликів для забезпечення цільових безпекових орієнтирів підприємств-постачальників електронних комунікаційних мереж та послуг (рис. 18).

Стратегічні напрями розвитку та відновлення безпечного функціонування підприємств взаємокомбінуються задля забезпечення цільових безпекових орієнтирів підприємств-постачальників електронних комунікаційних мереж та послуг, що націлено на пришвидшення усунення викликів та нейтралізації їх наслідків за рахунок наступних ініціатив:

– відбудови та модернізації інфраструктури (державно-приватного партнерства (співпраці 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);

– операційної ефективності та стійкості (планування безперервності бізнесу шляхом розробки надійних планів безперебійної роботи бізнесу для забезпечення надання послуг під час кризових ситуацій; гнучкість інтелектуального

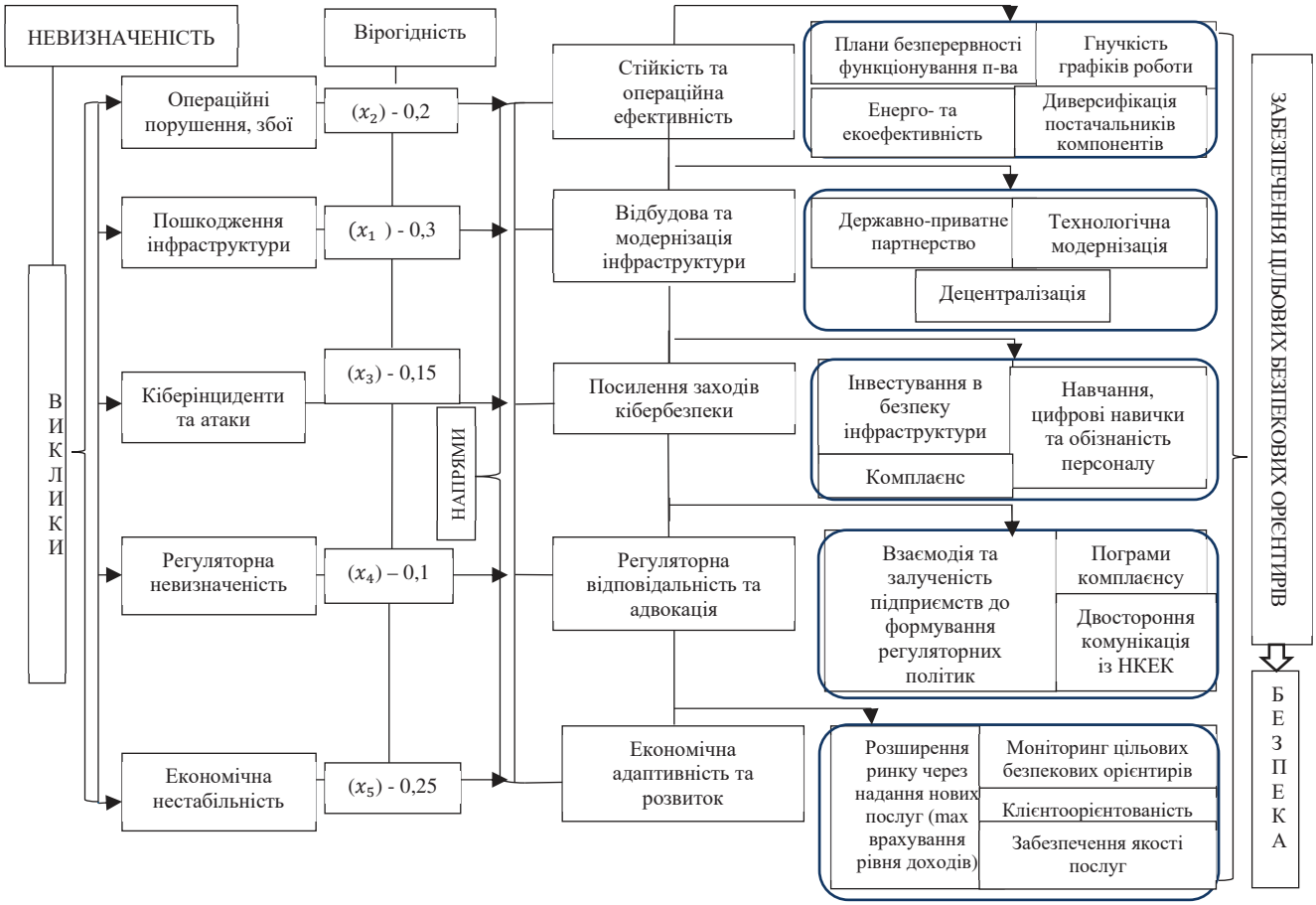


Рис. 18. Стратегічні напрями подолання викликів для забезпечення цільових безпекових орієнтирів підприємств ПЕКМП *(авторська розробка)*

капіталу (персоналу) за впровадження варійованого графіку роботи та можливості віддаленої роботи, щоб підтримувати діяльність під час збоїв; управління ланцюгами постачання за рахунок підвищення стійкості ланцюга постачання через диверсифікацію постачальників та створення планів на випадок непередбачуваних ситуацій для критично важливих компонентів);

– посилення заходів кібербезпеки (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; реагування на кіберінциденти та атаки за рахунок розробки та регулярного оновлення планів реагування на інциденти для оперативного реагування та відновлення після кібератак);

– посилення регуляторної відповідальності та адвокації, що вирішує проблему регуляторної невизначеності (активна взаємодія з регуляторними органами для врахування потенційно можливих змін та участі у розробці сприятливої політики розбудови цифрової економіки та надійної, ефективної інформаційно-комунікаційної інфраструктури підприємств-постачальників електронних комунікаційних мереж; впровадження комплексних програм комплаєнсу для забезпечення дотримання чинного законодавства, нормативно-правового регулювання питань щодо функціонування підприємств сфери

інфокомунікацій; активної участі у програмах та проєктах, формуванні стратегій розвитку сфери ІКТ за рахунок спільної роботи з галузевими асоціаціями, прийнятті рішень для впливу на формування політики та сприяння розвитку регуляторного середовища);

– налагодження економічної адаптивності та зростання, що спрямоване на нівелювання виклику економічної нестабільності (ЕН) – 0,25 (диверсифікація джерел фінансових 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 фінансової стабілізації під час економічних спадів та утримання підприємством цільового рівня платоспроможності; клієнтоорієнтованості, що передбачає розробку цільових (таргетованих послуг) та цінових стратегій для різних сегментів клієнтів, включаючи домогосподарства та підприємства з низьким рівнем доходу).

ВИСНОВКИ

У дисертаційній роботі узагальнено теоретико-методологічні засади та запропоновано нове розв'язання актуальної науково-прикладної проблеми рефлексії щодо управління безпекою підприємства за умов невизначеності.

Розв'язавши поставлені дослідницькі завдання, в результаті наукового пошуку вдалося дійти таких висновків:

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 (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 і 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 передбачає 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 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"; загроза 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" – передкризовий. 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 виклики 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.

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: 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/emb/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 ІІ 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. 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 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).*
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 III 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 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).*
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 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).*

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 I 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 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).*

62. Капелюшна Т. В. Проблеми та перспективи розвитку фондового ринку України. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку*: матеріали I 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 III 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 I 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. X 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. IX 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.).*

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 дисертаційному дослідженні обґрунтовано теоретико-методологічний базис управління безпекою підприємств, розвинуто наукові погляди до його сутності. Запропоновано концепт-методологію, яка ґрунтується на попередньо окресленій площині безпеки, в осередку якої – цільові безпекові результати діяльності підприємства, що визначаються 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 визначатиметься стан безпеки (небезпеки) підприємства й, відповідно, рух в окреслених безпекових площинах, що скеровує до цілеспрямованого використання підходу до управління безпекою підприємства. Побудовано модель за використання методу Ляпунова для окреслення стійкості та рівня (стану) безпеки підприємств, запропоновано диференціацію підходів до управління безпекою підприємств, зважаючи на окреслену безпекову площину з подальшою апробацією моделі на досліджуваних підприємствах ПЕКМП. Проаналізовано та узагальнено виклики, перед якими постали підприємства ПЕКМП, запропоновано чотири сценарії розвитку досліджуваних підприємств, визначено ентропію невизначеності для прогнозування вірогідного отримання прибутку за відповідними сценаріями й запропоновано стратегічні напрями управління

підприємствами в умовах невизначеності, низької прогностичності та емерджентності.

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.

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 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.

Надруковано в РВЦ
Державного університету інформаційно-комунікаційних технологій
Формат 60х90/16. Папір друкарський.
Наклад 100 прим. Зам. 565-е.

Свідоцтво суб’єкта видавничої справи ДК №7917 від 16.08.2023 р.

03110, м. Київ, вул. Солом’янська, 7.
Тел. (044) 249-25-76