

О.Є. Гудзь
А.А. Захаржевська

**РОЗВИТОК УПРАВЛІННЯ РИЗИКАМИ
ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ
В РЕАЛІЯХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ**

Монографія



**О.Є. Гудзь
А.А. Захаржевська**

**РОЗВИТОК УПРАВЛІННЯ РИЗИКАМИ
ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ
В РЕАЛІЯХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ**

Монографія

Кропивницький
Видавець Лисенко В.Ф.
2023

УДК 621.391:004.056(02)
Г 93

*Рекомендовано до друку Вченою радою Державного університету
телекомунікацій (протокол № 16 від 10.05.2023 р.).*

Рецензенти:

Боняр С. М. доктор економічних наук, професор;
Зеліско І. М. доктор економічних наук, професор;
Прокопенко Н. С. доктор економічних наук, професор.

Укладачі:

Гудзь Олена Євгенівна, доктор економічних наук, професор;
Захаржевська Аліна Анатоліївна, кандидат економічних наук.

Гудзь О.Є., Захаржевська А.А.

Г 93 Розвиток управління ризиками телекомунікаційних підприємств
в реаліях цифрової трансформації: монографія. – Кропивницький :
Видавець Лисенко В. Ф., 2023. – 200 с.
ISBN 978-617-7813-80-3

В монографії висвітлено теоретико-методологічні та практичні аспекти розвитку управління ризиками телекомунікаційних підприємств (РУРТП) в реаліях цифрової трансформації, зокрема розкрито сутнісну характеристику РУРТП, встановлено особливості управління ризиками в проектах цифрової трансформації телекомунікаційних підприємств, опрацьовано концепт формування механізму розвитку управління ризиками й визначено методичні підходи до діагностики РУРТП в реаліях цифрової трансформації, охарактеризовано стан та виявлено тенденції РУРТП, визначено ключові чинники впливу на ці процеси в реаліях цифрової трансформації, оцінено ризикозахищеність та ефективність, обґрунтовано напрями активізації, умотивовано методичні підходи до модернізації механізму розвитку управління ризиками, окреслено можливості нових інструментів страхування й методів управління ризиками та запропоновано стратегічні орієнтири РУРТП в реаліях цифрової трансформації, що забезпечить перехід до нової якості функціонування телекомунікаційних підприємств та стимулюватиме підвищення їх ризикозахищеності, результативності, адаптивності, зрілості та гнучкості.

Для викладачів, аспірантів, магістрів і студентів економічних спеціальностей, керівників й працівників телекомунікаційних підприємств та усіх, хто цікавиться теоретико-методологічними й практичними аспектами РУРТП в реаліях цифрової трансформації.

УДК 621.391:004.056(02)

ЗМІСТ

ПЕРЕДМОВА	4
РОЗДІЛ 1 ТЕОРЕТИЧНА ПЛАТФОРМА РОЗВИТКУ УПРАВЛІННЯ РИЗИКАМИ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ В РЕАЛІЯХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ	5
1.1. Сутнісна характеристика розвитку управління ризиками телекомунікаційних підприємств	5
1.2. Управління ризиками в проєктах цифрової трансформації телекомунікаційних підприємств	23
1.3. Механізм розвитку управління ризиками в телекомунікаційних підприємствах	38
1.4. Методичні підходи до діагностики розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації	52
РОЗДІЛ 2 ПРАКТИЧНІ АСПЕКТИ РОЗВИТКУ УПРАВЛІННЯ РИЗИКАМИ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ	67
2.1. Тенденції розвитку управління ризиками телекомунікаційних підприємств	67
2.2. Ключові чинники впливу на розвиток управління ризиками телекомунікаційних підприємств	78
2.3. Ефективність розвитку управління ризиками телекомунікаційних підприємств	89
2.4. Ризикозахищеність телекомунікаційних підприємств в реаліях цифрової трансформації	100
РОЗДІЛ 3 ПРІОРИТЕТНІ НАПРЯМИ РОЗВИТКУ УПРАВЛІННЯ РИЗИКАМИ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ В РЕАЛІЯХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ	111
3.1. Напрями активізації розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації	111
3.2. Модернізація механізму розвитку управління ризиками в телекомунікаційних підприємствах	126
3.3. Нові інструменти страхування та методи управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації	139
3.4. Стратегічні орієнтири розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації	145
ПІСЛЯМОВА	161
БІБЛІОГРАФІЯ	164
ДОДАТКИ	175

ПЕРЕДМОВА

Стрімке зростання кількості збиткових та неплатоспроможних підприємств спричинили кризові деформації економічного простору України, зумовлені введенням жорсткого локдауну, спровокованого пандемією COVID-19, а потім запровадженням воєнного стану, як реакції на повномасштабну збройну агресію Російської Федерації проти України. Для того, щоб вистояти у ці непрості часи, телекомунікаційні підприємства ведуть пошук і опрацьовують нові стратегії, технології, інструменти, методи управління ризиками. Проте, вітчизняні реалії сьогодення унеможливають це завдання, оскільки, більшість телекомунікаційних підприємств, опирається на застарілу фрагментарну парадигму розвитку управління ризиками. Тому, формування нової концепції активізації розвитку управління ризиками в телекомунікаційних підприємствах, яка передбачає необхідність докорінних якісних перетворень, перехід від невизначеності до зрілості, організаційної різноманітності й гнучкості, зміни пріоритетів і цінностей, набуває вагомого значення та актуалізується.

Безцінним надбанням щодо осмислення сутнісних аспектів і розробки методичних підходів стосовно розвитку управління ризиками телекомунікаційних підприємств, вважаємо потужні фундаментальні напрацювання, таких визнаних вчених як: І. Ансоф, Д. Баюра, О. Виноградова, В. Гранатуров, О. Гусева, В. Дергачова, О. Десятнюк, Н. Євтушенко, О. Князева, І. Ковшова, В. Колосок, Л. Лазоренко, М.Х. Мескон, Д. Никифорчук, Г. Осовська, О. Петрук, Н. Соловей, О. Сосновська, О. Старинець, І. Федун та інші. Високо оцінюючи їх наукові здобутки та незважаючи на масштаб накопичених по цій проблематиці знань, все ж бракує системного поглибленого розгляду теоретико-методологічних засад та обґрунтування науково-організаційних рекомендацій щодо розвитку управління ризиками телекомунікаційних підприємств, враховуючи специфіку та особливості їх функціонування в реаліях цифрової трансформації. Це й визначило наукову значимість, важливість та прикладну доцільність обраної теми монографічного дослідження.

Композиційна структура роботи орієнтована на вирішення двоєдиного завдання – проведення наукового, дослідження тенденцій розвитку управління ризиками телекомунікаційних підприємств та відповідного аналізу і пояснень прикладного, концептуального й стратегічного характеру в реаліях цифрової трансформації. Текст монографії доповнюється статистичними даними і посиланнями на вітчизняні та іноземні бібліографічні джерела.

Автори висловлюють щире подяку професору В.Б. Толубко, професору Л.Н. Беркман та рецензентам монографії професорам С. М. Боняр, І.М. Зеліско та Н.С. Прокопенко чий поради для підготовки монографії є безцінними.

РОЗДІЛ 1

ТЕОРЕТИЧНА ПЛАТФОРМА РОЗВИТКУ УПРАВЛІННЯ РИЗИКАМИ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ В РЕАЛІЯХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

1.1. Сутнісна характеристика розвитку управління ризиками телекомунікаційних підприємств

Проблема розвитку управління ризиками телекомунікаційних підприємств вважається досить актуальною у теоретичному та практичному зрізі. Брак фінансових ресурсів, обмеженість впровадження інновацій і відсутність адекватних стратегій робить цей процес недореалізованим, що посилюється наявністю зношеної матеріально-технічної бази, застарілого технологічного обладнання, недостатністю компетентного персоналу, дефіцитом результативних механізмів розвитку управління ризиками телекомунікаційних підприємств та недосконалістю понятійного апарату. Цікаво, що наявність потужного наукового базису із різноманітністю наукових підходів щодо визначення сутності понять „ризик”, „управління”, „розвиток”, залишає означену проблематику дискусійною. Тому, варто більш детально розглянути сутність та змістове наповнення даних понять, окреслити їх ключові переваги й обмеження, виявити характеристики, конститутивні атрибути та властивості процесу розвитку управління ризиками телекомунікаційних підприємств.

Діяльність усіх підприємств тісно переплітається з ризиками. „У процесі своєї діяльності підприємства стикаються з різними видами ризиків, які розрізняються між собою місцем і часом виникнення, сукупністю зовнішніх і внутрішніх чинників, що впливають на їх параметри, способом їх аналізу і методами впливу” [31].

Поняття „ризик” у загальному визначенні бере свій родовід від давньогрецького „*risdison*”, що означає скеля чи небезпека зіткнення з нею; древньою італійською „*risicare*”, що перекладається, як „посміти”, „наважитися”; французького слова – „*risdoe*”, що трактується, як загроза чи йти на ризик. І. А. Бланк обґрунтовує, що „поняття „ризик” має доволі давню етимологію, що бере свій початок від первіснообщинного ладу, зокрема, первісні люди, граючи в азартні ігри, оцінювали свої ризики” [11 с.10]. З розвитком суспільних відносин генеруються різні тлумачення ризику, поглиблюється їх зміст та розширюються сфери застосування. Еволюційно поняття „ризик” продемонстровано у додатку А. Проте, переважно, дослідники, походження ризику пов’язували „із загальнонауковими дисциплінами: філософією та економікою” [190].

Адам Сміт (1723 – 1790 рр.) у своєму видатному творі „Дослідження про природу і причини багатства народів”, стверджував, що „ризик є чинником частки прибутку, оскільки досягнення, навіть, звичайної норми прибутку пов’язане з більшим чи меншим ризиком” [188]. Водночас, Йоганн фон Тьонен

(1783 – 1850 pp.) акцентував „на відмінностях між ризиком, який можна застрахувати і ризиком, що не може бути застрахованим – йому повинна відповідати частка прибутку, яка розглядається як плата за можливість банкрутства” [188]. Далі, термін „ризик” з початку ХХ ст. активно використовується у багатьох практичних галузях та наукових розвідках. Так, „ризик” від окремих точних наук (механіка, математика, статистика, фізика) розповсюджується на гуманітарні наукові дослідження – економіки, психології, біології, демографії, права тощо. Дослідження Ф. Найта, Д. Робертсона, Дж. М. Кейнса, Дж. Мілля, А. Маршала, А. Пігу та інших вчених, мали вирішальний вплив на поступ теорії ризиків. „Поняття ризику було пов’язано з можливим виникненням втрат, недоодержанням доходу або прибутку” [139]. Практично, у цей період формуються дві основні теоретичні течії (класична і неокласична) щодо пояснення природи економічного ризику. Фундаторами класичної течії, вважають Дж. Мілля та Н. У. Сеніора, які доводили, що підприємницький дохід складається з частки від інвестованого капіталу, заробітної плати підприємця та компенсації за підприємницький ризик. Тобто, ризик, вони розглядали як математичний розрахунок можливих втрат, які підприємець може понести внаслідок реалізації ухваленого рішення. Таким чином, класична теорія ризику, трактує його як ймовірність отримання збитків від обраної стратегії діяльності. Фундаторами неокласичної течії, вважають видатних науковців А. Маршалла та А. Пігу, які доводили, що „підприємництво в умовах невизначеності має керуватися двома категоріями: розміром очікуваного прибутку та величиною можливих втрат” [190]. Американський дослідник Ф. Найт, який в 1921 р. першим запропонував розмежувати категорії „невизначеність” і „ризик”, акцентував увагу на „принциповій вимірності останнього, відтінюючи його як „вимірну невизначеність” [51]. Видатний англійський дослідник Дж. М. Кейнс окреслює „невизначеність як наслідок ірраціональностей, притаманних природі людини”, і далі доходить висновку, що „слід обов’язково враховувати діяльність людини як джерело невизначеності, а відтак і ймовірних втрат та враховувати притаманну людині схильність до ризику” [188].

На підставі великої чисельності трактувань різних дослідників (додаток Б), можемо стверджувати, що ризик – це багатогранне й складне поняття.

Цікаво, що колектив вчених під провідом А. В. Руснака обґрунтовує, що „ризик це діяльність суб’єктів підприємницької діяльності, що пов’язана з подоланням невизначеності в ситуації неминучого вибору, у процесі якої є можливість оцінити вірогідність досягнення бажаного результату, невдачі, відхилення від мети, що містяться у вірогідних альтернативах” [152].

За переконанням О. Б. Секеріна: „ризик – це характеристика підприємницької діяльності, пов’язана із суб’єктивною оцінкою підприємством наслідків впливу чинників невизначеності на результати рішення, що приймається з точки зору сприятливого і несприятливого впливу” [145 с. 69]. Акцентуємо, що ризику притаманне „діалектичне об’єктивно-суб’єктивне” [23] змістове наповнення (рис. 1.1).

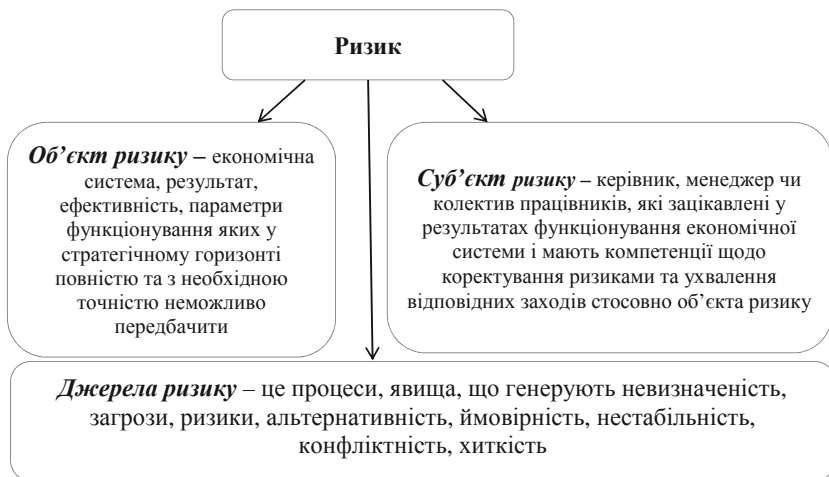


Рис. 1.1. Діалектичне об'єктивно-суб'єктивне змістове наповнення ризику
Примітка: сформовано на основі [23].

Рисунок 1.1. наочно демонструє помітний взаємозв'язок „ризик” з термінами ймовірності й невизначеності. Звертаємо увагу, що чинник ймовірності, невизначеності, відчутно впливає на ефекти ризику, які виражаються у негативному, позитивному чи нейтральному форматі (рис. 1.2).

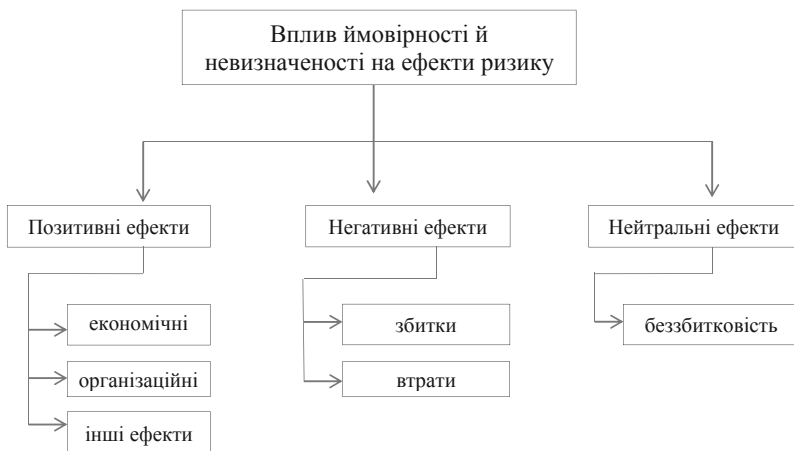


Рис. 1.2. Вплив ймовірності й невизначеності на ефекти ризику
Примітка: сформовано на основі [167 с. 124].

„Ймовірність” (від латинської „probabilitas” чи англійської „probability”) – це окреслення можливості того, що певна випадкова подія здійсниться за умов, які можуть багато чисельно повторюватися. А, наявність невизначеності пояснюється дослідниками як „передумова виникнення ризику, фундаментальна характеристика недостатньої забезпеченості процесу прийняття економічних рішень знаннями стосовно певної проблемної ситуації” [171 с. 16]. Водночас, передумовами ризику вважаються ще й конфліктність, альтернативність та хиткість.

Розгляд різноманітних наукових публікацій дає змогу, стверджувати, що, багато вчених розглядають ризик „post factum”, тобто не здійснюючи його превентивної оцінки, практично як накопичення статистики, інші виявляють лише окремі його ефекти тощо. Опираючись на узагальнені наукові підходи різних авторів до визначення категорії ризику, слід їх систематизувати – ймовірнісний, нерозривний, цільовий, ресурсний, ситуативний, синтезний (табл. 1.1).

Акцентуємо, що в сучасних економічних реаліях більш доцільним, вважаємо тлумачення ризику у контексті інтегрального підходу, що враховує багатоаспектність та змістовність цієї категорії. Тобто, ризик слід окреслювати не лише у контурі позитивних ефектів на прибутки чи фінанси підприємства, а й у зрізі ймовірнісних відхилень від запланованих бізнес-процесів та можливості примноження ціннісних показників підприємства, які у стратегічному горизонті подій визначатимуть приріст його дієвості та ефективності. Зважаючи на означене, окреслимо сутнісні характеристики „ризик” [9 с 33; 21; 167]:

Таблиця 1.1

Наукові підходи до тлумачення поняття „ризик”

Науковий підхід	Тлумачення поняття
Ймовірнісний	Потенційні можливі втрати, непевність у бажаному результаті, загроза несприятливих ефектів
Нерозривний	Постійна необхідність переборювати перешкоди задля досягнення визначеної мети
Цільовий	Можливість невизначеного відхилення від поставленої мети
Ресурсний	Загроза втрати, частини активів, недоотримання доходів, необхідність додаткових ресурсних витрат
Ситуативний	Ситуативна характеристика умов діяльності підприємства, що передбачає невизначеність генерування ефектів
Синтезний	Враховання багатьох кількісних та якісних індикаторів, для ідентифікації ризику та управління ним

Примітка: складено на основі [23].

Ризику притаманна економічна природа та невизначеність ефектів прояву; генерується постійно; коливання від бажаних мети та параметрів; можливість непередбачуваних, зумовлених обраними альтернативами результатів; не прогнозованість; незворотність прояву ефектів, результат яких не залежить від рішень менеджменту підприємства; можливість кількісного

обрахування його ефектів; об'єктивність прояву; зорієнтованість на стратегічні горизонти подій; конфліктність; суперечливість; альтернативність; динамічність; результативність; взаємозв'язок різновидів ризику. Узагальнення та систематизація зовнішніх та внутрішніх джерел виникнення ризику у діяльності підприємства наведена у таблиці 1.2.

Таблиця 1.2

Узагальнення та систематизація зовнішніх та внутрішніх джерел виникнення ризику у діяльності підприємства

Зовнішні джерела	Внутрішні джерела	Зовнішні джерела
Прямого впливу	Об'єктивні	Опосередкованого впливу
Природно-кліматичні та форс-мажорні кризові явища (кліматичні, вогні, екологічні, пандемія тощо)	Забезпеченість підприємства ресурсами та ефективність їх використання Розробка, впровадження нових технологій, інноваційних рішень тощо Якість і рівень маркетингової діяльності Рівень прибутковості підприємства	Непередбачені зміни в міжнародних відносинах
Нормативно-правове поле у телекомунікаційній сфері	Витрати виробництва та обігу Якість та конкурентоспроможність продукції Продуктивність праці Система оплати праці	Політична ситуація у країні
Нестабільність економічної (фінансової, податкової, зовнішньо-економічної тощо) політики	Непередбачені зміни у процесі ведення бізнесової діяльності Недотримання положень стратегії розвитку, тактичного й оперативного планування, або їх відсутність Недостатність бізнес-інформації на підприємстві Географічна локація виробничих потужностей підприємства	
Науково-технічний прогрес	ПІДПРИЄМСТВО	
Непередбачені дії органів державної влади та місцевого самоврядування	Недостатня пристосованість (маневреність) підприємства до змін конкурентного середовища Помилки під час прийняття та реалізації управлінських та виробничих рішень	Непередбачені зміни економічної ситуації у країні, регіоні, галузі
Зміна кон'юнктури внутрішнього і зовнішнього ринків	Помилки під час ідентифікації ризиків та реалізації стратегій управління ризиками Неефективна робота управлінської та інших служб	
Вплив конкурентного середовища	Інтелектуальний потенціал, рівень професійного досвіду, рівень і якість знань, компетентність управлінських кадрів та інших фахівців	
Зміни у відносинах з постачальниками, діловими партнерами, клієнтами	Система індивідуальних інтересів та мотивації у ділових ситуаціях	
	Суб'єктивні Внутрішні чинники	

Примітка: розроблено авторами на основі [37, 157, 185].

Підтримуємо тезу, що сучасні виклики зумовлюють специфіку прояву ризику [28]:

„ризик набули тотального, загального та глобального характеру; економічне середовище стає ризиковим (конкуренція, кон'юнктура, цінова нестабільність тощо);

дедалі більше виникає необхідність ухвалення миттєвих одноосібних рішень;

ризик стає об'єктом управління завдяки використанню: резервів, страхування, диверсифікації, лімітування, нормування й хеджування” [28].

Кожне підприємство має адаптуватись до непередбачуваних кризових, швидких, глибоких деформацій економічного простору, що притаманне для нашої країни, зберігаючи свої функції та характеристики. Виконання означених вимог можливе з використанням механізмів і технологій управління ризиком.

Узагальнене окреслення сутності категорії „управління” зводиться до наступного: управляти означає „...керувати, спрямовувати діяльність будь-кого, будь-чого” [17]; „управління – це свідомий цілеспрямований вплив з боку суб'єкта на об'єкт, що здійснюється задля спрямування їх дії у потрібне русло для отримання бажаного результату” [13]; „управління скеровує дію, результатом якої є зміна керованого процесу, предмета чи явища, їх перетворення, перехід із одного стану в інший” [83];

Сам термін „управління ризиками” розглядається в багатьох наукових вітчизняних та зарубіжних розвідках. Так, Устенко О.Л. [161], обґрунтовує „управління ризиком”, „як процес впливу на суб'єкт господарювання, при якому забезпечується максимально широкий діапазон охоплення ризиків, їх обґрунтоване прийняття та зведення ступеня їх впливу до мінімальних меж, а також розробка стратегії поведінки в разі реалізації конкретних видів ризику [161]. Гранатуров В.М. [33] визначає „управління ризиком” як „сукупність методів, прийомів, заходів, що дозволяють прогнозувати настання ризикованих подій, вживати заходів щодо виключення або зниження негативних наслідків їх настання” [33]. Штефаніч Д.А. [159], надає ширше формулювання „управління ризиком це сукупність дій економічного, організаційного та технічного характеру, спрямованих на визначення видів, факторів, джерел ризику, оцінку їх величини, розробку та реалізацію заходів щодо зменшення рівня та запобігання можливих втрат” [159].

Черненко Ю. О. [166], переконує, що „метою управління ризиками є забезпечення необхідного рівня стійкості та адаптивності підприємства до можливих загроз для його стабільного функціонування” [166]. Швець Ю. О. [169] окреслює „управління ризиками” через здійснення ключових функцій підприємства [169]. Підтримує такий підхід О. М. Лозовський [98]. На противагу такому функціональному підходу, Лук'янова В.В. [100] надає сутнісне тлумачення терміну „управління ризиками” за допомогою критеріїв і регламентів ухвалення управлінських рішень у цьому процесі.

Опираючись на дослідження науковців та зважаючи на мету нашого дослідження підтримаємо, що „управління ризиками будь якого підприємства,

це „цілісна система взаємопов’язаних елементів, що відображають процеси, спрямовані на діагностику, превенцію, нейтралізацію і мінімізацію ризиків та джерел їх генерування на всіх ієрархічних рівнях управлінського впливу” [40]. Таке визначення дає можливість уникнути логічних суперечностей при побудові механізму управління ризиками, формуванні відповідних методів, підходів, індикаторів діагностики тощо. Ключові принципи, якими слід керуватися при формуванні системи управління ризиками продемонстровано на рисунку 1.3.

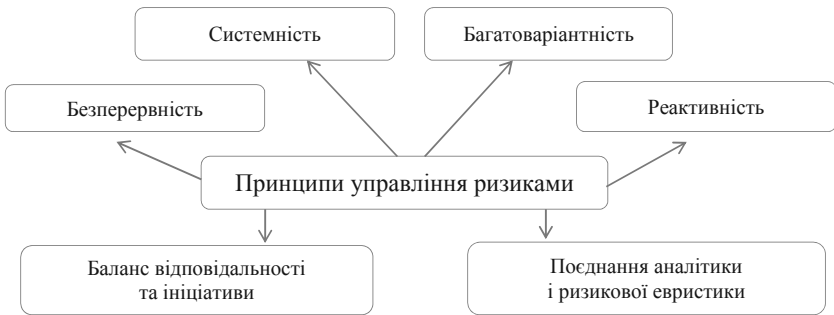


Рис. 1.3. Принципи управління ризиками підприємства

Джерело: складено за інформацією наведеною у додатках К, Л та [67].

„Ключовим завданням управління ризиками підприємства вважається встановлення оптимального рівня ризику на основі врахування чинників зовнішнього та внутрішнього середовища” [152]. Вочевидь, що результативність досягнення мети та виконання завдань управління ризиками зумовлюється адекватністю класифікації ризиків. В наукових публікаціях знаходимо багато пропозицій щодо класифікації ризиків підприємства, підґрунтям яких є різноманітні ознаки (додаток Е). Узагальнена класифікація ризиків підприємства представлена на рисунку 1.4.

На основі пропозицій науковців [9, 13, 23, 34, 37], сформулюємо низку узагальнень:

діапазон та асортимент ризиків підприємства залежить від складності його організаційної структури, різноманітності комунікаційних ланцюгів та стану його внутрішнього і зовнішнього середовища;

найбільш детальні класифікації ризиків, вважаємо громіздкими і незручними для практичного використання;

під ідентичною назвою різні дослідники мають на увазі різні ризики, при цьому спостерігаються значні розбіжності у визначенні їх сутності;

багато класифікаційних ознак штучно додано за рахунок суто теоретичних ознак, які неможливо використати на практиці;

не може існувати універсальної для усіх підприємств класифікації ризиків, водночас існують ознаки, що є спільними для усіх підприємств.



Рис. 1.4. Узагальнена класифікація ризиків підприємства
Примітка: сформовано за [34, 167].

Саме, підприємство вважається базисом будь якої національної економіки. Господарський Кодекс України визначає, що „підприємство – самостійний суб’єкт господарювання, створений компетентним органом державної влади або органом місцевого самоврядування, або іншими суб’єктами для задоволення суспільних та особистих потреб шляхом систематичного здійснення виробничої, науково-дослідної, торговельної, іншої господарської діяльності” [32]. При цьому, доцільно враховувати „особливості функціонування самого телекомунікаційного підприємства (організаційний дизайн, обсяги діяльності, форму власності, ступінь діджиталізації, вплив ризикоформуючих чинників тощо)” [184].

Специфіка ІТ-послуги й ІТ-продуктів зумовлюють і специфіку функціонування телекомунікаційних підприємств, притаманних їм ризиків та відповідно й особливостей розвитку управління ризиками (додаток Ж). Передусім, ринок телекомунікаційних послуг на якому вони функціонують, вважається інноваційно ємким через стрімкий поступ цифрових технологій. Окрім того, високий попит через широке споживання телекомунікаційних послуг і продуктів пояснюють наявність гострої конкурентної боротьби між телекомунікаційними підприємствами, що вимагає від них розвивати сучасну технічну інфраструктуру, мати потужне цифрове обладнання й налагоджену комунікаційну мережу зі споживачами.

Водночас, оскільки, надання телекомунікаційної послуги відбувається одночасно із її споживанням, це генерує високу ресурсну залежність телекомунікаційних підприємств щодо можливості виробляти і надавати якісні телекомунікаційні послуги.

Окреслимо характерні атрибути діяльності телекомунікаційних підприємств: наявність широкого спектру та асортименту ризиків; нестача компетентного персоналу, висока плинність кадрів; якісно нові вимоги до компетенцій працівників; можливість дистанційної роботи фахівців без втрат продуктивності праці; необмежена масштабованість діяльності; низька частка у собівартості продуктованих послуг та продуктів матеріальних витрат; необхідність використання сучасних технологій; необхідність своєчасної модернізації технічного та програмного забезпечення.

Враховання означених характерних атрибутів діяльності телекомунікаційних підприємств при управлінні їх ризиками забезпечить вищу ефективність управлінських процесів, сприятиме формуванню належного організаційного, інформаційного, комунікаційного забезпечення кожного етапу та генеруванню бажаних результатів.

Підтримуємо позицію тих науковців, що стверджують, що телекомунікаційні підприємства підпадають під вплив тих самих ризиків, як і інші підприємства різної галузевої належності, водночас, вони підпадають під вплив специфічних ризиків. Так, операційний ризик телекомунікаційних підприємств, може бути пов'язаний з неналежним виконанням зобов'язань щодо надання телекомунікаційних послуг, розробки програмного забезпечення через внутрішні проблеми. Тобто цей ризик, доцільно розкривати як специфічний.

Деякі вчені [29, 99] обґрунтовують наступні групи джерел ризику, що притаманні телекомунікаційним підприємствам: „технологічні, пов'язані з IT-інфраструктурою; втрати кадрового потенціалу; втрата або витік інформації; соціальні; проектні; юридичні; ринкові” [99]. Цікаві пропозиції щодо типології джерел ризику телекомунікаційних підприємств надають інші науковці [60].

Метою розвитку управління ризиком телекомунікаційних підприємств доцільно визначити підвищення ймовірності отримання позитивних результатів за рахунок зниження ймовірності невдач. Відповідно такого означення мети розвитку управління ризиком телекомунікаційних підприємств, дослідники переважно виокремлюють види ризиків та їх джерел (додаток 3). Так, дослідники [90, 99, 114] окреслюють „три групи ризиків: ризики, пов'язані з якістю розроблюваного продукту; ризики, пов'язані зі швидкістю розробки; ризики, пов'язані з бюджетом, який виділяється на розробку” [90, 99, 114]. Тобто, акцентується увага на строках, якості послуг (продукції) та бюджет. Підтримують такий підхід інші вчені [95, 163], які вважають ці ризики специфічними.

Нині, цифрова трансформація бізнес-процесів вважається необхідною умовою, для успішного функціонування усіх підприємств та споживачів, тому вони намагаються впровадити цифрову трансформацію у найкоротші часові терміни, що пояснюється загостренням конкурентної боротьби та прагненням

генерування додаткових конкурентних переваг. Цим пояснюється і посилення вимог до якості IT- послуг та IT-продуктів, що впливає на можливості їх модернізації, інтеграції та розширення клієнтського кола.

До специфічних ризиків телекомунікаційних підприємств відносять [95, 163] „помилки при розрахунках, порушеннях строків надання інформації, збоїв в програмному забезпеченні, втраті бази даних, тобто технологічні ризики”. Звертаємо увагу, що цими ризиками складно управляти, оскільки вони не документуються і не висвітлюються підприємствами. Вагомим ризиком телекомунікаційних підприємств є кадровий ризик, оскільки він зумовлений плінністю персоналу та необхідною високою їх кваліфікацією та рівнем їх перепідготовки.

Ринковий ризик пояснюється деформаціями економічного простору, змінами кон'юнктури. З однієї сторони телекомунікаційний ринок функціонує під дією чинників, які вважаються типовими для усіх підприємств, а з іншої – їх специфіка та темпи впливу помітно змінюють параметри функціонування. Зокрема, це стосується впровадженням і швидким розповсюдженням хмарних обчислень, потужного використання мобільних пристроїв та сучасних інформаційно-комунікаційних технологій, широкого використання соціальних мереж в бізнесі. Неадекватне врахування означених чинників може звузити попит на окремі IT-послуги та IT-продукти, що зумовить економічні втрати через коливання цін. Незважаючи на високі темпи розвитку телекомунікаційної сфери, нормативно-правове поле її функціонування в Україні почало формуватися та удосконалюватися лише протягом останніх років. Часті коливання нормативно-правового поля щодо функціонування телекомунікаційних підприємств, зокрема в регламентній, податковій сфері, пояснюють генерування високих юридичних ризиків.

Типові бізнес-процеси телекомунікаційних підприємств складаються з трьох основних блоків: процеси розвитку, операційні процеси та процеси підтримки (рис. 1.5). Крім фінансових, маркетингових та управлінських ризиків, вагома частка втрат телекомунікаційних підприємств визначається ризиками операційної діяльності, тобто, ризиками бізнес-процесів, безпосередньо пов'язаних із наданням IT - послуг чи IT – продуктів своїм клієнтам. Тому операційні ризики відносяться до суттєвих ризиків. До таких ризиків можна віднести:

1) *ризик основної діяльності*, спричинений технічними питаннями, що зумовлюють зростання вартості електроенергії, сировини та матеріалів, витрат на охорону навколишнього середовища;

2) *ризик недостатньої кваліфікації працівників* та низької продуктивності;

3) *техніко-технологічний ризик*, який включає недосконалість бізнес-процесів, помилки тарифікації, не оптимальність маршрутизації трафіку, збої технологічного обладнання, шахрайство, дії конкурентів, розвиток телекомунікаційних мереж, впровадження нових послуг.



Рис. 1.5. Специфічні ризики телекомунікаційних підприємств у зрізі бізнес-процесів.

Примітка: сформовано за [99, 114, 150].

Так, зокрема, за оцінками експертів, „у результаті реалізації ризикових подій операційної діяльності компанія-оператор зв'язку може втратити близько 15% своїх доходів, що негативно вплине на інвестиційну привабливість компанії” [150 с.170]. Крім операційних ризиків для телекомунікаційних підприємств особливо характерні інвестиційні ризики, оскільки особливі умови конкуренції ринку телекомунікаційних послуг змушують вкладати кошти в інноваційні проекти, створені задля розвитку нових технологій.

До таких новаторських технологій та послуг, що надаються на їх основі, можна віднести: широкосмуговий доступ до Інтернету, послуги інтелектуальної мережі зв'язку, цифрове телебачення, організація відео конференцій, пропуск трафіку за допомогою віртуальних приватних мереж та інші. Головним заходом подолання наслідків та ризиків кризи стало скорочення інвестиційних програм. Систематизація ризиків телекомунікаційних підприємств, зважаючи на мету нашої розвідки наведена у додатку 3.

Між виокремленими блоками специфічних ризиків (додаток И) проявляється взаємозалежність. Представлений систематизований опис специфічних ризиків для функціонування телекомунікаційних підприємств надасть можливість сформувати індикатори цих ризиків для проведення діагностики та виявити результативність розвитку управління ризиками телекомунікаційних підприємств.

Тепер на часі, з'ясувати сутність поняття „розвиток управління ризиками телекомунікаційних підприємств”, оскільки, „внаслідок розвитку управління виникає новий якісний стан підприємства, що проявляється у зміні його складу або структури (тобто виникнення, трансформація або зникнення його елементів чи зв'язків) [6; 168]. Цікаво, що ще Г. Гегель стверджував, що розвиток не проходить по замкнутому колу, а здійснюється поступово від нижчих до вищих форм, супроводжуючись переходом кількісних змін в якісні, і джерелом розвитку є протиріччя [26]. У наукових публікаціях знаходимо розгляд трьох ключових підходів до сутнісного тлумачення категорії „розвиток [6; 25; 138]: через вивчення і виділення властивостей систем, які розвиваються; через формування трактувань цієї дефініції; як порівняльної характеристики об'єкта” [6; 25; 138].

Системне узагальнення наукових підходів щодо визначення сутнісних ознак категорії „розвиток” продемонстровано на рисунку 1.6.

Тобто, розвиток як закон самого буття, окреслює перехід за певною траєкторією від одного його стану до іншого, який буде характеризуватися новими кількісними та якісними властивостями. Зважаючи на швидкість трансформацій економічного простору для функціонування підприємств, слід, окреслювати „розвиток управління” у контурі: зміни мети і завдань підприємства, нової траєкторії розвитку, адаптації до внутрішніх і зовнішніх конкурентних умов, перетворення організаційного дизайну підприємства (рис. 1.7).



Рис. 1.6. Системне узагальнення наукових підходів до визначення сутнісних ознак категорії „розвиток“
Примітка: сформовано за [6; 25; 138].

В. Шандова [168], Т. Надтока [113], Н. Мала [104], І. Підкаміний [124], Ю. Плугіна [125] погоджуються, що „розвиток управління є сукупністю змін якісного стану підприємства під впливом факторів зовнішнього та внутрішнього середовищ” і далі стверджують, що „за своєю спрямованістю розвиток може бути висхідним, спадним чи нейтральним, в залежності від стадій життєвого циклу підприємства” [127 с. 67].

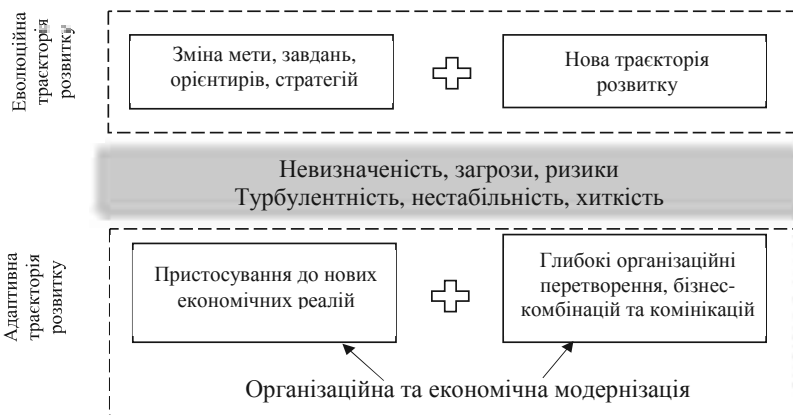


Рис. 1.7. Підходи до формування траєкторії розвитку управління ризиками
Примітка. систематизовано на основі [104, 113, 124, 125, 127, 168]

Підґрунтям змістовної інтерпретації категорії „розвиток управління ризиками” доцільно визначити вимоги наступних ключових принципів: сутнісної повноти, комплексності, системної цілісності управління, синергетичності, гармонійної збалансованості управління, цільової зорієнтованості управління, органічної єдності усіх складових.

Отже, розвиток управління ризиками підприємства – це динамічний процес трансформації якісного та кількісного стану управлінської системи підприємства під впливом дії ризиків внутрішнього та зовнішнього середовища, що передбачає формування нових характеристик і властивостей управлінської системи з використанням ситуаційної адаптації до кризових умов функціонування. Нині, дослідники окреслюють декілька ключових моделей і концепцій розвитку управління ризиками підприємства (додаток В). Опираючись на обґрунтування дослідників [56 с.238-240; 127 с.109-110] щодо поняття „розвиток управління ризиками” підтримуємо його розгляд у зрізі трьох ключових траєкторій (рис. 1.8).



Рис. 1.8. Траєкторії розвитку управління ризиками телекомунікаційних підприємств

Примітка: сформовано за [104, 113, 124, 125, 127, 168].

Наочно, формування унікальної траєкторії розвитку управління ризиками продемонстровано на рисунку 1.9. Обґрунтовані наукові положення до формування унікальної траєкторії розвитку управління ризиками для кожного телекомунікаційного підприємства, які на відміну від існуючих враховують специфіку його організаційного дизайну, обсяги діяльності, рівень діджиталізації, вплив ризикоформуючих чинників, конкретизують площини витоків загроз та ризиків, що забезпечить обґрунтованість, об’єктивність і своєчасність прийняття адекватних управлінських заходів, сприятиме пошуку

стратегічних альтернатив та імплементації превентивних управлінських рішень щодо мінімізації чи уникнення ризиків.

В. Ляшенко стверджує, що „розвиток управління ризиками невід’ємно пов’язано зі змінами, але найбільшим результатом розвитку є вдосконалення та пропонує розглядати розвиток у зрізі трьох аспектів: „зміна”, „зростання”, „вдосконалення” [103].

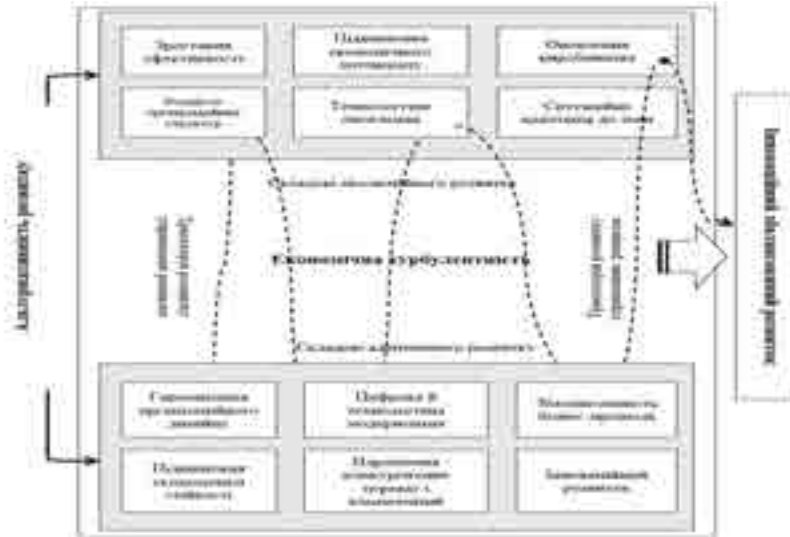


Рис. 1.9. Формування унікальної траєкторії розвитку управління ризиками телекомунікаційного підприємства

Примітка: сформовано за [104, 113, 124, 125, 127, 168].

Водночас, результатами розвитку управління ризиками на підприємстві, переважно дослідники визначають: „зменшення впливу зовнішнього середовища через опір, стійкість, адаптивність тощо” [82 с. 6; 128 с. 32; 130 с. 62]; „підвищення значущості підприємства” [115 с. 161]; „збільшення можливостей” [15]; „зростання ефективності функціонування” [82 с. 6; 130 с. 62].

Згідно загальної теорії оптимізації розвитку розглянемо алгоритм вибору оптимальної траєкторії розвитку управління ризиками телекомунікаційного підприємства [58, 61, 94]. Для прикладу, на вхід альтернативного розвитку управління ризиками впливає один з m – ризиків, що рівномірно й рівнопотужно діє з тривалістю τ :

$$S_{j\varphi}(t) = S_j(t) \cos \varphi + S_j^*(t) \sin \varphi, \quad j = 1, 2, \dots, m,$$

з рівномірним розподіленням на інтервальному часовому відрізку від 0 до 2π з початковою інтенсивністю φ і так званим гаусовським шумом $n(t)$, тобто:

$$x(t) = S_{j\varphi}(t) + n(t).$$

За таких умов, ймовірність помилки чи відхилення буде мінімальним, коли телекомунікаційне підприємство ухвалить рішення про управління такого ризику S_i , для якого при усіх методах $j \neq i$ виконується нерівність:

$$\begin{aligned} & \left[\int_0^{\tau} x(t) S_i(t) dt \right]^2 + \left[\int_0^{\tau} x(t) S_i^*(t) dt \right]^2 > \\ & > \left[\int_0^{\tau} x(t) S_j(t) dt \right]^2 + \left[\int_0^{\tau} x(t) S_j^*(t) dt \right]^2. \end{aligned} \quad (1.1)$$

Де S_i^* – трансформований за Гільбертом ризик S_j .

Тобто, тривалість та інтенсивність впливу τ дорівнює тривалості ухвалення рішень щодо інструментів та методів управління ризиком, тобто $\tau = 2T$, тому алгоритм вибору оптимальної траєкторії розвитку управління ризиками телекомунікаційного підприємства наступний: на інтервальному часовому відрізку n -ого ризику впливу варто ухвалити рішення на користь траєкторії стійкого розвитку управління ризиками S_i з різницею траєкторних фаз $\Delta\varphi_i$

$$S_i(t) = \begin{cases} a \sin \omega t, & 0 < t \leq T, \\ a \sin(\omega t + \Delta\varphi_i), & T < t \leq 2T, \end{cases}$$

водночас, якщо за усіх $j \neq i$, то матимемо:

$$\begin{aligned} & \left[\int_{(n-1)T}^{nT} x(t) \sin \omega t dt + \int_{nT}^{(n+1)T} x(t) \sin(\omega t + \Delta\varphi_i) dt \right]^2 + \\ & + \left[\int_{(n-1)T}^{nT} x(t) \cos \omega t dt + \int_{nT}^{(n+1)T} x(t) \cos(\omega t + \Delta\varphi_i) dt \right]^2 > \\ & > \left[\int_{(n-1)T}^{nT} x(t) \sin \omega t dt + \int_{nT}^{(n+1)T} x(t) \sin(\omega t + \Delta\varphi_j) dt \right]^2 + \\ & + \left[\int_{(n-1)T}^{nT} x(t) \cos \omega t dt + \int_{nT}^{(n+1)T} x(t) \cos(\omega t + \Delta\varphi_j) dt \right]^2. \end{aligned} \quad (1.2)$$

Здійснимо в нерівності (2.2) прості скорочення й трансформаційні перетворення і використаємо наступні позначення:

$$\left. \begin{aligned} X_{n-1} &= \int_{(n-1)T}^{nT} x(t) \sin \omega t dt, & X_n &= \int_{nT}^{(n+1)T} x(t) \sin \omega t dt, \\ Y_{n-1} &= \int_{(n-1)T}^{nT} x(t) \cos \omega t dt, & Y_n &= \int_{nT}^{(n+1)T} x(t) \cos \omega t dt, \end{aligned} \right\} \quad (1.3)$$

Таким чином, одержимо такий алгоритм вибору оптимальної траєкторії розвитку управління ризиками телекомунікаційного підприємства:

$$\begin{aligned} & \cos \Delta \varphi_i (X_{n-1} X_n + Y_{n-1} Y_n) + \sin \Delta \varphi_i (X_{n-1} Y_n - Y_{n-1} X_n) > \\ & > \cos \Delta \varphi_j (X_{n-1} X_n + Y_{n-1} Y_n) + \sin \Delta \varphi_j (X_{n-1} Y_n - Y_{n-1} X_n), \quad (1.4) \\ & j = 1, 2, \dots, m; \quad j \neq i. \end{aligned}$$

Отримана сукупність нерівностей (1.4) вважається найбільш прийнятним алгоритмом вибору оптимальної траєкторії розвитку управління ризиками телекомунікаційного підприємства, що є доцільним для реалізації за будь-якого асортименту ризиків та інформаційного забезпечення траєкторної фази: $\Delta \varphi_1, \Delta \varphi_2, \dots, \Delta \varphi_m$.

Особливість і перевага такого алгоритму вибору оптимальної траєкторії розвитку управління ризиками телекомунікаційного підприємства проявляється у тому, що розмах інтенсивності впливу між векторами дії різних ризиків розраховується через їх проекції впливу та взаємних ортогональних коливань $\sin \omega t$ і $\cos \omega t$ (що ще називають – квадратурним прийомом). Тоді параметри X і Y , що можна розрахувати за (2.3), а, можливі проекції доцільно визначити за тригонометричною функцією $\Delta \varphi_{n\xi}$ між векторами впливу ризиків n і $(n-1)$ -й їх інтенсивності дії:

$$\left. \begin{aligned} \cos \Delta \varphi_{n\xi} &= \frac{X_{n-1} X_n + Y_{n-1} Y_n}{\sqrt{X_{n-1}^2 + Y_{n-1}^2} \sqrt{X_n^2 + Y_n^2}}, \\ \sin \Delta \varphi_{n\xi} &= \frac{X_{n-1} Y_n - Y_{n-1} X_n}{\sqrt{X_{n-1}^2 + Y_{n-1}^2} \sqrt{X_n^2 + Y_n^2}} \end{aligned} \right\} \quad (1.5)$$

Таким чином, сукупність нерівностей (1.4) можна представити у вигляді:

$$\begin{aligned} & \cos \Delta \varphi_i \cos \Delta \varphi_{n\xi} + \sin \Delta \varphi_i \sin \Delta \varphi_{n\xi} > \cos \Delta \varphi_j \cos \Delta \varphi_{n\xi} + \\ & + \sin \Delta \varphi_j \sin \Delta \varphi_{n\xi}, \quad j = 1, 2, \dots, m; \quad j \neq i, \end{aligned} \quad (1.6)$$

або простіше записати:

$$\cos(\Delta \varphi_{n\xi} - \Delta \varphi_i) > \cos(\Delta \varphi_{n\xi} - \Delta \varphi_j), \quad j = 1, 2, \dots, m; \quad j \neq i. \quad (1.7)$$

Тобто, використовуючи сукупність нерівностей (1.4), отримуємо більш прості алгоритми вибору оптимальної траєкторії розвитку управління ризиками телекомунікаційного підприємства для конкретного асортименту ризиків. При різниці траєкторної фази $\Delta \varphi_1 = 0$ і $\Delta \varphi_2 = \pi$ можна використати:

$$X_{n-1} X_n + Y_{n-1} Y_n > -(X_{n-1} X_n + Y_{n-1} Y_n), \quad (1.8)$$

тобто використаємо двійковий символ для означення ризиків:

$$J_n = \text{sgn}(X_{n-1} X_n + Y_{n-1} Y_n). \quad (1.9)$$

Таким чином, отриманий алгоритм вибору оптимальної траєкторії

розвитку управління ризиками телекомунікаційного підприємства (1.9) може відіграти важливу роль для ухвалення відповідного рішення.

Вирішальними передумовами, що спонукають підприємство до розвитку управління ризиками можна вважати [126 с.130; 127 с.75]:

кризові ситуації та явища в його економічній та управлінській діяльності;

унеможливлення використання існуючого стилю, методів, технології управління, які вже вичерпали себе;

трансформації у зовнішньому середовищі, що зумовлюють генерування нових загроз, викликів, ризиків, на які підприємство має своєчасно знайти адекватну відповідь;

примноження економічного потенціалу, зростання сукупності ресурсів, здатностей, компетенцій персоналу і відповідно до яких, система управління ризиками не відповідає наявним резервам та можливостям;

недосконалість організаційних аспектів, невідповідність комунікаційних ланцюгів новим бізнес-комбінаціям та бізнес-процесам підприємства;

досягнення ліміту можливостей нарощення ефективності діяльності підприємства та продуктивності праці у контурі існуючої організаційної та управлінської системи;

трансформація цільових орієнтирів партнерів, споживачів, клієнтів підприємства;

загострення конкурентної боротьби на ринку, падіння іміджу чи конкурентоспроможності підприємства.

Формування конкурентних переваг зумовлює знаходження нових підходів до траєкторій розвитку управління ризиками на підприємстві (додатки Д, М).

Підсумовуючи, означимо, що розпізнання ризикових явищ, симптомів настання загроз, процесів та управління ними пояснює необхідність впровадження управління ризиками телекомунікаційних підприємств та його розвиток, а традиційні класичні наукові постулати щодо сутнісних аспектів категорії „ризик” стали перепорою і вказують на глибокі протиріччя між існуючими науковими теоріями та практикою, тому, ризик, необхідно розглядати у контексті інтегрального підходу, що враховує багатоаспектність та змістовність цієї категорії, ключовим чинником загроз якого в телекомунікаційних підприємствах виступають технологічні чинники, що зумовлює нерівномірність інтенсивності прояву інших ризикоутворюючих чинників та ускладнює формування комплексу результативних проактивних методів управління ризиками. Виявлено, що особливості функціонування телекомунікаційних підприємств здійснюють відчутний вплив на процеси управління їх ризиками.

Запропонований науковий підхід дозволяє точніше обрати унікальний методичний інструментарій управління ризиками для кожного телекомунікаційного підприємства з урахуванням особливостей його організаційного дизайну, обсягів діяльності, рівня діджиталізації, впливу

ризикоформуючих чинників тощо, конкретизувати площини витоків загроз та ризиків, здійснити їх систематизацію, що забезпечить обґрунтованість, об'єктивність і своєчасність прийняття адекватних управлінських заходів, сприятиме пошуку стратегічних альтернатив та імplementації превентивних управлінських рішень щодо мінімізації чи уникнення ризиків.

1.2. Управління ризиками в проектах цифрової трансформації телекомунікаційних підприємств

Сьогодні цифрова економіка зумовлює, те, що лідерів ринку визначає не багаторічна історія успіху, не вартість нерухомості та активів, не кількість патентів чи доступ до капіталу, а здатність змінюватись та адаптувати свій бізнес до нових умов. Цифрові технології, що з'явилися протягом останнього десятиліття, допомагають знайти джерела підвищення ефективності та можливості стрімкого конкурентного розвитку підприємств. Водночас, вони вимагають змінити існуючі моделі управління, переформатувати комунікації, технології та організаційну структуру підприємств на основі нових цінностей, пріоритетів та орієнтирів, що ґрунтуються на партнерстві, клієнтоорієнтованості, інноваційності та синергії.

Проблемам становлення цифрової економіки та трансформаційним процесам, що відбуваються в економічному просторі під її впливом, значну увагу приділяли вітчизняні та зарубіжні дослідники, зокрема: І. Ансофф, Р.Акофф, В. Апалькова, О. Виноградова, С. Войтко, В. Геєць, А. Глушенкова, О. Гусєва, П. Дойль, П. Друкер, С. Коляденко, І. Карчева, Б. Кінг, І. Ковшова, Л. Лазоренко, Р. Ліпсі, Л. Лямін, І. Малик, А. Томпсон, Е. Тоффлер, К. Шваб та ін. Незважаючи на численні наукові дослідження поза межами обговорення науковою спільнотою залишаються проблеми щодо виявлення впливу цифрових трансформацій на умови господарювання, ризикозахищеність й управління ризиками підприємствами, окреслення передумов, можливостей та обґрунтування завдань і заходів щодо зміни цінностей, пріоритетів та орієнтирів побудови якісно нових моделей розвитку управління ризиками підприємствами на основі сучасних цифрових технологій.

Поняття „цифрова економіка” Дон Тапскот увів у науковий вжиток ще у 1995 р. [231]. У класичному розумінні цифрова економіка – це економіка, що базується на цифрових технологіях, яку ще називають інтернет-економікою, новою економікою, або веб-економікою. Переважно, науковці, під цифровою економікою розуміють виробництво, продаж і постачання продуктів за допомогою інформаційно-комунікаційних мереж.

Ніколас Негропonte особливості цифрової економіки окреслив, як „перехід від обробки атомів до обробки бітів”. В.В. Апалькова переконує, що цифрова економіка є найважливішим двигуном інновацій, конкурентоспроможності і економічного розвитку [226 с. 13]. Томас Месенбург обґрунтував основні складові цифрової економіки [230]:

1) підтримуюча інфраструктура (апаратне забезпечення, програмне забезпечення, телекомунікації, мережі);

2) електронний бізнес (будь-які процеси, які організація проводить через комп'ютерні мережі);

3) електронна комерція (передача товарів он-лайн).

С.М. Веретюк стверджує, що цифрова економіка є складовою частиною економіки, в якій домінують знання суб'єктів та нематеріальне виробництво – основний показник під час визначення інформаційного суспільства [229].

В епоху конкурентної економіки і за часів Сміта мало сенс розраховувати точку беззбитковості і оптимальні розміри підприємств, для цифрової економіки – це не важливо: підприємство може бути дуже маленьким і при цьому успішно розвиватися. Поява Amazon, Netflix, Google, Uber та Apple знищила цілу низку індустрій та відкрила нові ринки. Так, усі ми знаємо приклад компанії Uber, яка не є власником всіх машин, що надають сервіс, навіть не має ліцензії на послуги таксі, а проте ми бачимо результат. Власник може бути одночасно і керівником, і виконавцем всіх етапів роботи компанії. За рекомендаціями фахівців корпорацій „Telstra” і „Deloitte” [230], необхідними умовами для підприємств, які прагнуть до успішної діяльності в умовах цифрової економіки, вважаються наступні цінності:

вони інвестують в нові здібності, а не в старі ділові моделі;

вони високо цінують свої взаємини з клієнтами;

вони стають більш швидкими і оперативними;

вони знають своїх дійсних конкурентів;

вони інвестують в талант.

„Цифрові” технології необхідні для зростання ефективності української економіки, а в деяких секторах і галузях вони стають основою продуктових та виробничих стратегій. Їх перетворююча сила змінює традиційні моделі бізнесу, виробничі ланцюжки та зумовлює появу нових продуктів та інновацій. Цифрові трансформації для України носять позитивний соціальний характер, адже зосереджені на поліпшенні якості інфраструктури соціального забезпечення, якості соціальних послуг, організації прозорості та адресності соціальної допомоги та скороченні витрат [228 с. 39, 230].

Основними напрямками розвитку цифрової-економіки та відповідних цифрових трансформацій мають бути:

здійснення різних транзакцій (торгових і фінансових операцій);

створення бізнес-порталів для розміщення замовлень і пропозицій;

пошук постачальників через мережу Інтернет;

продаж продукції через Інтернет;

покупка продукції і сировини через Інтернет;

пошук персоналу через мережу Інтернет;

розміщення інформації в Інтернет-довідниках;

створення власного сайту;

онлайн-реклама;

впровадження системи Інтернет-банкінгу для роботи з активами в режимі он-лайн;

створення платіжних механізмів для підтримки торгівлі товарами і послугами;

створення нових форм і інститутів кредитування, інвестування та страхування.

Впровадження цифрових трансформацій в Україні стикається з великими труднощами. Серед них:

нестача фахівців;

перманентна проблема з використанням нелегального і піратського програмного забезпечення;

порушення авторських прав та інтелектуальної власності;

повільне впровадження в життя нових інформаційних і фінансових технологій;

повільна реакція держави на нові перетворення в економіці з використанням ІТ в правовій площині.

нівелювання ціни цифрового продукту та інтелектуальної власності в цілому;

відсутність орієнтації виробників ПЗ і інших видів економічної діяльності, суб'єкти яких створюють цифровий продукт, на внутрішній ринок у зв'язку з високим рівнем піратства інтелектуальної власності;

погіршення іміджу держави і періодичному політичному і економічному тиску з боку провідних економічно розвинених держав;

ігноруванні локалізації під український ринок провідних виробників ПЗ.

Нині телекомунікаційні підприємства мають використовувати не одну, а цілий комплекс інтегрованих цифрових технологій, продуктів та послуг (BioTech, NanoTech, RetailTech, FinTech, LegalTech, InsurTech, GovTech, BlockChain, Digital marketing, CRM&BPM на платформах bpm'online, Grid-технології, Digital-страхування, ePrescription, TeleHealth).

Всі вони мають певну цінність для бізнесу – прискорюють роботу, економлять ресурси, збільшують прибуток, створюють унікальний користувальницький досвід, відкривають принципово нові гілки розвитку. Зовсім необов'язково і навіть протипоказано впроваджувати все і відразу. Мати повний спектр технологій – не мета. Важливо оцінити користь і вірно розставити пріоритети. Цифрові трансформації варто розглядати як інструмент стратегічних змін телекомунікаційного підприємства, а не як самоціль.

Для оптимізації внутрішніх комунікацій використовують спеціалізоване програмне забезпечення – ERP, системи електронного документообігу, CRM, Bmps-системи, UPE-платформи з управління ефективністю.

Цікаво, що за дослідженнями ESG (на замовлення Dell EMC), 95% великих підприємств не відповідають вимогам нового цифрового бізнесу, причому 71% підприємств згодні, що втрачають конкурентоспроможність без цифрової трансформації. Успішно трансформовані підприємства в 7 разів частіше називають цифрові технології конкурентною перевагою і джерелом отримання вигоди, а 96% з них майже вдвічі перевиконали свої плани по доходах. Саме, поява новітніх технологій, спровокувала й генерування якісно нових альтернатив, які вважаються ключовим драйвером цифрової трансформації, що зумовлює стрімке впровадження стратегічних змін. Нині,

переважно, стратегічний успіх телекомунікаційного підприємства пов'язаний із цифровою трансформацією. Вплив цифрової трансформації на добробут телекомунікаційного підприємства проілюстровано на прикладі ухвалення рішення щодо доцільності її впровадження (рис. 1.10).

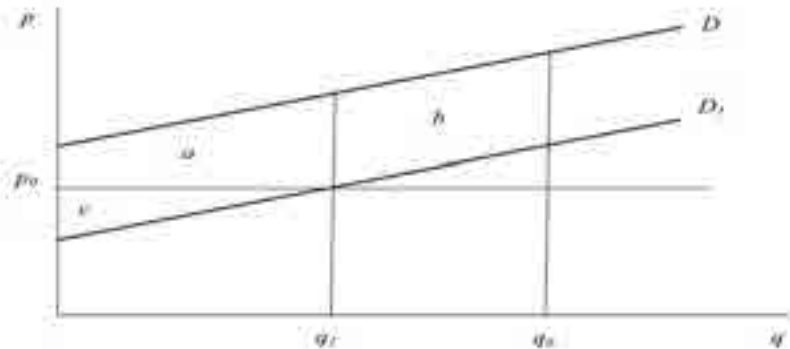


Рис. 1.10. Взаємозв'язок між добробутом телекомунікаційного підприємства та цифровою трансформацією.

Примітки: побудовано за даними [231].

„Об'єктом загостреної уваги є тенденція цифрової трансформації, яка намітилася в останні роки ХХ ст.” [232]. Це трансформації, що безпосередньо пов'язані з новими цифровими технологіями й електронною комерцією, а саме: платформи й сервіси онлайн послуг, інтернет-магазини, інформаційні сайти тощо. Останніми роками концепція цифрової трансформації почала виходити за межі суто технологічного аспекту. Нині, набуває масштабів використання підприємствами цифрових і віртуальних бізнес-процесів (рис. 1.11).

Будь-який бізнесовий проект щодо цифрових трансформацій телекомунікаційного підприємства тісно переплітається з невизначеністю і ризиками

Невизначеність в проекті щодо цифрових трансформацій – це недолік або відсутність інформації, знань або розуміння можливих наслідків дій, що робляться, рішень або подій. Результатом присутності невизначеності є ризики. Один з процесів в управлінні проектом – управління ризиками. Як і інші процеси, він є „наскрізним” для проекту і присутній на всіх стадіях його життєвого циклу.

Відповідно до визначення американського стандарту в галузі управління проектами РМВОК, ризик проекту – це невизначена подія або умова, яка в разі виникнення має позитивний або негативний вплив, щонайменше, на одне з обмежень проекту, наприклад, терміни, вартість, обсяги або якість.

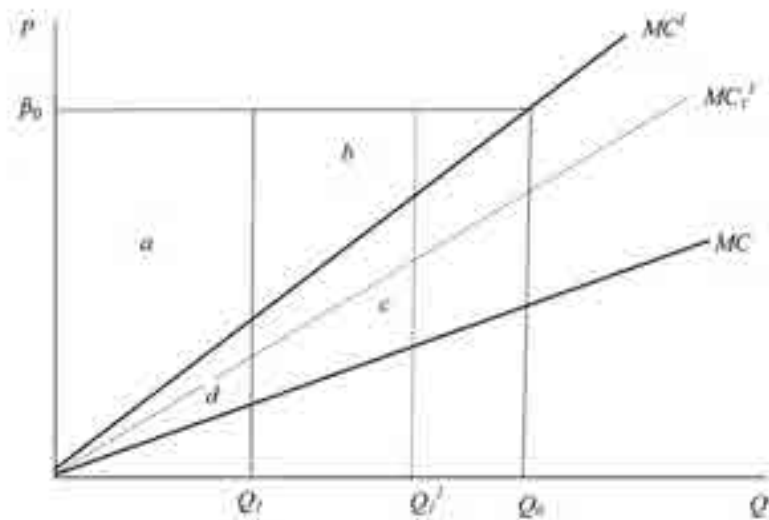


Рис. 1.11. Взаємозв'язок між добробутом телекомунікаційного підприємства та цифровою трансформацією.

Примітка: побудовано за даними [231].

Підкреслюється значимість того, що ризик у проекті може мати не тільки негативний, але і позитивний вплив на проект, тобто приводити до поліпшення якісних і кількісних характеристик кінцевих цілей проекту. Відповідно, можна виділити негативні ризики, позитивні ризики і непередбачені обставини:

1. Негативні ризики – загрози, іншими словами, події, що ведуть до погіршення якості виконання проекту, що вимагають залучення додаткових витрат ресурсів і часу або, ймовірно, що знижують якісні характеристики кінцевого результату.

2. Позитивні ризики – можливості, або події, що надають шанс поліпшити якість реалізації проекту і досягти цілей, можливо, з меншими витратами ресурсів і часу або більш високою якістю.

3. Непередбачувані обставини – ті, що неможливо було або не змогли передбачити на стадії ідентифікації ризиків.

Ризик може бути викликаний однією або декількома причинами і в разі виникнення будь-якої з цих точно не відомих заздалегідь подій може вплинути на вартість проекту, його розклад або виконання. Ризики визначаються як зовнішні по відношенню до проекту щодо цифрових трансформацій або телекомунікаційного підприємства умовами середовища та внутрішніми реаліями реалізації такого проекту.

Для підвищення якості виконання проекту цифрової трансформації і досягнення кінцевих завдань менеджер проекту телекомунікаційного підприємства реалізує процес управління ризиками.

Управління ризиками – це систематичний процес зниження невизначеності та управління ймовірністю подій в проекті. Мета управління ризиками проекту цифрової трансформації – підвищення ймовірності виникнення і впливу сприятливих подій і зниження ймовірності виникнення і впливу несприятливих для проекту подій.

Весь процес управління ризиками проекту цифрової трансформації поділяється на окремі підпроцеси, які виникають як мінімум один раз в кожному проекті, а деякі реалізуються на декількох стадіях проекту, маючи ітеративний характер:

1. Планування управління ризиками – інтегруючий процес вибору підходу, планування і виконання операцій з управління ризиками проекту. Реалізується на стадії планування проекту цифрової трансформації.

2. Ідентифікація ризиків – визначення того, які ризики можуть вплинути на проект, і документальне оформлення їх характеристик. Виникає на стадії планування проекту цифрової трансформації, але носить повторюваний характер, виникаючи періодично для поповнення реєстру ризиків проекту в міру його реалізації.

3. Якісний аналіз ризиків – розташування ризиків за ступенем їх пріоритету для подальшого аналізу або обробки шляхом оцінки і підсумовування ймовірності їх виникнення та впливу на проект цифрової трансформації.

4. Кількісний аналіз ризиків – кількісний аналіз потенційного впливу ідентифікованих ризиків на загальні цілі проекту цифрової трансформації.

5. Планування реагування на ризики – розробка можливих варіантів і дій, що сприяють підвищенню сприятливих можливостей і зниження загроз для досягнення цілей проекту цифрової трансформації.

6. Моніторинг та управління ризиками – відстеження ідентифікованих ризиків, моніторинг залишкових ризиків, ідентифікація нових ризиків (і пов'язаний процес якісного і кількісного аналізу, а також вироблення планів реагування), виконання планів реагування на ризики і оцінка їх ефективності на протязі життєвого циклу проекту цифрової трансформації.

Всі проекти цифрової трансформації для окремих телекомунікаційних підприємств різняться, і кращий метод виявлення потенційних ризиків всередині складного проекту – звернутися до досвіду минулих проектів в тій же галузі. Навіть в різних галузях існує багато однакових або схожих потенційних ризиків.

Перший підхід – повністю проаналізувати різні сегменти проекту цифрової трансформації: масштаб, устаткування, технологія, існуючі дані, персонал, терміни, бюджет. Потім розбивається кожен розділ проекту на більш дрібні фрагменти. Груповий пошук ідей з невеликою групою членів команди, що представляють різні відділи і групи, може принести користь. Він

не повинен займати багато часу, але вкрай важливий для успішного управління проектом цифрової трансформації.

Масштаб. Суть масштабу – визначення того, що входить або не входить в документ бізнес-вимог. Тому сегменти, які можуть створити проблеми, поставлять питаннями, пов'язані з тим, що передбачено або не передбачено у цьому документі. З цієї причини першими виявленими ризиками можуть бути „недолуго визначені бізнес-вимоги”, „відсутність досвідченого персоналу, що визначає вимоги” або „бізнес-вимоги, не затверджені підприємством”.

Устаткування. Цей сегмент аналізу повинен стосуватися обладнання, необхідного для виконання проекту, а не того, що надається або є кінцевим результатом проекту. Воно може включати в себе комп'ютерну техніку або устаткування для виготовлення кінцевого продукту або шерэг інших варіантів, в залежності від конкретного проекту цифрової трансформації. При виявленні ризиків в даному розділі потрібно розглянути такі ризики, як: „яка надійність обладнання”, „наскільки легко замінюється обладнання в разі його пошкодження чи поломки”, „яка вартість заміни несправного обладнання”.

Технологія. У проектах цифрової трансформації, направлених на розробку програмного забезпечення, даний розділ охоплює всі пов'язані з комп'ютерами сфери, крім фізичної апаратури. Потрібно перевірити залежності пакетів програм (внутрішні та зовнішні) і системи управління базами даних. Для довгострокових проектів оновлення до різних версій програмного забезпечення може вплинути на терміни або викликати непередбачені витрати, якщо воно вимагає додаткового персоналу або перенавчання наявного персоналу.

Існуючі дані. Чи потребують існуючі дані переходу на нову систему – якщо так, то чи працюватиме використаний раніше відпрацьований метод, або потрібно принципово нове рішення? Все, що не робилося раніше, ймовірно, несе високий ризик; особливо якщо існуючі дані є пропрієтарними, тому немає досвіду і знань з попередніх проектів всередині або поза організацією, до яких можна звернутися.

Персонал. Наскільки важливий існуючий персонал для успіху проекту? Чи мають вони спеціальні знання, які було б важко або дорого знайти де-небудь ще? Чи висока нинішня плінність кадрів, або ж існуючі групи міцні, добре мотивовані і ймовірно залишаться протягом усього проекту? Керівник глобального проекту цифрової трансформації може навіть не знати проектні групи в різних місцях, а лише підтримувати контакт з локальними керівниками проектів. Проте для невеликого проекту цифрової трансформації знання складу проектної групи дуже важливе в оцінці потенційних ризиків.

Терміни. Наскільки точні оцінки для цілого проекту і для кожної окремої задачі? Чи відрізняється проект від усього, що робилося раніше, і тому є всі оцінки наближеними, або, що ще гірше, чистими здогадками? Чи продиктовані строки бізнесовою необхідністю, як у випадках, коли випуск продукту на ринок раніше конкурентів є першорядним чинником? Чи було дозволено групам, які мають знання для надання точних оцінок, зробити їх? Зазначені фактори впливають на тип і ймовірність виникнення ризиків у сфері термінів.

Бюджет. Чи був бюджет визначений більше бізнесовою доцільністю, ніж реальною вартістю, необхідною для виконання проекту цифрової трансформації? Обмежений бюджет не обов'язково губить успіх проекту. Досвідчений керівник проекту має навички, необхідні для отримання максимальної користі з обмеженого бюджету і для мінімізації ризиків всередині такого проекту.

Багато чинників, які недосвідчені керівники проектів цифрової трансформації вважають такими, що створюють більш ризикований проект, насправді легко управляються, оскільки вони виникають досить часто, наприклад, обмежені ресурси часу або бюджету. Ризиком швидше є те, що виникає рідко, або революційні нові цифрові технології або продукти, що збивають проект з вірного шляху.

Виявлення ризиків в проекті цифрової трансформації має вирішальне значення для успішного управління ними, і описані вище сфери є найважливішими для аналізу при виявленні ризиків.

Кожен керівник проекту цифрової трансформації має бути обізнаним у практиці і принципах ефективного управління ризиками. Якщо керівництво телекомунікаційного підприємства знає, як визначати ризики цифрової трансформації і як з ними поводитися, то, таким чином, можна запобігти зайвим складнощам у майбутньому і підготуватися до них.

Варто, виділити декілька принципів, які винайдені не для того, щоб давати інструкції, а для того, щоб забезпечити підтримку керівнику, яка надає можливість телекомунікаційним підприємствам розвивати процес цифрової трансформації й будувати відповідні стратегії і плани.

1) Організаційне середовище. Всі телекомунікаційні підприємства відрізняються одне від одного. Це є основним принципом всіх загальних методів управління, включаючи підхід PRINCE2 і метод управління успішними програмами проектів цифрової трансформації, так само як управління ризиками. Керівникам проектів, керівникам програм і менеджерам за ризиками необхідно розглянути специфічне середовище телекомунікаційного підприємства для того, щоб гарантувати повне визначення ризиків і відповідні процедури роботи з ними. Термін „організаційне середовище” містить в собі економічний, соціальний, технологічний, правовий аспекти і відноситься до зовнішнього середовища телекомунікаційного підприємства.

2) Залучення учасників. Керівній команді легко засвоїти і також легко забути, що зацікавлені особи є ключовими учасниками в щоденних процедурах бізнесу, а короткострокові і великі ділові проекти цифрової трансформації змінюють програму. Розуміння ролі окремих учасників і їх залучення є ключовим моментом для досягнення успіху. Учасники повинні бути інформовані про ризики проекту настільки, наскільки це можливо. Усередині організаційного середовища залучення учасників має на увазі особу учасника і його роль, ступінь впливу на телекомунікаційне підприємство і за її межами, рівень інвестицій, тип, можливості і потенційний вплив ризику.

3). Організаційні цілі. Ризик є в діях і цілях телекомунікаційного підприємства. Приміром, дощ є негативним ризиком для пікніка, позитивним – для посушливого ділянки і не є ризиком для екіпажу субмарини. Персональна відповідальність за управління ризиками лежить на лідері, керівнику проекту цифрової трансформації, і стосується цілей телекомунікаційного підприємства, для гарантування ретельного підходу.

4). Підхід до управління ризиками. Процес, політика, стратегія і план в межах структури управління ризиками забезпечують загальні принципи і шаблони всередині окремого телекомунікаційного підприємства. Ці принципи ґрунтуються на досвіді управління і на знаннях і дослідженнях професійних менеджерів за ризиком широкого шерегу телекомунікаційних підприємств. Дотримання кращої практики гарантує, що окремі особи, залучені до асоціації управління ризиками та в організаційну діяльність, здатні вчитися на своїх помилках, експериментах і на уроках інших.

5). Звіт. Точне і чітке надання даних і їх передача відповідним співробітникам, керівникам і зацікавленим особам є ключовим чинником успішного управління ризиками. Методологія управління ризиками забезпечує стандартний зразок і перевірену структуру управління учасниками, а також частотою і змістом ризику цифрової трансформації.

6). Ролі та відповідальності. Для кращої практики управління ризиками істотним чинником є чітке визначення ролі управління і відповідальності. Індивідуальні функції і відповідальність повинні бути очевидними всередині телекомунікаційного підприємства та за його межами. Це важливо для термінів організаційного управління та для гарантії того, що вся необхідна відповідальність покладена на відповідну особу.

7). Структура підтримки. Структура підтримки – це забезпечення всередині телекомунікаційного підприємства стандартних принципів, інформації, навчання та фінансування індивідуального управління ризиками, які можуть виникнути в будь-якій цифровій галузі, або в будь-якому проекті цифрової трансформації. Ця структура може включати централізовану команду управління ризиками, стандартний підхід і кращі практичні принципи звіту і перегляду організаційних ризиків.

8). Цикл перегляду. Цикл перегляду пов'язаний з необхідністю отримання показників попереднього сповіщення про настання ризикової події. Він забезпечує постійний перегляд встановлених ризиків і гарантує, що менеджери залишаться відкритими для виявлення нових ризиків цифрової трансформації.

9). Подолання бар'єрів на шляху управління ризиками. Будь-яка успішна стратегія вимагає ретельного розгляду можливих перешкод для здійснення проекту цифрової трансформації. Загальні питання включають в себе:

- встановлення ролей, відповідальностей, підвітності та власності;
- відповідний бюджет для впровадження підходу і виконання діяльності;
- відповідне і доступне навчання, інструменти і методи;

орієнтування на управління ризиками цифрової трансформації, ознайомлення та навчальні процеси.

Регулярне оцінювання підходу управління ризиками, включаючи всі перераховані вище питання.

10). Підтримуюча культура. Управління ризиками має на увазі багато різних сфер і аспектів організаційної діяльності. Підтримуюча культура дуже важлива для того, щоб всі відповідальні особи відчували впевненість, обговорюючи і керуючи ризиками. Підтримуюча культура управління ризиками буде також включати в себе оцінку та винагороду компетентності відповідних осіб.

11). Постійне поліпшення. Телекомунікаційне підприємство, яке прагне успіху не стоїть на місці, а постійно розвивається.

Ефективна політика управління ризиками цифрової трансформації включає здатність до переоцінки і удосконалення. На практичному рівні потрібно призначення окремої особи або групи осіб відповідальних за гарантію того, що політика управління ризиками і методика відповідає сучасним вимогам цифрової трансформації.

Ризики управління проектом цифрової трансформації складаються з виробничих, фінансових та інвестиційних.

Основними джерелами виробничого ризику є виробничий брак, погані умови на будівельних майданчиках, виплата підвищених податків, відрахувань і штрафів, помилки планування, брак координації робіт, зміни в персональному складі керівництва проектом, інциденти, нещасні випадки, дефіцит і відсутність персоналу необхідної кваліфікації для виконання робіт проекту. У вітчизняних реаліях до цих чинників додається низька дисципліна поставок, переобіз з паливом і електроенергією, фізичний і моральний знос устаткування.

Фінансовий ризик враховує грошові витрати, збитки і втрати. Особливістю фінансового ризику є ймовірність настання збитку в результаті проведення яких-небудь операцій у фінансово-кредитній і біржовій сферах, здійснення операцій з фондовими цінними паперами, тобто ризику, що впливає з природи цих операцій. До фінансових ризиків відносяться наступні:

кредитний ризик – небезпека несплати позичальником основного боргу і відсотків, належних телекомунікаційному підприємству;

процентний ризик – небезпека фінансових втрат в результаті перевищення процентних ставок, виплачуваних телекомунікаційним підприємством за залученими засобами, над кредитними ставками;

валютний ризик – небезпека валютних втрат, пов'язаних зі зміною курсу однієї іноземної валюти по відношенню до іншої, у тому числі національній валюті при проведенні зовнішньоекономічних, кредитних та інших валютних операцій.

Фінансовий ризик, як і будь-який ризик, має математично виражену ймовірність настання втрат, яка спирається на статистичні дані і може бути розрахована з досить високою точністю. Щоб кількісно визначити величину фінансового ризику, необхідно знати всі можливі наслідки якої-небудь окремої дії щодо цифрових трансформацій і ймовірність самих наслідків.

Імовірність означає можливість отримання певного результату. Стосовно до економічних задач методи теорії ймовірності зводяться до визначення значень імовірності настання подій і до вибору з можливих подій самого кращого виходячи з найбільшої величини математичного очікування. Інакше кажучи, математичне очікування якої-небудь події дорівнює абсолютній величині цієї події, помноженої на ймовірність його настання.

При будь-якій цифровій трансформації завжди існує небезпека втрат для телекомунікаційного підприємства, яка генерується із специфіки тих чи інших цифрових операцій. Небезпека таких втрат являє собою комерційні (підприємницькі) ризики. Комерційний ризик означає невпевненість у можливому результаті, невизначеність цього результату діяльності. Комерційні ризики пов'язані, зокрема, з непередбачуваністю зміни закупівельної ціни товарів, зростанням витрат обігу, втратами і псуванням сировини, матеріалів і устаткування при зберіганні і транспортуванні.

Розрізняють чисті, (прості) і спекулятивні комерційні ризики. Наявність чистих ризиків означає можливість збитку або „нульового” результату: цей ризик розрахований тільки на програш. Спекулятивні ризики виражають можливості одержання як позитивного, так і негативного результату.

Інвестиційний ризик цифровій трансформації можна визначити як відхилення фактичного доходу від очікуваного доходу. Інвестиція вважається не ризикованою, якщо дохід по ній гарантований. Одним з прикладів не ризикованої інвестиції є цінні папери казначейства, оскільки шанс того, що уряд не зможе купити свої цінні папери, практично дорівнює нулю. Навпаки, при вкладенні коштів у проект цифрової трансформації, пов'язаний, наприклад, з виробництвом принципово нового продукту, або виходом на новий ринок, або впровадження нових інформаційно-комунікаційних технологій, завжди існує певна ймовірність того, що в результаті непередбачених обставин генерування доходів за ним не буде отримано або буде отримано не в повному обсязі.

Загальний або сукупний ризик являє собою суму всіх ризиків, пов'язаних із здійсненням проекту цифрової трансформації і класифікується за різними ознаками.

Виділяються наступні види загального ризику цифрової трансформації: короткострокові – пов'язані з окремими фазами життєвого циклу проекту цифрової трансформації і припиняються разом із завершенням фази; довгострокові – пов'язані з декількома або всіма фазами проекту цифрової трансформації.

За масштабом і ймовірності втрат розрізняють ризики:

високі – висока ймовірність настання ризикових подій і великі масштаби втрат і витрат на подолання наслідків ризикової події;

слабкі – низький рівень втрат.

Залежно від ступеня впливу на фінансове становище проекту цифрової трансформації виділяються:

допустимий ризик – загроза уповільнення виконання проекту або збільшення його вартості в допустимих межах;

критичний ризик – ризик, пов’язаний із загрозою істотного відхилення проекту за термінами і вартістю;

катастрофічний ризик – найнебезпечніший ризик, що приводить до високої ймовірності дострокового припинення проекту або нанесення непоправної шкоди соціально-природним системам.

За сферами прояву виділяють такі ризики цифрової трансформації:

економічні – пов’язані зі зміною економічних чинників здійснення проекту цифрової трансформації;

політичні – пов’язані зі зміною політичного курсу країни, регіону;

соціальні – пов’язані з соціальними проблемами (наприклад, ризик страйків);

екологічні – пов’язані із загрозою екологічних катастроф і лих;

нормативно-законодавчі – пов’язані зі змінами законодавства та нормативної бази.

Залежно від джерел виникнення та можливості усунення проектні ризики цифрової трансформації бувають:

несистемні (специфічні) ризики – ризики, викликані такими особливими для проекту цифрової трансформації подіями, як дефіцит сировини, матеріалів, робочої сили, успішні або невдалі програми взаємодії зі стейкхолдерами проекту, невиконання договорів субпідрядниками, неефективні аутсорсингові заходи, помилки у прийнятті управлінських рішень, аварії, викликані порушенням норм, правил, технологій та багато іншого. Такі ризики носять індивідуальний, специфічний для кожного проекту цифрової трансформації характер, і управління ними залежить від досвіду, знань і навичок менеджера проекту;

системні ризики виникають із зовнішніх подій, що впливають на ринок в цілому: це війна, інфляція, економічний спад, висока ставка відсотка тощо. На систематичний ризик припадає до 50% загального ризику проекту цифрової трансформації. Системні ризики, що мають спільні корені, але різні прояви у різних проектах цифрової трансформації, легше прогнозуються і для них легше скласти загальні правила і рекомендації, які мінімізують їх негативний вплив на проект.

Ризики виникають тоді, коли діють чинники ризику – виникають ситуації, що породжують ризики. Сам по собі чинник ризику не веде до зриву робіт за проектом цифрової трансформації або їх подорожчання, він тільки підвищує ймовірність настання несприятливої події, яка, в принципі, може і не виникнути. Чинником ризику може бути сам проект цифрової трансформації, якщо подібні проекти в телекомунікаційному підприємстві не робилися. Знизити тиск цього чинника може, зокрема, запрошення досвідченого менеджера проекту цифрової трансформації.

Успіх проекту цифрової трансформації залежить від того, яку стратегію або стратегії реагування на ризики запланує і реалізує команда управління проектом. Заплановані операції з реагування на ризики повинні:

відповідати серйозності ризику;

бути економічно ефективними в рішенні проблеми;

бути своєчасними;
бути реалістичними в контексті проекту;
бути узгодженими з усіма учасниками.

Виконання заходів з управління ризиком цифрової трансформації має бути покладено на відповідальну особу, іншими словами, конкретним ризиком управляє конкретний учасник проекту.

У стандартах управління проектами цифрової трансформації виділяються:

1. Стратегії реагування на негативні ризики (загрози);
2. Стратегії реагування на позитивні ризики (сприятливі можливості);
3. Загальні стратегії реагування на ризики;
4. Стратегії реагування на непередбачені обставини.

Будь-яка стратегія цифрової трансформації має бути спрямована на управління ймовірністю ризику, або наслідками ризику, або одночасно двома даними параметрами.

Стратегії реагування на негативні ризики:

Ухилення. Ухилення від ризику передбачає зміну плану управління проектом цифрової трансформації таким чином, щоб виключити загрозу, викликану негативним ризиком, захистити мету проекту від наслідків ризику або послабити обмеження, що знаходяться під загрозою (наприклад, розширити контури розкладу або змінити зміст проекту). Деяких ризиків, що виникають на ранніх стадіях проекту, можна уникнути за допомогою уточнення вимог, отримання інформації, поліпшення комунікації або проведення експертизи.

Ризики уникаються шляхом простого невиконання частини проекту цифрової трансформації. Прикладом стратегії ухилення є використання перевіреної цифрової технології замість недавно розробленої, ще не відпрацьованої технології, що, ймовірно, допоможе уникнути технологічного ризику. Вибір постачальника з політично більш стабільного регіону знизить ймовірність того, що політичні ризики постачальника вплинуть на поставки для даного проекту. Опрацювання кількох альтернативних напрямів створення продукту на ранніх стадіях проектів цифрової трансформації, які згодом визначають ключовий напрямок, дозволить уникнути отримання продукту, який не буде відповідати цілям проекту. Наприклад, на ранніх стадіях концептуального визначення цифрової технології опрацьовуються альтернативні варіанти реалізації і згодом вибирається один – оптимальний, з точки зору команди управління проектом.

Цьому варіанту дається „зелене світло”, і проводиться детальне опрацювання. Звичайно, це не знімає повністю ймовірність того, що обраний варіант повністю забезпечить поставлені цілі проекту цифрової трансформації, проте це виключає з подальшого опрацювання свідомо неробочі варіанти. Наприклад, у разі можливого значного зсуву термінів поставок через ймовірний зрив поставок обладнання постачальником, команда проекту виключає даного постачальника з тендерного списку. Ризикова подія виключається з плану проекту, команда ухиляється від ризику.

Передача і розподіл. Передача і розподіл ризику має на увазі перекладення негативних наслідків загрози з відповідальністю за реагування на ризик на третю сторону, частково або повністю. Передача ризику просто переносить відповідальність за його управління іншій стороні, ризик при цьому не усувається. Передача відповідальності за ризик найбільш ефективна щодо фінансових ризиків. Передача ризику практично завжди передбачає виплату премії за ризик стороні, що приймає на себе ризик.

Інструменти передачі ризиків включають в себе, зокрема:

- страхування;
- гарантії виконання контракту;
- поручительства і гарантійні зобов'язання;
- прописування умов в контракті;
- інше.

Умови передачі відповідальності за певні ризики третій стороні можуть визначитися в контракті. Наприклад, на стадії укладення контракту Замовник і Виконавець обумовлюють фіксовану вартість контракту на проведення робіт. Надалі в разі підвищення вартості матеріалів і комплектуючих Виконавець покриває дані зміни з власного прибутку. Замовник же знімає з себе цей ризик.

Більш м'яким варіантом передачі є розподіл ризиків, якому приділяється все більше уваги в останні роки. За такої стратегії відповідальність за ризик несуть обидві сторони договору при реалізації проекту цифрової трансформації. Поділ ризиків між постачальником і командою проекту ініціює взаємовигідний процес удосконалення, спонукаючи постачальників до інновацій.

Послаблення. Стратегія послаблення (пом'якшення) ризиків передбачає:

- зниження ймовірності реалізації ризику;
- зниження наслідків негативного впливу ризикової події до прийнятних меж – ризик або не збудеться, або збудеться, але з меншими наслідками.

Вжиття запобіжних заходів щодо зниження ймовірності настання ризику цифрової трансформації або його наслідків часто виявляється більш ефективним, ніж зусилля щодо усунення негативних наслідків, що вживаються після настання події ризику. Як приклади заходів щодо зниження ризиків можна привести:

1. Впровадження менш складних процесів, структурне спрощення, деталізацію процесів до такого рівня, який дозволить ґрунтовно знизити ймовірність реалізації ризику. Крім спрощення процесів, ймовірність ризиків може знизити більш детальний опис процесів цифрової трансформації або застосування додаткових програм навчання персоналу проектів.

2. Проведення більшої кількості випробувань або реалізацію прототипів, на яких виробляється відпрацювання основних рішень проекту. Наприклад, при реалізації проектів цифрової трансформації можливе виділення дослідної групи або ділянки, на якому проводиться перевірка розроблених технічних цифрових рішень.

3. Вибір постачальника, поставки якого носять більш стабільний характер. Вибір може здійснюватися на підставі даних архівів минулих проєктів.

Стратегії реагування на позитивні ризики:

Використання. Ця стратегія може бути обрана для реагування на ризики з позитивним впливом, якщо необхідно, щоб дана сприятлива можливість гарантовано була реалізована.

Дана стратегія призначена для усунення всіх невизначеностей, пов'язаних з ризиком верхнього рівня, за допомогою заходів, що забезпечують появу даної слушної нагоди в різних формах. До числа заходів прямого реагування на дану можливість належать залучення до участі в проєкті цифрової трансформації більш талановитого персоналу, з тим щоб скоротити час, необхідний для його завершення, або забезпечення більш високої якості, ніж було передбачено початковим планом.

На приклад, керівник проєкту знає, що застосування більш якісних і сучасних вогнетривких матеріалів підвищить термін служби обладнання. Якщо у команди проєкту з'явиться можливість і / або ресурс на використання таких матеріалів, то вони вдадуться до них, і в результаті якісні характеристики даного проєкту підвищаться.

Спільне використання. Спільне використання позитивних ризиків передбачає передачу відповідальності третій стороні, здатній щонайкраще скористатися можливістю, що виникла, в інтересах проєкту. До числа заходів зі спільним використанням сприятливих можливостей відноситься створення партнерств зі спільною відповідальністю за ризики, команд, спеціалізованих компаній або спільних підприємств, створених спеціально для управління сприятливими можливостями.

Посилення. При застосуванні цієї стратегії змінюється „розмір” слушної нагоди шляхом підвищення ймовірності виникнення та / або конструктивного впливу, а також шляхом виявлення і максимізації основних джерел цих ризиків.

Для підвищення цієї ймовірності можна спробувати полегшити або зміцнити причину, яка викликає сприятливу можливість, і цілеспрямовано підсилити умови її появи. Можна також вплинути на джерела впливу, намагаючись підвищити чутливість проєкту до цієї слушної нагоди.

Загальні стратегії реагування на ризики:

Прийняття. Ця стратегія означає, що команда проєкту прийняла рішення не змінювати план проєкту у зв'язку з ризиком або не знайшла іншої підходящої стратегії реагування на ризики, оскільки або ймовірність ризику занадто мала, або ефект від ризику надто великий і його вплив на цілі проєкту в разі реалізації ставить під сумнів ключові цілі проєкту.

Ця стратегія може бути застосована або до загроз, або до сприятливих можливостей. Вона може бути або активною, або пасивною.

Ця стратегія використовується у випадках, коли:

виключити всі ризики з проєкту мало ймовірно;

наслідки ризику настільки великі, що недоцільно розробляти варіанти його передачі з метою зменшення впливу на проект;

ймовірність ризику і його наслідки малі, його можна прийняти, оскільки вартість розробки заходів з управління ризиком перевершує вартість наслідків.

Пасивне прийняття даної стратегії не передбачає проведення будь-яких запобіжних заходів, залишаючи команді проекту цифрової трансформації право діяти на власний розсуд в разі настання події ризику. Деякі способи реагування призначені для використання тільки в разі виникнення певних подій, тобто реалізації ризиків.

Стосовно до деяких ризиків команда проекту може задіяти план реагування на ризики, який може бути введений в дію тільки при заздалегідь визначених умовах – якщо є впевненість і достатня кількість ознак того, що даний план буде успішно виконаний. Необхідно визначити і відстежувати події, які приводять в дію механізм реагування на непередбачені обставини, наприклад, відсутність проміжних контрольних подій або привласнення певному постачальнику високого рівня пріоритетності.

Моніторинг ризиків і реалізація планів дій, в разі їх реалізації, вимагає закладання в бюджет і плани проекту резервів на ризики – резервів на відоме невідоме. Однак в будь-якому проекті буде те, що не можливо передбачити і передбачити, – „невідоме невідоме”. Для впливу на подібні події в проекті цифрової трансформації створюється управлінський резерв (бюджетний фонд), який має використовуватися командою управління проектом у разі виникнення подібних обставин.

Яку б стратегію реагування на ризик не обрало телекомунікаційне підприємство щодо проекту цифрової трансформації, план реагування на ризик і формування резервів на його забезпечення має проводитися до можливої реалізації ризику.

1.3. Механізм розвитку управління ризиками в телекомунікаційних підприємствах

Характерною рисою сучасного етапу поступу економіки є глибокі зміни, які проходять в усіх її сферах під впливом трансформаційних зрушень та глобальних перетворень. Посилення процесів нестабільності впливає на систему управління ризиками підприємств та її подальший розвиток. Враховуючи ці особливості на фоні турбулентності ринкового середовища, доцільна побудова механізму розвитку управління ризиками в телекомунікаційних підприємствах, який у процесі реалізації здатен забезпечити збалансованість бізнес-процесів й ефективне їх функціонування, що допоможе менеджменту підтримувати стійкість конкурентних позицій та ефективність функціонування підприємства через певний набір методів, інструментів, важелів, функцій та принципів.

Проблематика управління ризиками та побудови відповідних механізмів відображена в наукових розробках відомих вітчизняних вчених, таких як:

Т.Борисова, В. Вітлінський, О. Виноградова, І. Гришова, О. Гусєва, Л. Донець, О. Гудзь, Н. Євтушенко, Т. Ковальова, К. Семенова, К. Тарасова, О. Старинець, Т. Цвігун, В. Шпандарук. Високо оцінюючи їх наукові здобутки та незважаючи на масштаб накопичених по цій проблематиці знань, все ж бракує системного розгляду та обґрунтування концепту побудови механізму розвитку управління ризиками в телекомунікаційних підприємствах в нових реаліях сьогодення.

Сама категорія „механізм” запозичена з технічної термінології та давно широко використовується в різних науках та практиках.

Так в економічній літературі вчені по різному трактують поняття „механізм”, зокрема:

сукупність (або систему) формальних і неформальних правил, процедур, методів, способів, форм, важелів, функцій управління економічними відносинами різного рівня [162 с. 130];

комплексна система інструментів (правових, економічних, адміністративних, організаційних, освітніх, пропагандистських тощо), пов'язаних єдиними цілями, принципами та забезпечених відповідними ресурсами [24 с. 123];

механізм, що забезпечує взаємодію підсистеми, яка управляє, та підсистеми, якою управляють. Він складається із сукупності конкретних форм і методів свідомого впливу на економіку [35 с. 25].

Подальші дослідження механізму у контексті розвитку управління розглядаються як „механізм розвитку управління”.

Так група вчених [6] трактує механізм розвитку як спеціалізований вузол механізму управління, що забезпечує динамічну зміну конфігурацій, що склалися, та набори елементів у блоках господарського механізму.

У класичному розумінні механізм, що забезпечує процеси розвитку управління ризиками, визначається найчастіше як складова механізму управління, яка, відповідно до теорії управління, повинна об'єднувати цілі управління, критерії управління, фактори управління, методи управління [171 с. 208].

Механізм розвитку управління, за ствердженням О. В. Раєвнєвої [138, с. 226], розуміється як „сукупність: засобів управління, які включають інструменти та важелі, що відповідають орієнтирам, передбачуваним наслідкам, критеріям відбору й оцінки, обмеженням і вимогам процесу розвитку підприємства з урахуванням певної стадії циклу його розвитку; організаційних і економічних методів управління, що представляють собою способи, прийоми та технології приведення в дію та використання засобів управління” [138 с. 226].

Інший погляд на механізм розвитку управління підприємства надає О.Ю. Гаркуша [25], та характеризує його як „комплекс дій і технік організаційно-економічного характеру, спрямованих на забезпечення стійкого економічного зростання при збалансованості бізнес-процесів на основі використання певних способів, методів та інструментів управління розвитком підприємств, що відповідають специфіці їх діяльності та галузевим особливостям функціонування” [25].

Цікавий погляд на зміст механізму розвитку управління надає О.Є. Гудзь, яка розглядає його з позицій гармонізації та інноваційного розвитку у стратегічній перспективі. На думку О.Є. Гудзь, основною вимогою до формування та гармонізації механізму розвитку управління підприємства з боку системного підходу є „визначення кожного елемента системи у його зв'язку і взаємодії з іншими, виявлення впливу й властивостей її складових, визначення оптимального режиму функціонування” [38 с. 276].

Таке розуміння змісту механізму розвитку управління підсилює можливість підприємств виживати у нестабільному ринковому середовищі відповідно до цілей підприємств.

Підтримуємо підходи вчених щодо розгляду механізму розвитку управління підприємства – як сукупності дій та технік організаційно-економічного характеру, які надають можливість проектувати новий механізм функціонування із заданими властивостями під впливом різноманітних чинників, що допоможе підприємству перейти з одного стану до іншого, більш досконалого.

Зазначимо, що ефективність механізму розвитку управління підприємства, залежить від різноманітних чинників, зокрема, ступеня розвитку виробництва та раціонального споживання матеріальних ресурсів, поділу і кооперації праці, використання результатів науково-технічного прогресу, застосування інтелектуальних ресурсів, форм стимулювання та мотивації праці менеджерів та працівників підприємства тощо. Кожний зазначений чинник не створює окремого впливу на діяльність підприємства, а тільки у взаємодії з іншими, та за умов взаємного інтегрування. Застосування того чи іншого чинника без зв'язку з іншими не є доцільним. Для забезпечення стабільного економічного поступу підприємств у період несприятливих подій, необхідною складовою механізму розвитку управління вважається механізм розвитку управління ризиками.

На рисунку 1.12 наведено схему розв'язання комплексу завдань механізму розвитку управління ризиком.

Методи фінансування ризику спрямовані на компенсацію втрат і збитків, які трапляються навіть за ефективного управління ризиком, але, звичайно, такі витрати будуть меншими, ніж коли управління ризиком взагалі немає або воно неефективне [91; 111 с.66-67].

На думку Л. І. Донець механізм управління ризиком, або ризик-менеджмент (management by the risk), є специфічним видом управлінської діяльності (галуззю менеджменту), спрямованим на ефективний захист підприємства від небажаних закономірних чи випадкових обставин (подій), які у підсумку можуть негативно впливати на роботу підприємства [51].

З точки зору О. Л. Устенко механізм управління ризиком – це процес впливу на суб'єкт господарювання, при якому забезпечується максимально широкий діапазон охоплення можливих ризиків, їх обґрунтоване прийняття та зведення ступеня їх впливу до мінімальних меж, а також розробка стратегії поведінки даного суб'єкта у разі реалізації конкретних видів ризику [160].

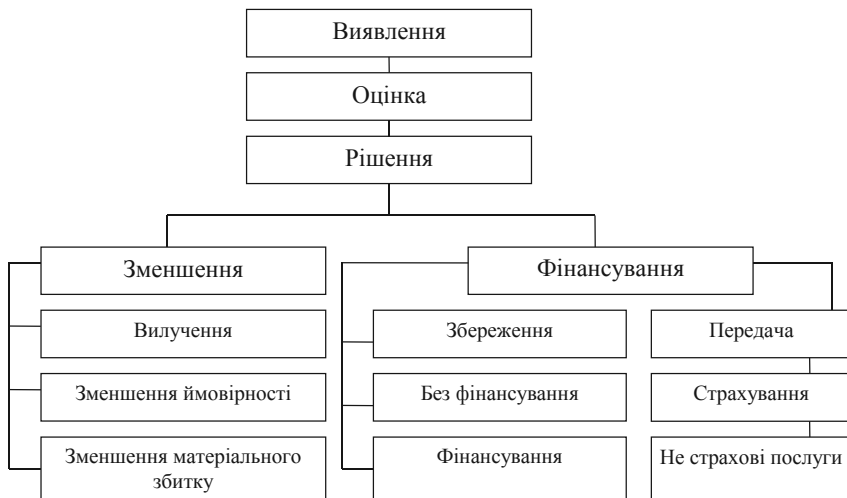


Рис.1.12. Схема розв'язання комплексу завдань механізму розвитку управління ризиком

Примітка: сформовано на основі [111 с.66-67]

Обґрунтовуючи зміст процесу управління ризиками М. Гранатуров [33 с. 7], ототожнює його із певним механізмом та характеризує механізм управління ризиком як сукупність методів, прийомів, заходів, що дозволяють певною мірою прогнозувати настання ризикованих подій і вживати заходи щодо виключення або зниження негативних наслідків їх настання.

Подібний погляд мають І.Ю. Івченко, І.П. Миколайчук та Т.В. Цвігун. Вони розглядають механізм управління ризиками як:

сукупність методів, прийомів і заходів, що дозволяють певною мірою прогнозувати настання ризикових подій і вживати заходів до їхнього зменшення (І.Ю. Івченко [84]);

сукупність структурних елементів, методів, важелів, інструментів впливу на об'єкт управління з відповідним ресурсним забезпеченням, що формується після практичної апробації системи управління ризиками підприємства (І.П. Миколайчук [109]);

сукупність принципів, методів та важелів управління, різноманітні складові підсистеми забезпечення, взаємодія та послідовність використання яких забезпечить ефективне прийняття рішень у сфері управління ризиками підприємства (Т.В. Цвігун [164]).

Іншу наукову позицію має О. Беляєв [10], яка механізм управління ризиками характеризує як цілеспрямовану практичну діяльність, що направлена на зниження ризику, зменшення потенційних матеріальних втрат та інших негативних наслідків.

Оригінальну думку на сутнісні характеристики механізму управління ризиками надає Д.А. Штефанич, який визначає цей механізм як сукупність дій економічного, організаційного і технічного характеру, спрямованих на встановлення видів, факторів, джерел ризику, оцінку величини, розробку і реалізацію заходів щодо зменшення його рівня та запобігання можливих втрат [159].

Існує окремий погляд на сутнісні характеристики механізму управління ризиками, який представлено у вигляді сукупності механізмів мінімізації ризиків, серед яких обов'язково присутні механізми нормування, планування та бюджетування, а також управління людським капіталом. Кожний окремий механізм мінімізації ризиків має свою організацію, складається з власних процесів, регулюється за допомогою конкретних форм і методів керування, а також правових норм та правил [91].

У ході проведеного дослідження щодо суті механізму розвитку управління ризиками виявились різноманітні позиції, які характеризувалися неоднозначністю підходів, що пояснюється використанням різних методичних засад. Припускаємо, що ключовою відмінністю механізму розвитку управління ризиками доцільно вважати різні процеси за об'єктом прояву. Механізм розвитку управління ризиками має прямий вплив на об'єкт, що передбачає проведення змін якісного стану об'єкту де підґрунтям для якісних змін стають інновації. Він вважається складним багатоаспектним і багаторівневим явищем, характеризується складовими, що мають різноспрямований вплив на об'єкт управління (чи побічний вплив на об'єкт управління), та передбачає наявність двох підсистем – керованої підсистеми та керуючої підсистеми.

Підтримуємо підходи тих вчених, які зміст механізму розвитку управління ризиками, розкривають як сукупність принципів, функцій, методів та важелів, що дозволять спрогнозувати настання ризикових подій, звести ступінь впливу виявлених ризиків до мінімальних та розробити стратегії виключення або зниження негативних наслідків, у разі їх настання.

З цього приводу О. М. Полінкевич [129] підкреслює, що механізм управління – це сукупність інструментів, методів та важелів, а також групи людей, які вступають у формальні і неформальні взаємодії, які направлені на досягнення мети підприємства, що є позитивом, або ж на чинення опору різним змінам, які завжди супроводжують нововведення, що часто спостерігається в трудовому колективі будь-якого підприємства і є негативним моментом.

Фактично, механізм розвитку управління ризиками має створювати стратегічні можливості підприємствам своєчасно адаптуватися у мінливих умовах сьогодення. Пропонуємо механізм розвитку управління ризиками розуміти як динамічну сукупність взаємопов'язаних субсистем, інструментів, методів та важелів, що дозволяють ідентифікувати, діагностувати та спрогнозувати настання ризикових подій, звести ступінь їх впливу до мінімуму та своєчасно розробити інноваційні стратегії здійснення організаційно-економічних змін щодо зниження негативних наслідків, у разі їх настання, системне застосування яких спрямоване на стійке економічне зростання

телекомунікаційних підприємств при збалансованості бізнес -процесів, що сприятиме укріпленню їх конкурентних позицій й підвищенню прибутковості.

Вважаємо, що доцільність механізму розвитку управління ризиками в телекомунікаційних підприємствах відповідно до траєкторій розвитку з точки зору якості впливу на господарську діяльність підприємства буде проявлятися через негативні, нейтральні чи позитивні ефекти. Зазначимо, що негативні ефекти даного механізму розвитку супроводжуються значною кількістю ризиків, які є складно керованими у часі, та які спричиняють появу незапланованих втрат та збитків. Нейтральні ефекти механізму розвитку управління ризиками характеризуються невеликою кількістю ризиків, які є керованими, та наявність яких дозволяє де який час працювати як без прибутків так і без збитків. Найбільш привабливою для підприємства є механізм розвитку управління ризиками в підприємствах з генеруванням позитивних ефектів, які за наявності керованих ризиків у процесі функціонування дозволяють отримувати прибутки з урахуванням постійної реалізації заходів щодо ефективної програми управління ризиками.

Типова блок-схема ланцюга механізму розвитку управління ризиками передбачає ідентифікацію ризиків та побудову ієрархічної мультимодульної карти ризиків, діагностику розвитку управління ризиків, фільтрацію методів та інструментів щодо мінімізації чи нейтралізації ризиків, формування ризик профілю, вибір альтернатив і стратегічних орієнтирів та забезпечення постійного моніторингу і контролінгу впливу ризикоформуючих чинників для генерування стійкості, гнучкості й надійності функціонування телекомунікаційного підприємства (рис. 1.13).

Результативність механізму розвитку управління ризиками в телекомунікаційних підприємствах залежить від композиції управління, в яку входять:

- 1) підсистема розвитку (мета; об'єкт управління; суб'єкт управління; завдання);
- 2) підсистема забезпечення (яка представлена підходами, функціями, принципами, методами, важелями та інструментами);
- 3) функціональна підсистема (включає блоки за ключовими бізнес-процесами, які знаходяться у постійній взаємодії один з одним, зокрема: операційний, фінансово-економічний, комунікаційний, технологічний, маркетинговий);

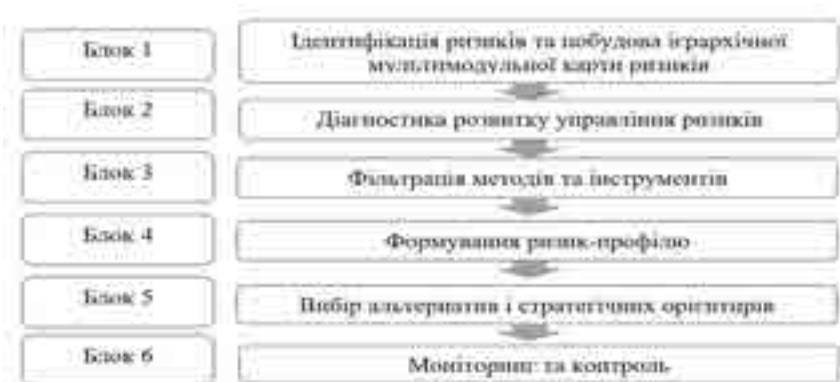


Рис. 1.13. Блок-схема ланцюга розвитку управління ризиками

Примітка: складено з використанням [35, 36, 114, 144, 164, 166].

4) процесна субсистема забезпечує процес підготовки і прийняття управлінських рішень оперативного та стратегічного характеру з врахуванням негативних, нейтральних та позитивних ефектів, що допоможе керівництву оперативно реагувати (приймати управлінські рішення та розробляти стратегії розвитку управління ризиками за обраною траєкторією) на зміни зовнішнього і внутрішнього середовища відповідно до траєкторій розвитку, що в подальшому створить умови для досягнення заданого рівня конкурентоспроможності підприємства;

5) субсистема моніторингу і контролю (спостережень і перевірки процесу функціонування підприємства).

Зміст кожної із субсистем механізму розвитком управління ризиками та кількість блоків в кожній з них залежить від типу підприємства, сфери і масштабів діяльності, ступеня впливу чинників зовнішнього середовища і результатів діяльності підприємства відповідно до обраної траєкторії розвитку управління ризиками. Концепт побудови механізму розвитку управління ризиками в телекомунікаційних підприємствах представлено на рис. 1.14. Система цілей механізму розвитку управління ризиками в телекомунікаційних підприємствах формується на основі існуючої стратегії підприємства із врахуванням можливостей та очікувань.

В умовах цифрової економіки менеджмент телекомунікаційних підприємств сприяє активному впровадженню цифрових технологій у бізнес-процеси, що призводить до підвищення ефективності функціонування, зокрема, зростання обсягів виробництва та реалізації, підвищення продуктивності праці та якості продукції (послуг), зниження собівартості, освоєння нових видів продукції (послуг), закріплення конкурентних позицій на ринку тощо. Запроваджуючи цифрові рішення, менеджмент змінює існуючі бізнес-процеси підприємств, моделі управління, переформовує комунікації, технології та організаційну структуру, ризикуючи не отримати належного результату.

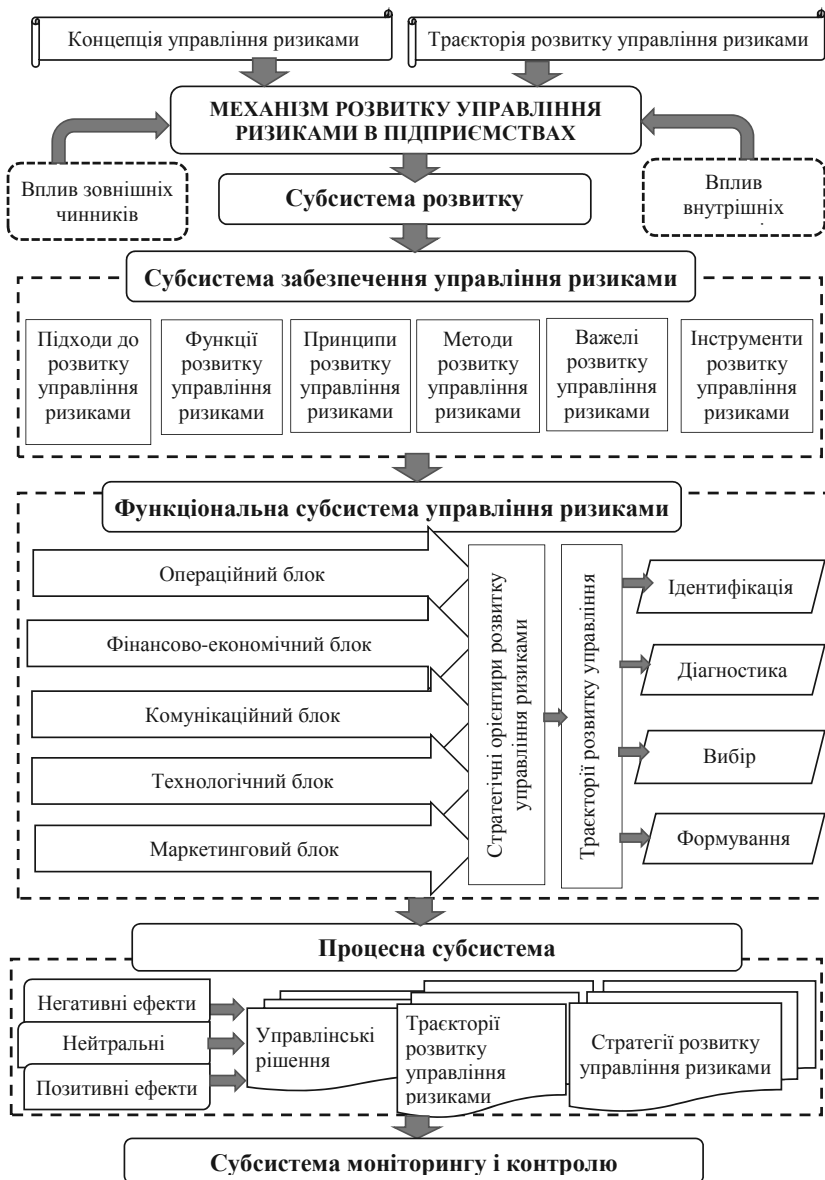


Рис. 1.14. Концепт побудови механізму розвитку управління ризиками в телекомунікаційних підприємствах

Примітка: сформовано за [35, 36, 114, 144, 164, 166].

Крім того, не треба забувати, що проведення будь яких змін у діяльності підприємства вимагає постійного залучення фінансових ресурсів та участі у програмах інвестиційного характеру. Саме тому, процес формування та реалізації механізму розвитку управління ризиками відбувається у межах наукових підходів, функцій, принципів, важелів, методів та інструментів.

Наукові підходи до формування концепту побудови механізму розвитку управління ризиками в телекомунікаційних підприємствах враховують особливості їх функціонування у:

системному зрізі, який забезпечує цілісність механізму як системи з визначеною структурою (цілі, ресурси, засоби, процеси, способи); *процесному зрізі*, який гарантує безперервність застосування адаптаційних заходів підприємства;

ситуаційному зрізі, який забезпечує постійні дослідження зовнішнього та внутрішнього середовища з метою виявлення певних закономірностей і визначення характеру поведінки підприємства у відповідній ситуації.

Таким чином, розвинуто концепт побудови механізму розвитку управління ризиками в телекомунікаційних підприємствах, принциповою відмінністю якого є врахування особливостей їх функціонування у системному зрізі (забезпечує цілісність механізму як системи з визначеною структурою (цілі, ресурси, засоби, процеси, способи), процесному зрізі (гарантує безперервність застосування адаптаційних заходів підприємства) й ситуаційному зрізі (сприяє постійному моніторингу зовнішнього та внутрішнього середовища з метою виявлення закономірностей і визначення характеру поведінки підприємства у відповідній ситуації) із включенням управлінської, функціональної, процесної, контрольної субсистем й відповідних технологічних, економічно-фінансових, організаційних, інформаційних, нормативно-регламентних інструментів й важелів та методів управління ризиками.

До функцій механізму розвитку управління ризиками в телекомунікаційних підприємствах відносять наступні:

організація – це процес створення, узгодження та виконання планів для менеджерів й виконавців, які об'єднуються з метою розробки і реалізації механізму розвитку управління ризиками;

планування – це процес постановки цільових настанов щодо управління ризиками та опрацюванні напрямів, якими підприємство буде досягати очікуваних результатів відповідно до завдань функціонування (тактика) і розвитку (стратегія);

мотивація – це процес впливу на менеджерів із управління ризиками та інших працівників підприємства з метою формування мотивів і стимулів персоналу до узгоджених та ефективних дій відповідно до цілей підприємства та особистих цілей;

контроль – систематичне спостереження та перевірка результатів діяльності підприємства у межах механізму розвитку управління ризиками, а також аналіз результатів, їх корегування та шляхи реалізації.

Принципами механізму розвитку управління ризиками в підприємствах є наступні: системності, комплексності, гнучкості, стійкості, орієнтованості на стратегічні цілі, інтегрованості, динамізму. До основної групи принципів, пропонуємо додати ті, які доповнюють розвиток управління ризиками, зокрема, інерційності, адаптивності, безперервності, пропорційності та стабілізації [56].

Системність механізму розвитку управління ризиками завжди доповнюється його комплексністю, під якою розуміється не тільки необхідність урахування та аналізу всього спектру особливостей та чинників розвитку, але й належне поєднання застосовуваних методів здійснення змін на підприємстві.

Гнучкість механізму розвитку управління ризиками передбачає стійкість, адаптацію та пристосування підприємства до змін зовнішнього середовища, можливість коригування цільових параметрів в цілому чи окремих кількісних значень, забезпечує можливостей проведення своєчасних змін в процесі управління [162 с. 164].

Інтегрованість механізму розвитку управління ризиками із загальною системою управління підприємством, є важливим чинником, оскільки управлінські рішення, безперечно, будуть здійснювати безпосередній чи непрямий вплив на зміни підприємства. В даному випадку, рішення щодо розвитку управління ризиками поєднуються в ефективну взаємодію з усіма функціональними системами управління

Високий динамізм та безперервність механізму розвитку управління ризиками в телекомунікаційних підприємствах також є важливими принципами. Специфіка передачі інформації у просторі та часі висуває відповідні вимоги стійкості до об'єктів. У той же час, динамічна реакція на можливі відхилення в ході впровадження змін на підприємстві під впливом внутрішніх та зовнішніх факторів означає гнучкість системи управління.

Інерція механізму розвитку управління ризиками проявляється в продовженні змін потенціалу системи на деякий час навіть після закінчення впливу змін у зовнішньому та внутрішньому середовищі. У свою чергу швидкість змін у механізмі розвитку управління ризиками залежить від інтенсивності поступу підприємства та його мети і стратегій. Принцип стабілізації вказує на прагнення системи стабілізувати зміни щодо управління ризиками у період зростання.

До важелів механізму розвитку управління ризиками в телекомунікаційних підприємствах відносять: економічні; правові; техніко-технологічні; інформаційно-технологічні, соціальні, управлінські; організаційні.

Вагоме значення у механізмі розвитку управління ризиком телекомунікаційного підприємства відіграє вибір і використання адекватних методів управління ризиком. Ми підтримуємо наукові позиції дослідників [65], які до ключових методів управління ризиком відносять: „запобігання (уникнення), відхилення, зниження, збереження (прийняття), передача, поділ відповідальності, використання, ігнорування” [60] (рис. 1.15).

При відборі та використанні методів управління ризиками, варто зважати на „особливості функціонування самого підприємства (організаційний дизайн, обсяги діяльності, форму власності, ступінь діджиталізації, вплив ризикоформуючих чинників тощо)” [60].

Визначаючи конкретні методи управління ризиком, слід зважати на наступні чинники:

складність операційних бізнес-процесів щодо генерування продуктів чи послуг (функції та алгоритми; адаптивність організаційного дизайну; значний неформальний вплив на персонал; великий обсяг інформаційних потоків; обмеженість часу та ресурсів);



Рис. 1.15. Методи управління ризиком

Примітка: систематизовано на основі [35, 36, 40, 51, 114, 144, 154, 164, 166, 169]

технологічні вимоги (необхідність чіткого дотримання технологічних вимог; постійна технологічна модернізація та діджиталізація бізнес-процесів; вимоги до якості продуктів та послуг);

клієнтське та зовнішнє середовище (кількість мереж, вузлів і клієнтів; ефективність процедур взаємодії із клієнтами; компетентність клієнтів та рівень їх вимог; пріоритети, виклики та вплив зовнішнього середовища; часова

обмеженість для відповідей на запити клієнтів; необхідність трансформацій процедур, взаємозв'язки із партнерами, постачальниками, субпідрядниками);

середовище функціонування підприємства (розклади, їх незмінність, хиткість та гнучкість; рівень компетенцій та стабільності кадрів; реорганізація офісів, філій та процедур; оцінка часових, ресурсних та організаційних контурів).

В принципі доцільно гармонізувати використання сукупності методів управління ризиками. Для цього доцільно скористатися певним алгоритмом, який можна використати для кожного конкретного телекомунікаційного підприємства враховуючи варіанти коливань та інтенсивності різних ризиків $\Delta\varphi_1 = 0$ і $\Delta\varphi_2 = \pi$:

$$J = \operatorname{sgn} \left\{ \left[\int_0^{2T} x(t) \sin \omega t dt \right]^2 + \left[\int_0^{2T} x(t) \cos \omega t dt \right]^2 - \left[\int_0^{2T} x(t) \sin \omega t \left(\operatorname{sgn} \sin \frac{\pi}{T} t \right) dt \right]^2 - \left[\int_0^{2T} x(t) \cos \omega t \left(\operatorname{sgn} \sin \frac{\pi}{T} t \right) dt \right]^2 \right\} \quad (1.10)$$

Передбачувані коливання:

$f_1(t) = \sin \omega t$, $f_2(t) = \cos \omega t$, $f_3(t) = \sin \omega t \operatorname{sgn} \sin(\pi/T)$, $f_4(t) = \cos \omega t \operatorname{sgn} \sin(\pi/T)$, , формуються за допомогою статистичних спостережень (Γ) і експертних оцінок на $\pi/2$, та з використанням коефіцієнтів відхилень (Π_1 і Π_2).

Порівняння доцільності гармонізації використання сукупності методів управління ризиками розглянутих алгоритмів варто робити, якщо подати алгоритм (1.10) через параметри трансформаційних перетворень (1.3) у вигляді:

$$J_n = \operatorname{sgn} [(X_{n-1} + X_n)^2 + (Y_{n-1} + Y_n)^2 - (X_n - X_{n-1})^2 - (Y_n - Y_{n-1})^2]. \quad (1.11)$$

Як переконуємось, алгоритми (1.9) і (1.11) еквівалентні.

Тобто, для визначення конкретних методів управління ризиком, слід зважати на: складність алгоритмів операційних бізнес-процесів; адаптивність організаційного дизайну; обсяг інформаційних потоків; технологічні вимоги та компоненти й рівень діджиталізації; кількість мереж, вузлів, партнерів і клієнтів; ефективність комунікаційних ланцюгів взаємодії; обмеження й виклики та пріоритети й можливості; хиткість і гнучкість зовнішнього середовища; рівень компетенцій кадрів; параметри часових, ресурсних та організаційних контурів.

Вважаємо за необхідне виділити ряд інструментів механізму розвитку управління ризиками в телекомунікаційних підприємствах:

технологічні інструменти для підвищення ефективності (компоненти цифровізації, програмні продукти);

фінансові інструменти (реструктуризації, фінансового контролінгу);

управлінські інструменти, що сприяють досягненню цілей та ефективному розвитку підприємства (проекти, плани, стратегії, методики);

кадрові інструменти, що сприяють розвитку кадрового потенціалу (обмін досвідом, перекваліфікація, навчання);

нормативно-регламентні інструменти (податкові ставки, субсидії та пільги, стандарти якості, організаційні й комунікаційні регламенти тощо).

В даних обставинах, всі заходи, що з'являться у ході реалізації концепту побудови механізму розвитку управління ризиками в підприємствах будуть спрямовані на задоволення економічних інтересів власників окремого підприємства та його працівників з метою формування максимального потенціалу підприємства в умовах невизначеності та ризику.

Однак є випадки прояву інерційності в діяльності телекомунікаційних підприємств, які проявляється у використанні застарілого обладнання, знань, організаційних структур, норм, правил тощо. Тому є необхідним організувати на підприємствах систему моніторингу та контролю, що дозволить оперативно вирішувати не тільки поточні проблеми, але й задачі стратегічної спрямованості. У цьому сенсі, механізм розвитку управління ризиками, допоможе приймати рішення щодо оптимізації співвідношення між прибутковістю та ризиком для максимізації прибутку та вартості телекомунікаційного підприємства як нині, так і на стратегічну перспективу.

Знайдемо алгоритм оптимізації співвідношення між прибутковістю та ризиком спочатку для максимізації прибутку [58, 61]. Підставивши відповідні варіанти різниць між прибутковістю та ризиком $\Delta\varphi_i = (2i - 1)\pi/4$, $i = 1, \dots, 4$, у загальний алгоритм вибору оптимальної траєкторії розвитку управління ризиками телекомунікаційного підприємства (1.6), одержимо наступні варіанти показників прибутку (при цьому множник $1/\sqrt{2}$ не враховуємо):

$$\left. \begin{aligned} a &= \cos \Delta\varphi_{n\xi} + \sin \Delta\varphi_{n\xi}, \rightarrow \Delta\varphi_n = \pi/4, \\ b &= -\cos \Delta\varphi_{n\xi} + \sin \Delta\varphi_{n\xi}, \rightarrow \Delta\varphi_n = 3\pi/4, \\ c &= -\cos \Delta\varphi_{n\xi} - \sin \Delta\varphi_{n\xi}, \rightarrow \Delta\varphi_n = 5\pi/4, \\ d &= \cos \Delta\varphi_{n\xi} - \sin \Delta\varphi_{n\xi}, \rightarrow \Delta\varphi_n = 7\pi/4. \end{aligned} \right\} \quad (1.12)$$

Кожному із отриманих варіантів показників прибутку відповідає рішення щодо передачі чи утримання ризиків, якщо ці показники прибутку більші за інші варіанти. Неважко перевірити, що такий алгоритм спрацьовує і для інших альтернатив. Таким чином, співвідношення ризику та прибутку J_{1n} и J_{2n} можна представити у наступному вигляді:

$$J_{1n} = \text{sgn} \sin \Delta\varphi_{n\xi}; \quad J_{2n} = \text{sgn} \cos \Delta\varphi_{n\xi} \quad (1.13)$$

або через використання коливань проєкції ризиків (1.3):

$$\begin{aligned} J_{1n} &= \text{sgn}(X_{n-1}Y_n - X_nY_{n-1}); \\ J_{2n} &= \text{sgn}(X_{n-1}X_n + Y_{n-1}Y_n). \end{aligned} \quad (1.14)$$

Знайдемо відповідний (1.14) алгоритм для варіанту оптимізації співвідношення між прибутковістю та ризиком для максимізації вартості телекомунікаційного підприємства. Підставивши показники різниці вартості $\Delta\varphi_i = i\pi/2$ ($i = 0,1,2,3$) в алгоритм вибору оптимальної траєкторії розвитку управління ризиками телекомунікаційного підприємства (1.6), одержимо величини:

$$\left. \begin{aligned} a &= \cos \Delta\varphi_{n\xi}, \rightarrow \Delta\varphi_n = 0, \\ b &= \sin \Delta\varphi_{n\xi}, \rightarrow \Delta\varphi_n = \pi/2, \\ c &= \cos \Delta\varphi_{n\xi}, \rightarrow \Delta\varphi_n = \pi, \\ d &= -\sin \Delta\varphi_{n\xi}, \rightarrow \Delta\varphi_n = 3\pi/2. \end{aligned} \right\} \quad (1.15)$$

У (1.15) продемонстровані рішення, котрі можуть максимізувати вартість телекомунікаційного підприємства, якщо відповідні параметри більші за інші, тобто:

$$\sin \Delta\varphi_{n\xi} + \cos \Delta\varphi_{n\xi} > 0; \cos \Delta\varphi_{n\xi} - \sin \Delta\varphi_{n\xi} < 0. \quad (1.16)$$

Таким чином, неважко перевірити, що такий алгоритм спрацює і для інших альтернатив, коли максимальними будуть a, c чи d .

Отже, відповідний алгоритм оптимізації співвідношення між прибутковістю та ризиком за максимізації вартості телекомунікаційного підприємства матиме наступний вигляд:

$$\left. \begin{aligned} J_{1n} &= \text{sgn}[(X_{n-1}Y_n - X_nY_{n-1}) + (X_{n-1}X_n + Y_{n-1}Y_n)]; \\ J_{2n} &= \text{sgn}[(X_{n-1}X_n + Y_{n-1}Y_n) - (X_{n-1}Y_n - X_nY_{n-1})]. \end{aligned} \right\} \quad (1.17)$$

При цьому загальний алгоритм оптимізації співвідношення між прибутковістю та ризиком (1.17) можна представити як:

$$J_{1n} = \text{sgn} \sin(\Delta\varphi_{n\xi} + \pi/4); J_{2n} = \text{sgn} \cos(\Delta\varphi_{n\xi} + \pi/4). \quad (1.18)$$

Таким чином, доведено, що механізм розвитку управління ризиками необхідно розуміти як динамічну сукупність взаємопов'язаних субсистем, інструментів, методів та важелів, що дозволяють ідентифікувати, діагностувати та спрогнозувати настання ризикових подій, звести ступінь їх впливу до мінімуму та своєчасно розробити інноваційні цифрові стратегії здійснення організаційно-економічних змін щодо зниження негативних наслідків, у разі їх настання, системне застосування яких спрямоване на стійке економічне зростання телекомунікаційних підприємств при збалансованості бізнес - процесів, що сприятиме укріпленню їх конкурентних позицій й підвищенню прибутковості.

Обґрунтовано, концепт побудови механізму розвитку управління ризиками в телекомунікаційних підприємствах, реалізація якого вагомо впливатиме на ефективність функціонування підприємств відповідно до його

мети та обраної стратегії поступу, що зорієнтує менеджерів та працівників підприємства на активну й цілеспрямовану діяльність направлену на підвищення їх конкурентних можливостей й зміцнення конкурентних позицій на ринку та зростання прибутків у довгостроковій перспективі, допоможе приймати рішення щодо оптимізації співвідношення між прибутковістю та ризиком для максимізації прибутку та вартості телекомунікаційного підприємства як нині, так і на стратегічну перспективу

Змістове наповнення і структура кожної із субсистем механізму розвитком управління ризиками залежить від типу телекомунікаційного підприємства, сфери, масштабів і результатів його діяльності, ступеня впливу чинників зовнішнього і внутрішнього середовища, що надасть можливість удосконалювати проектування такого механізму із заданими властивостями, що допоможе підприємству більш досконалого перейти з одного стану до іншого.

Умотивовано, що для визначення конкретних методів управління ризиком, слід зважати на: складність алгоритмів операційних бізнес-процесів; адаптивність організаційного дизайну; обсяг інформаційних потоків; технологічні вимоги та компоненти й рівень цифрової трансформації; кількість мереж, вузлів, партнерів і клієнтів; ефективність комунікаційних ланцюгів взаємодії; обмеження й виклики та пріоритети й можливості; хиткість і гнучкість зовнішнього середовища; рівень компетенцій кадрів; параметри часових, ресурсних та організаційних контурів.

1.4. Методичні підходи до діагностики розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації

Функціонування та поступ сучасного економічного простору відбувається за умов систематичної та перманентно зростаючої невизначеності. Це супроводжується ускладненням причино-наслідкових та функціональних зв'язків, турбулентністю економічної реальності та генеруванням загроз і негативних подій у діяльності телекомунікаційних підприємств. Саме тому важливим ключовим напрямом сучасної економічної науки вважається діагностика управління ризиком та його розвитку й впровадження різноманітних методичних підходів та інструментів щодо активізації та ефективності процесу розвитку управління ризиками в реаліях цифрової трансформації з метою їх нейтралізації та мінімізації.

Теоретико-методичні та практичні підходи до питань оцінки розвитку управління ризиками підприємств в реаліях цифрової трансформації описані в роботах Афанасьєва М.В., Білоконенка [5], Лук'янової В.В. [101], Гранатурова В. М., Литовченка І. В., Харічкова [34], Ковальнової Т.В., Євтушенко Н. О. [91], Лозовського О. М. [98], Лоскоріх Г.Л. [99], Супрун А.А. [154], Устенка О. Л. [160]. Незважаючи на те, що в останні роки проблема управління ризиками в реаліях цифрової трансформації виходить на провідні позиції фундаментальних досліджень, відчувається нестача уваги до

практичних аспектів діагностики розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації.

Термін „діагностика”, запозичений з медицини, де слово „діагноз” означає розпізнавання, визначення, тобто процес дослідження об’єкту діагностики задля одержання результату (діагнозу) – висновку про його стан. Загалом, діагностика розглядається з різних точок зору і трактування її не є однозначним.

Здебільшого, вчені-економісти трактують діагностику як: спосіб встановлення характеру порушень, виявлення кризових явищ та процесів, банкрутства, рівня фінансової та економічної безпеки [45]; напрям економічного аналізу, що дозволяє виявити характер порушення нормального ходу економічних процесів на підприємстві [97]; дослідження, що дозволяє не тільки всебічно оцінювати стан об’єкта в умовах неповної інформації, але й виявляти проблеми його функціонування, окреслювати шляхи їх вирішення, враховуючи коливання параметрів системи [102]. Цікаві пропозиції розроблено щодо системи оцінювання ризиків підприємства (додаток Р) та комплексної оцінки ризиків підприємства та прийняття управлінських рішень на основі результатів оцінки (додаток С).

В.В. Лук’янова стверджує: „сучасним управлінським інструментарієм є діагностика – процес розпізнавання і виявлення на основі визначених ознак (ключових оціночних показників, вивчення окремих результатів, неповної інформації) у функціонуванні об’єкта з метою оцінки наявних тенденцій і виявлення можливих перспектив його розвитку та аналізу варіантів найкращого вирішення виявлених проблем” [101].

Залежно від масштабів, мети і напрямів діагностики, а також доступної інформації та ресурсних можливостей, доцільно здійснювати: „діагностичний експрес-аналіз (найпростіша і найперша діагностична процедура), комплексний діагностичний аналіз (найскладніший вид діагностики), діагностичний аналіз функціональних напрямів (зокрема, діагностика ризиків виробництва, пов’язаних з високо ризикованим природнім середовищем), діагностичний аналіз прикладних питань, діагностику проблемних зон, діагностику в проєкті організаційного розвитку” [5].

На наш погляд, діагностика розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації – це структурований процес оцінки поточного рівня організації управління ризиками на підприємстві та досягнутого ним рівня економічної стійкості з урахуванням реалій цифрової трансформації й структурованих чинників ризику, що має на меті виявлення стратегічних пріоритетів і перспектив подальшого розвитку управління ризиками в реаліях цифрової трансформації.

Необхідність діагностики розвитку управління ризиками підприємства в реаліях цифрової трансформації для виявлення проблемних зон, не викликає сумнівів та усвідомлюється усіма дослідниками. Проте, вимоги до змісту, алгоритму її проведення, перелік об’єктів діагностики, системи показників та методології узагальнення отриманих результатів перебувають у стадії вдосконалення та неоднозначно трактуються науковцями.

На рисунку 1.16, продемонстровано загальний алгоритм діагностики розвитку управління ризиками телекомунікаційного підприємства.

Сам процес діагностики розвитку управління ризиками підприємства переважно розглядається як система елементів, призначених для перетворення вихідної інформації про стан об'єкта управління шляхом проведення діагностичних процедур на можливі рекомендації щодо зменшення негативних впливів і поліпшення (відновлення) стану об'єкта.



Рис.1.16. Загальний алгоритм діагностики розвитку управління ризиками телекомунікаційного підприємства

Примітка: сформовано за [5, 34, 91, 98, 99, 101, 154, 160].

Фактично, діагностика розвитку управління ризиками підприємства має враховувати обмеженість управлінського впливу та параметри стійкості самого підприємства, тобто варто виділити три напрями діагностики розвитку управління ризиками підприємства на різних ієрархічних рівнях (рис. 1.17).

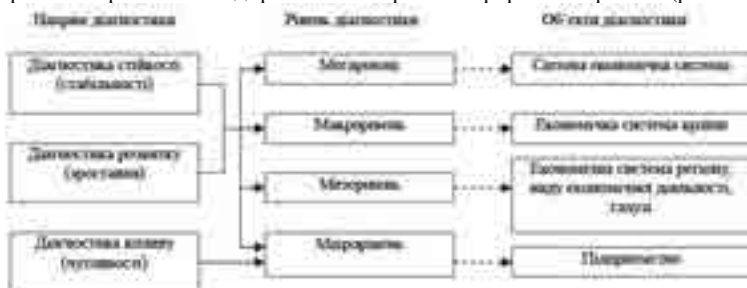


Рис. 1.17. Діагностика розвитку управління ризиками підприємства на різних ієрархічних рівнях

Примітка: сформовано за [5, 34, 91, 98, 99, 101, 154, 160].

Переконуємось, що вирішення проблеми діагностики розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації

відноситься до складних, багатокритеріальних завдань, оскільки має передбачати:

визначення тенденцій розвитку управління ризиками телекомунікаційних підприємств в Україні та побудова на цій основі багатовекторних концептуальних схем і моделей управління ризиками на усіх ієрархічних управлінських рівнях;

обґрунтування ключових чинників, які впливають на розвиток управління ризиками телекомунікаційних підприємств на мікрорівні;

діагностика ефективності розвитку управління ризиками на підприємствах з урахуванням існуючого рівня цифрової трансформації й організації управління ризиками та рівня економічної стійкості підприємств.

Ґрунтовні рекомендації щодо кількісної діагностики управління ризиками наводять В. В. Вітлінський та Г. І. Великоіваненко: „вимірювальними властивостями економічних систем повинні бути характеристики структури, стану, динаміки чи поведінки цих систем та зовнішнього середовища, котрі дають змогу в умовах невизначеності та конфлікту віднайти й деталізувати за потенційними наслідками можливі майбутні стани чи траєкторії (їх множини) поведінки певних економічних об’єктів, можливі відхилення від цілей, можливі збитки, невикористані можливості” [22 с.16].

Слід вказати, що визначення рівня стійкості підприємств і здійснення інтегральної оцінки рівня окремих її складових вже застосовується вітчизняними ученими в процесі діагностики управління ризиками.

Так, Савченко М. В. і Солоненко Ю. В. розробляючи науково-методичний підхід до управління ризиками підприємств підкреслюють, що необхідно в першу чергу визначити важливий результат функціонування підприємств, а саме стійкість [143]. Автори вказують, що стійкість є зовнішнім проявом внутрішньої структури об’єкта. А для того щоб підвищити його стійкість до впливу різних чинників ризику, необхідно, перш за все, удосконалювати сам об’єкт. Погоджуючись з ученими в плані того, що для забезпечення стійкості підприємства керівництво повинно прагнути мінімізувати ризики його діяльності, вважаємо за доцільне відштовхуватись саме від досягнутої економічної стійкості в реаліях цифрової трансформації.

На наш погляд, високий рівень економічної стійкості є головним проявом ефективного розвитку управління ризиками на підприємстві в реаліях цифрової трансформації. Оцінку рівня економічної стійкості телекомунікаційних підприємств, на наш погляд, необхідно проводити на основі визначених ключових макро-, мезо- і мікро чинників, які впливають на розвиток управління ризиками в реаліях цифрової трансформації.

Найбільш релевантною для телекомунікаційних підприємств, на наш погляд, є така 4-ох елементна система показників (додаток Т). Іншим аспектом, який повинен бути врахований при діагностиці розвитку управління ризиками телекомунікаційних підприємств, вважаємо за доцільне обрати рівень організації управління ризиками на підприємстві.

Організаційним аспектам управління ризиками присвячені дослідження Сосновської О.О., Ріщук Л.І., Гусевої О.Ю. та інших.

Означені роботи розкривають групи оціночних критеріїв для визначення ефективності управління ризиками [81], виокремлюють бізнес-процеси управління ризиками і впорядковують компоненти управління ризиками за провідними методологіями і стандартами (наприклад, COSO ERM) [195], визначають та ув'язують організаційні центри відповідальності з етапами управління ризиками на підприємстві [146] (додатки Н, П).

Отже, у сучасних умовах ключовими, на нашу думку, є два імперативи діагностики ефективності розвитку управління ризиками в реаліях цифрової трансформації (рис. 1.18).



Рис. 1.18. Імперативи діагностики ефективності розвитку управління ризиками в реаліях цифрової трансформації

Примітка: сформовано за [5, 34, 91, 98, 99, 101, 154, 160].

Узагальнення означених досліджень дозволило розвинути підходи до організації управління ризиками підприємства (табл. 1.3).

На основі визначених підходів до організації управління ризиками телекомунікаційних підприємств обґрунтовано критерії оцінки рівня розвитку управління ними і запропоновано відповідні показники для оцінки (табл. 1.4).

**Примітка. Наближення кожного із запропонованих коефіцієнтів до 1 свідчить про високий рівень організації управління ризиками на підприємстві*

Далі, в процесі обробки даних розраховуються таксономічні показники рівня розвитку підприємства, що узагальнено характеризують напрями та масштаб перетворень, пов'язаних з розвитком управління ризиками в реаліях цифрової трансформації.

На першому етапі досліджень відбувається побудова матриці розвитку окремих показників управління ризиками у часі.

Слід зазначити, що показники, які включено до матриці, є неоднорідними, оскільки описують різні властивості досліджуваного підприємства і характеризуються різними одиницями виміру.

Таблиця 1.3

Підходи до організації управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації

№	Підхід	Характеристика (складові елементи підходу)	Переваги	Недоліки
1	Реактивний	1. Система організації, планування і контролю ризиків побудована на виконанні формальних вимог Українського законодавства. 2. Інструменти і методи управління ризиками є типовими і не адаптованими до специфіки підприємства. 3. Не застосовуються сучасні програмні рішення для оцінки і прогнозування ризиків. 4. В організаційній структурі немає чітко визначених організаційних підрозділів (центрів), відповідальних за управління ризиками. 5. Корпоративна культура не орієнтована на цінності, пов'язані з розвитком схильностей до ризику та розумінням значущості управління ризиками.	- мінімальні витрати на організацію управління ризиками; - при достатньому зростанні потенціал тарифів телекомунікаційні послуги усі втрати від реалізації ризику компенсуються за рахунок додаткового прибутку.	- невизначеність рівня загроз; - невідслідковування динаміки ризикового потоку; - недостатня фіксація ризикових подій; - максимізація витрат на компенсацію збитків і страхування ризиків.
2	Стандартний	1. Система організації, планування і контролю ризиків є достатньо зрілою, проте недостатньою для ефективної протидії складним ризикам; враховано імплементації в Україні міжнародні стандарти ISO 31000:2018 та COSO; 2. Інструменти і методи управління ризиками адаптовані до специфіки підприємства; більше половини (від 50 %) ризиків розподіляються і компенсуються до появи деструктивних факторів. 3. Частково застосовуються сучасні програмні рішення для оцінки і прогнозування ризиків. 4. В організаційній структурі або на основі	- компенсація витрат на організацію управління ризиками відбувається за зростання доходів, що відбувається завдяки ідентифікації і нейтралізації більшості ризиків;	- середній (недостатньо упереджуваний) рівень визначення загроз; - несистематичний («час від часу») контроль ризиків за умов передачі функцій управління ризиками на аутсорсинг.

3	Прогресивний	<p>аутсорсингу сформовані підрозділи (центри), відповідальні за управління ризиками. 5. Корпоративна культура розвиває і підтримує цінності, пов'язані з схильностями до ризику та управління ним.</p> <p>1. Система організації, планування і контролю ризиків є динамічною та ефективною протиіде складним ризикам; враховано імплементації в Україні міжнародні стандарти ISO 31000:2018, COSO та FERMA; всі функції управління ризиками збалансовані;</p> <p>2. Інструменти і методи управління ризиками адаптовані до специфіки підприємства; більша частина (від 75 %) ризиків розподіляються і компенсуються до появи деструктивних факторів.</p> <p>3. Застосовуються програмні рішення останніх поколінь для оцінки і прогнозування ризиків.</p> <p>4. В організаційній структурі сформовані підрозділи (центри), відповідальні за управління ризиками.</p> <p>5. Корпоративна культура формує максимальну залученість усіх працівників у розумінні значущості управління ризиками.</p>	<p>- ефективність стратегічного та оперативного управління підприємством за рахунок збалансованості усіх функцій управління ризиками;</p> <p>- створення максимально сприятливих умов для безперервності і захищеності ключових бізнес-процесів.</p>	<p>- висока витрата зусиль і підтримки прогресивної системи управління і контролю ризиків.</p>
---	--------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------

Примітка: сформовано за [5, 34, 91, 98, 99, 101, 154, 160].

Таблиця 1.4

Обґрунтування критеріїв і показників оцінки рівня організації управління ризиками телекомунікаційного підприємства в реаліях цифрової трансформації

Складові елементи підходу	Критерій оцінки	Відповідний показник для оцінки та алгоритм розрахунку
Система організації, планування і контролю ризиків	Рівень збалансованості усіх елементів системи управління ризиками	Коефіцієнт нейтралізації складних ризиків ($K_{нспр}$) $K_{нспр} = \frac{РИЗ_{нс}}{РИЗ_{зс}}$ де $РИЗ_{нс}$ – кількість нейтралізованих складних ризиків за звітний період; $РИЗ_{зс}$ – загальна кількість ідентифікованих складних ризиків за звітний період.
Інструменти і методи управління ризиками	Рівень адаптивності (інноваційності, гнучкості) інструментів управління ризиками	Коефіцієнт адаптації інструментів управління ризиками до специфіки підприємства (K_{aip}) $K_{aip} = \frac{ІНР_{ад}}{ІНР_{ад} + ІНР_{тип}}$ де $ІНР_{ад}$ – кількість адаптованих (інноваційних, гнучких) інструментів управління ризиками; $ІНР_{тип}$ – кількість типових інструментів управління ризиками
Програмні рішення, що застосовуються для оцінки і прогнозування ризиків	Рівень застосування сучасних програмних рішень, для оцінки і прогнозування ризиків	Коефіцієнт автоматизації (цифровізації) оцінки ризиків (K_{aop}) $K_{aop} = \frac{РИЗ_{авт}}{РИЗ_{зс}}$ де $РИЗ_{авт}$ – кількість автоматизованих сучасними програмними рішеннями етапів оцінки ризиків; $РИЗ_{зс}$ – загальна кількість ідентифікованих етапів оцінки ризиків.
Наявність організаційних центрів, відповідальних за управління ризиками	Рівень охоплення функцій управління ризиками організаційними підрозділами	Коефіцієнт організаційної відповідальності за управління ризиками ($K_{орв}$) $K_{орв} = \frac{ФУР_{орв} + ФУР_{аут}}{ФУР_{заг}}$ де $ФУР_{орв}$ – кількість функцій управління ризиками закріплених за підрозділами підприємства; $ФУР_{аут}$ – кількість функцій управління ризиками відданих на аутсорсинг; $ФУР_{заг}$ – загальна кількість встановлених функцій управління ризиками
Спрямованість цінностей корпоративної культури на розвиток управління ризиками	Рівень підтримки працівниками культури «проактивного управління ризиками»	Коефіцієнт розвитку культури проактивного управління ризиками ($K_{пур}$) $K_{пур} = \frac{ПР_{пур}}{ПР_{заг}}$ де $ПР_{пур}$ – кількість працівників, які підтримують культуру проактивного управління змінами та відповідні цінності; $ПР_{заг}$ – загальна кількість працівників підприємства

Примітка: сформовано за [5, 34, 91, 98, 99, 101, 154, 160].

$$X_{ii} = \begin{bmatrix} x_{i1} \dots & x_{i1} \dots & x_{i1m} \\ x_{i1} \dots & x_{ii} \dots & x_{im} \\ x_{T1} \dots & x_{Ti} \dots & X_{Tm} \end{bmatrix} \quad (1.19)$$

де $t = 1, \dots, T$ - номер часового етапу;

$i = 1, \dots, m$ - номер показника збалансованої системи для підприємства, що розглядається.

Отже, в процесі проведення таксономічного аналізу виконується процедура стандартизації показників, яка призводить не тільки до елімінування одиниць виміру, а й до вирівнювання значень показників.

Під час стандартизації показників можуть вводитись коефіцієнти ієрархії, що розділяють показники за ступенем їх вагомості. Стандартизація показників з урахуванням їх змін у часі здійснюється за наступними правилами.

$$Z_{ii} = \frac{x_{ii} - \bar{x}_i}{S_i} \quad (1.20)$$

де Z_{ii} - стандартизоване значення елемента матриці x_{ii} ;

\bar{x}_i - середнє значення показника x_i у підмножині $t = 1, \dots, T$;

S_i - стандартне відхилення показника x_i .

$$\bar{x}_i = \frac{1}{T} \sum_{t=1}^T x_{it} \quad (1.21)$$

$$S_i = \left[\frac{1}{T} \sum_{t=1}^T (x_{it} - \bar{x}_i)^2 \right]^{1/2} \quad (1.22)$$

Стандартизована матриця спостережень має такий вигляд.

$$Z_{ii} = \begin{bmatrix} Z_{i1} \dots & Z_{ii} \dots & Z_{im} \\ Z_{i1} \dots & Z_{ii} \dots & Z_{im} \\ Z_{T1} \dots & Z_{Ti} \dots & Z_{Tm} \end{bmatrix} \quad (1.23)$$

Для визначення напрямку подальшого розвитку управління ризиками в реаліях цифрової трансформації доцільно використовувати таксономічний показник рівня розвитку, запропонований З. Хельвігом. У даному дослідженні показник рівня розвитку використовується для встановлення характеру та напрямку управління ризиками для підвищення економічної ефективності підприємства. В процесі оцінки рівня розвитку управління ризиками підприємства в реаліях цифрової трансформації множина обраних показників піддається диференціації в залежності від характеру впливу кожного з них на рівень розвитку досліджуваного об'єкту. Показники, які спричиняють позитивний, стимулюючий вплив на рівень розвитку об'єкту, відносять до групи стимуляторів. Відповідно, показники, що мають негативний вплив, – до групи дестимуляторів.

На основі врахування означеного впливу виділяється еталон розвитку об'єкту, який являє собою точку P_0 з координатами $Z_{01}, Z_{02}, \dots, Z_{0s}, \dots, Z_{0m}$,

$$Z_{0s} = \max_r Z_{rs}, \quad \text{якщо } s \in I \quad (1.24)$$

$$Z_{0s} = \min_r Z_{rs}, \quad \text{якщо } s \notin I \quad (1.25)$$

де I – множина стимуляторів;

Z_{rs} – стандартизоване значення показника s для часового періоду r .

Показник рівня розвитку розраховується у такий спосіб.

$$d_t = 1 - \frac{C_{t0}}{C_0} \quad (1.26)$$

де d_t – таксономічний показник рівня розвитку підприємства для часового періоду t ($t = 1, \dots, T$);

C_{t0} – відстань кожного показника у різні періоди t від його максимального (еталонного) значення.

$$C_0 = \overline{C_0} + 2S_0 \quad (1.27)$$

де $\overline{C_0}$ – середнє значення відстані C_{t0} .

$$\overline{C_0} = \frac{1}{T} \sum_{t=1}^T C_{t0} \quad (1.28)$$

$$C_{t0} = \left[\sum_{s=1}^m (Z_{ts} - Z_{0s})^2 \right]^{1/2} \quad (1.29)$$

$$S_0 = \left[\frac{1}{T} \sum_{t=1}^T (c_{t0} - \overline{c_0})^2 \right]^{1/2} \quad (1.30)$$

Розраховані у такий спосіб показники рівня економічної стійкості та рівня організації управління ризиками описують динаміку змін досліджуваних наборів показників і узагальнено ефективність розвитку управління ризиками в телекомунікаційному підприємстві в реаліях цифрової трансформації.

$$d_t = d_1, \dots, d_t, \dots, d_T \quad (1.31)$$

Інтерпретуються ці показники таким чином: чим більш наближеним є значення показника d_t до одиниці, тим більш економічно стійким і ефективнішим в плані організації управління ризиками є досліджуване телекомунікаційне підприємство у різні періоди часу і напрям (фокус) змін у такому випадку формулюється як: „Забезпечення стійкого розвитку підприємства на основі постійних покращень та удосконалень вже досягнутого високого (проактивного) рівня розвитку управління ризиками”. Значення показника d_t далеке від одиниці засвідчує низький рівень розвитку управління ризиками (тобто реактивний, який не відповідає вимогам сьогодення) і,

відповідно, вимагає принципового перегляду організаційних та економічних складових управління ризиками.

Водночас, для превентивного гальмування розгортання ризикових процесів та явищ в телекомунікаційних підприємствах необхідно виявляти, ідентифікувати та оцінювати ризики в реаліях цифрової трансформації. Доцільно це здійснювати з використанням конкретизації ієрархічної мультимодульної карти ризиків, що дасть змогу генерувати стратегічні конкурентні перспективи, забезпечити економічну сталість функціонування телекомунікаційних підприємств до агресивних впливів зовнішнього оточення. На підтримку цієї позиції Р. Каплан і Д. Нортон [186 с.169], зазначають, що „для того, щоб послідовно захищати підприємство від ризиків, необхідно чітко їх описати у форматі, що буде однозначно зрозумілим усім.

Один із таких способів опису є картографування”. Артищук І.В. [4], Рішук Л.І. [140], Супрун А.А. [154] вважають, що доцільно використовувати карту ризиків, в якій надається графічний опис та характеристика ризиків підприємства, переважно ризики розміщують у матричній таблиці, на якій наочно демонструють вагомість впливу чи значення ризику та імовірність, інтенсивність чи частоту його настання (рис. 1.19).

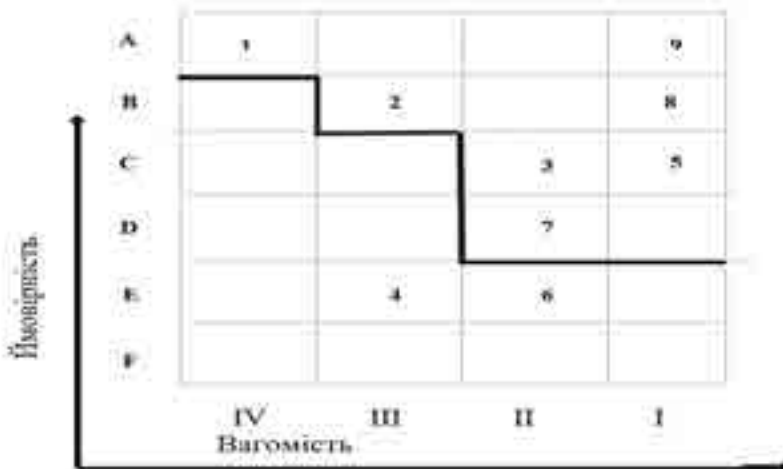


Рис. 1.19. Приклад ієрархічної мультимодульної карти ризиків

Примітка: Складено з використанням [4, 140, 154], 1- технологічні ризики; 2- ризики діджиталізації; 3- виробничі ризики; 4 – підприємницькі ризики; 5 – кібер-ризики; 6 - інвестиційні ризики; 7 – нормативно-регламентні ризики; 8 – технологічні ризики; 9 – організаційно-комунікаційні ризики.

Існують різні способи формування ієрархічної мультимодульної карти ризиків та її використання. Розглянемо принципи формування ієрархічної мультимодульної карти ризиків. Принцип побудови *m*-позицій ризиків дуже

простий: m сигнальні точки ризиків розташовуються в прямокутній таблиці, залежно від потужності та інтенсивності впливу з інтервалом $2\pi/m$.

Якщо вектори сигнальних точок ризиків, співпадають із іншими відрізками векторів, прирівнюються до кореня квадратного із інтенсивністю сигналу: $R = \sqrt{E}$. Якщо вектором відображається гармонійне коливання з відхиленням $a, \omega i \varphi$, то їх параметри дорівнюють:

$$R = \sqrt{E} = \sqrt{\int_0^T a^2 \sin^2(\omega t + \varphi) dt} = \frac{a\sqrt{T}}{\sqrt{2}}. \quad (1.32)$$

Відстань впливу між двома гармонійними сигналами ризиків S_1 і S_2 тривалістю T , які різняться за інтенсивністю на φ :

$$d(S_1, S_2) = \sqrt{\int_0^T [S_1(t) - S_2(t)]^2 dt} = \sqrt{\int_0^T [a \sin(\omega t + \varphi) - a \sin \omega t]^2 dt} = \sqrt{a^2 T - a^2 T \cos \varphi} = \sqrt{2E} \sqrt{1 - \cos \varphi}, \quad (1.33)$$

де $E = a^2 T / 2$. Ймовірність похибки залежить від комунікаційних сигналів в підприємстві в цілому. Однак для конкретної конфігурації сигнальних точок ризиків імовірність похибок вважається монотонно спадаючою функцією. Мінімальна відстань у такій композиції:

$$d_8 = ab = \frac{\sqrt{E} \sin 2\pi/7}{\cos \pi/7} \approx 0.86\sqrt{E}. \quad (1.34)$$

Не зважаючи на деякі недоліки, цей спосіб формування ієрархічної мультимодульної карти ризиків та її використання широко використовується в зарубіжних компаніях. Для знаходження і порівняння інтенсивності й потужності впливу сигналів ризиків, доцільно виходити з середньої їх потужності. Середня і максимальна інтенсивність сигналу ризиків (IP):

$$E_{cp}(IP) = E_{\max}(IP) = E. \quad (1.35)$$

Середня інтенсивність і потужність ризику (ПП) проявляється через альтернативи:

$$E_{cp}(ПП) = \frac{1}{9} \sum_{i=1}^9 E_i. \quad (1.36)$$

Максимальна інтенсивність і потужність ризику в телекомунікаційних підприємствах має місце в сигналах ризиків 2, 5, 8 і 9:

$$E_2 = E_5 = E_8 = E_9 = E_{\max}. \quad (1.37)$$

Інтенсивність і потужність ризику інших сигналів матимуть вигляд для E_{\max} :

$$E_1 = E_3 = E_4 = E_6 = E_{\max} / 3;$$

Тобто, об'єднавши (1.36) та (1.37), одержимо:

$$E_{cp}(АФМ) = (2 + \sqrt{5})E_{\max} / 6. \quad (1.38)$$

Прирівнюючи (1.35) і (1.38), маємо:

$$E_{\max} = \sqrt{6/(2 + \sqrt{5})} \sqrt{E} \approx 1.19 \sqrt{E}. \quad (1.39)$$

Розрахунки переконують, що для випадку різної інтенсивності і потужності сигналів ризику при обмеженості середньої потужності впливу матимемо:

$$\sqrt{E_{\max}} \approx 1.2 \sqrt{E}; \quad d_{16}(AFM) \approx 0.58 \sqrt{E}. \quad (1.40)$$

Зауважимо, що цей принцип формування ієрархічної мультимодульної карти ризиків та її використання не вважається повністю оптимальним, однак він допомагає формувати оптимальну ризикостійкість.

Ієрархічна мультимодульна карта ризиків, дозволяє наочно продемонструвати місце, роль і значення конкретного ризику відносно діяльності телекомунікаційного підприємства та формує передумови щодо ефективного управління ним в реаліях цифрової трансформації.

Загалом, мультимодульна карта ризиків сприяє систематизації ризиків підприємства за пріоритетами, вагомістю, інтенсивністю та дає змогу якісно їх ідентифікувати. Інструментами при формуванні карти ризиків можуть бути: інтерв'ю, анкетування, формалізовані і неформалізовані опитувальники, спеціально зібрана інформація, дослідження тенденцій галузі, економічний моніторинг звітів підприємства тощо.

Важливими завданнями формування мультимодульної карти ризиків вважаються: виявлення критичних чи катастрофічних ризиків, визначення контурів управлінського впливу та ресурсних можливостей для цього, сприяння формуванню команди, окресленню часових горизонтів і пріоритетів, розробці альтернативних сценаріїв, прогнозів та плану заходів і моделюванню.

Опираючись на узагальнення наявних методичних підходів щодо діагностики управління ризиками підприємства в реаліях цифрової трансформації, як засобу виявлення та ідентифікації й оцінки кризових явищ та процесів, представляємо організаційний контур діагностики розвитку управління ризиками телекомунікаційних підприємств (рис. 1.20).

Таким чином, для ефективного функціонування телекомунікаційного підприємства необхідно постійно розглядати ризикоформуючі чинники, вчасно їх ідентифікувати та здійснювати комплексну діагностику ризиків, що витікають зі специфіки діяльності телекомунікаційного підприємства та на підґрунті отриманої діагностики ухвалювати рішення щодо оптимального пакету варіантів управління ризиками в реаліях цифрової трансформації.

З'ясовано, що для превентивного гальмування розгортання ризикових процесів та явищ в телекомунікаційних підприємствах необхідно виявляти, ідентифікувати та оцінювати ризики за допомогою здійснення діагностики та побудови ієрархічної мультимодульної карти ризиків

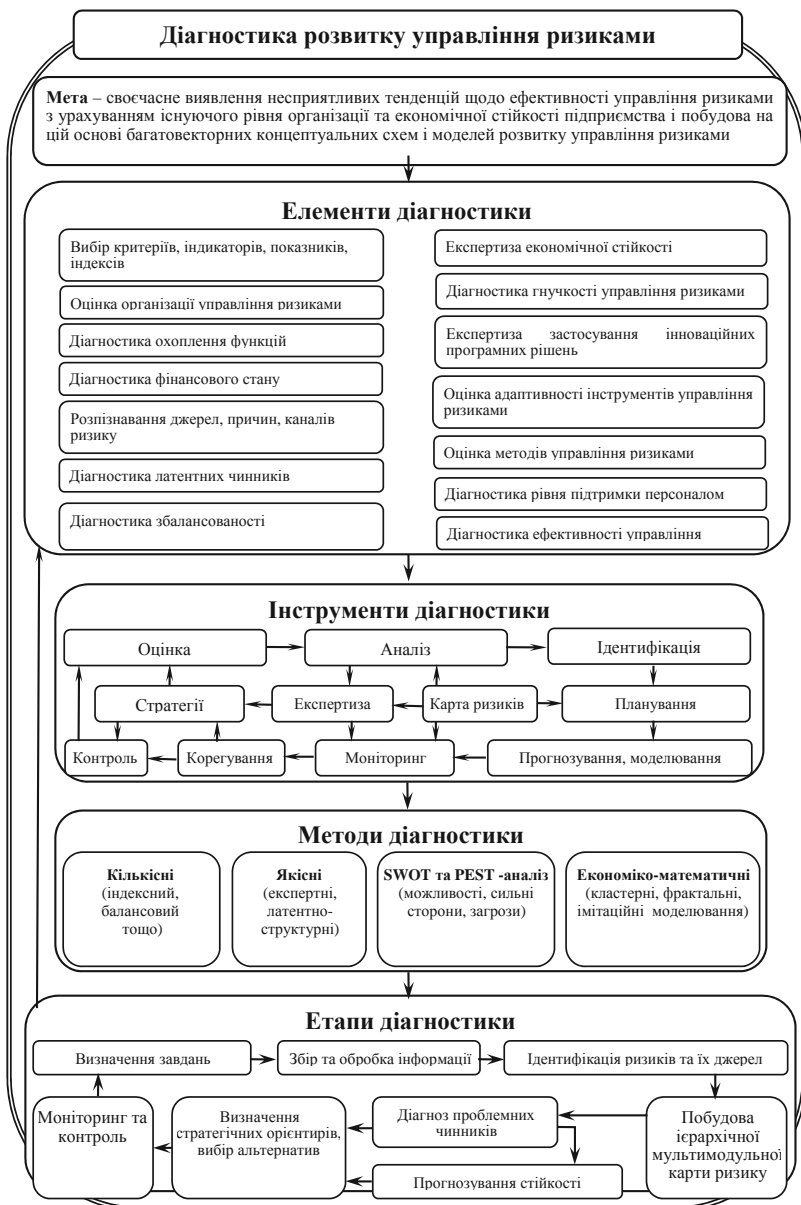


Рис. 1.20. Організаційний контур діагностики розвитку управління ризиками телекомунікаційних підприємств Примітка: сформовано за [5, 34, 91, 99, 154, 160].

Встановлено, що діагностика розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації – це структурований процес виміру й аналізу досягнутого рівня управління ризиками з урахуванням економічної стійкості підприємства з метою виявлення можливостей та визначення стратегічних орієнтирів і перспектив подальшого розвитку управління ризиками в умовах цифрової економіки, що являється складним багатокритеріальним завданням.

Обґрунтовано організаційний контур й релевантність її здійснення з використанням ключових макро-, мезо- і мікро чинників, які впливають на розвиток управління ризиками на основі 4-ох елементної системи показників та розрахунків таксономічних індикаторів й критеріальної оцінки рівня розвитку з відповідними оціночними індексами, що дає змогу окреслити динаміку змін досліджуваних наборів показників, побудувати ієрархічну мультимодульну карту ризиків та визначити ефективність розвитку управління ризиками в телекомунікаційному підприємстві.

Якісною відмінністю розроблених пропозицій щодо діагностики розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації вважаємо те, що він дає змогу, на підставі обґрунтованих інструментів, методів, етапів діагностики, запропонованих коефіцієнтів та їх нормативних значень, шляхом застосування методу вирішення багатокритеріальних задач, своєчасно передбачити ризикові явища та обрати оптимальні механізми і методи їх нейтралізації чи мінімізації.

Побудова й конкретизація ієрархічної мультимодульної карти ризиків, з використанням інтерв'ю, анкетування, формалізованих і неформалізованих опитувальників, спеціально зібраної інформації, досліджень тенденцій галузі, економічного моніторингу звітів підприємства тощо, дозволяє наочно продемонструвати місце, роль і значення конкретного ризику, сприяє якісній ідентифікації й систематизації ризиків підприємства за пріоритетами, вагомістю, інтенсивністю, виявленню критичних чи катастрофічних ризиків, визначенню контурів управлінського впливу та ресурсних можливостей, окресленню часових горизонтів і пріоритетів, розробці альтернативних сценаріїв, прогнозів та плану заходів і моделюванню, що дасть змогу мати своєчасну об'єктивну ідентифікацію про стан ризикозахищеності телекомунікаційних підприємств в реаліях цифрової трансформації та моделювати альтернативні траєкторії розвитку для досягнення бажаних результатів, організувати відповідну команду, генерувати стратегічні конкурентні переваги й забезпечити економічну сталість функціонування телекомунікаційних підприємств до агресивних впливів зовнішнього оточення.

РОЗДІЛ 2

ПРАКТИЧНІ АСПЕКТИ РОЗВИТКУ УПРАВЛІННЯ РИЗИКАМИ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ

2.1. Тенденції розвитку управління ризиками телекомунікаційних підприємств

Нині, характерним для телекомунікаційних підприємств вважається диверсифікація послуг та продуктів, орієнтація на розширення аудиторії споживачів, загострення конкурентної боротьби. Відповідно, кожне телекомунікаційне підприємство стикається з багатьма ризиками, і підприємства, які управляють ризиками отримують конкурентні переваги. Для виявлення тенденцій розвитку управління ризиками в телекомунікаційних підприємствах, у відповідності до розробленого методичного підходу та зважаючи на те, що вагомий вплив мають кібер-ризиками, доцільно використати міжнародні індекси рівня розвитку цифровізації. До основних таких показників відносять індекс розвитку електронного уряду, індекс відкритості державних даних, індекс розвитку ІКТ [29]. У таблиці 2.1 представлений узагальнений аналіз цих індексів.

Таблиця 2.1

Рейтинг України за міжнародними індексами розвитку цифровізації

Показники	Рейтинг України	Загальна кількість країн для оцінки
Індекс розвитку електронного уряду (EGDI)	82	193
Індекс відкритості державних даних (GODI)	32	134
Індекс розвитку ІКТ (ICT)	79	176
Глобальний інноваційний індекс (GII)	47	131

■ Загальна кількість країн для оцінки □ Рейтинг України

Примітка: побудовано на основі [29, 197]

Згідно проведених досліджень ООН (United Nations E-government Survey 2018) за індексом розвитку електронного уряду (EGDI - E-Government Development Index) Україна займає 82 місце із представлених для оцінки 193 країн. Треба відзначити, що за результатами даної оцінки Україна має „високий” рівень показника EGDI – індексу розвитку електронного уряду.

[197]. Індекс розвитку електронного уряду (EGDI) є добутком середньозважених значень оцінок трьох найбільш важливих елементів формування електронного уряду, а саме: обсягу і якості онлайн-обслуговування, стану розвитку телекомунікаційної інфраструктури і оцінки формування людського капіталу.

Проведене дослідження ООН стимулює до покращення тенденцій підвищення рівнів цифрового розвитку телекомунікаційних підприємств. Світовими лідерами за індексом розвитку електронного уряду завдяки високому ступеню захисту від цифрових ризиків та синтезу використання людського капіталу і он-лайн технологій є такі країни, як: Данія, Австралія, Південна Корея, Фінляндія, Сінгапур, Нова Зеландія, Франція і Японія.

За світовим рейтингом відкритості державних даних Global Open Data Index серед 134 досліджуваних країн Україна займає 31 місце. Уряд України і підприємства активують політику і дії у напрямку прогресивного розвитку відкритості інформаційного простору нашої країни. За проведеною оцінкою Україні 20% даних мають відкритий характер – інформація щодо формування і виконання Державного бюджету, законодавчі нормативно-правові акти, реєстри підприємств та суб'єктів підприємництва.[183].

За оцінкою Міжнародного союзу електрозв'язку (підрозділ ООН) індексу розвитку ІКТ (ICT Development Index – IDI), Україна посідає посереднє місце у рейтингу і займає 79 місце серед 176 досліджуваних країн [174]. На жаль, Україна, не зважаючи на постійний розвиток інформаційно-комунікаційних технологій істотно відстає за індексом розвитку ІКТ від сусідніх європейських країн – Польщі, Угорщини, Молдови, Словаччини та Румунії.

Ще одним важливим міжнародним показником рівня розвитку цифрових трансформацій є Глобальний інноваційний індекс (GIІ – The Global Innovation Index), який проводить Всесвітня організація інтелектуальної власності. За Глобальним індексом інновацій Україна займала 47 місце серед 131 країн світу [196]. Глобальний індекс інновацій формується на основі системи показників щодо інноваційних можливостей країн і чинників зовнішнього середовища діяльності бізнесу – політичного середовища, рівня освіти, інфраструктури та перспективних можливостей для функціонування бізнесу. Найбільш інноваційними країнами, за проведеними дослідженнями є Швейцарія, США, Нідерланди та Велика Британія.

Проведений аналіз цифрових трансформацій в Україні та її місця на міжнародній арені підтверджує наявність позитивних тенденцій побудови відкритого інформаційного суспільства, впровадження інновацій, технологій і інших результатів цифрових трансформацій. Виявлене, пояснює активізацію інтеграції вітчизняних телекомунікаційних підприємств у світовий глобальний інформаційний простір. Фактично, телекомунікаційні підприємства, переходять у нову якісну парадигму цифрового розвитку на засадах збалансованого використання ресурсів, оптимізації і мобільності прийняття управлінських рішень задля мінімізації чи нівелювання наростаючих загроз та ризикових процесів.

Відповідно до Державного класифікатора видів економічної діяльності ДК 009:2010, у секції J „Інформація та телекомунікації” виокремлено розділ 61 „Телекомунікації (електрозв’язок)”, до якого входить „діяльність із надання телекомунікаційних та інших супутніх послуг, таких як передавання голосових, текстових, звукових або відеоданих” [50].

В сучасних кризових умовах діяльності, для всебічного дослідження особливостей розвитку управління ризиками телекомунікаційних підприємств, доцільно провести більш детальний аналіз їх стану, соціально-економічних показників, що дозволить виявити чинники впливу й розвитку, проблеми, окреслити перспективні напрями активізації та стратегічні орієнтири управління ризиками. Дане дослідження було проведено на основі вивчення інформації Державної служби статистики України щодо секції J „Інформація та телекомунікації”.

Так, за даними Державної служби статистики України, в роботі була проаналізована динаміка кількості суб’єктів господарювання телекомунікаційної галузі у 2010-2021 роках (табл. 2.2).

Таблиця 2.2

Динаміка кількості суб’єктів господарювання телекомунікаційної галузі України у 2010-2021 рр.

Рік	Кількість суб’єктів господарювання						
	усього				у тому числі фізичні особи-підприємці		
	суб’єкти великого підприємництва	суб’єкти середнього підприємництва	суб’єкти малого підприємництва	з них суб’єкти мікропідприємництва	суб’єкти середнього підприємництва	суб’єкти малого підприємництва	з них суб’єкти мікропідприємництва
2010	9	410	55558	53441	1	42787	42713
2011	10	431	53798	51544	2	39865	39796
2012	13	413	66142	63808	2	53118	53043
2013	12	411	85954	83709	5	71487	71405
2014	6	379	113970	112019	5	101031	100906
2015	6	342	115788	113997	4	102515	102467
2016	6	335	129363	127631	4	117768	117698
2017	6	328	146575	144765	4	133492	133368
2018	7	335	174280	172354	2	160105	159934
2019	9	360	190230	203795	5	190230	190078
2020	8	348	15698	13912	1	218133	218034
2021	9	364	16011	14239	1	267756	267642

Примітка: складено основи [118].

Здійснена діагностика за кількісним складом телекомунікаційних підприємств засвідчує, що у 2020 р. їх кількість становила 234188 [118], причому у 2010 році частка юридичних осіб складала 23,56%, або 13189 підприємств, а вже у 2020 році – лише 6,86%, що вказує на наявність значної кількості дрібних посередників, тобто відбувається суб’єктне здрібнення телекомунікаційної сфери. Так, кількість великих телекомунікаційних

підприємств, практично не змінилась, кількість середніх телекомунікаційних підприємств та суб'єктів малого підприємництва продовж досліджуваного періоду знизилась на 11% і 71% відповідно. Динаміка темпів зміни кількості суб'єктів господарювання телекомунікаційної галузі України у 2010-2020 рр. продемонстрована на рисунку 2.1.

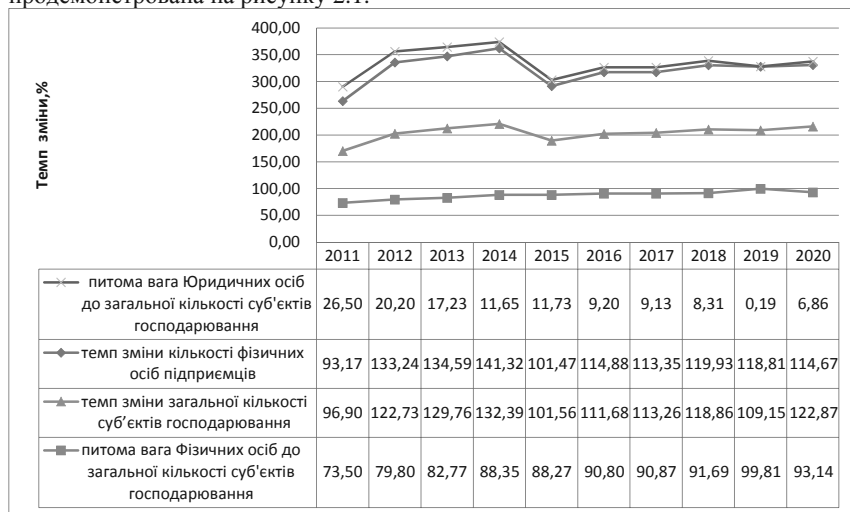


Рис.2.1. Динаміка темпів зміни кількості суб'єктів господарювання телекомунікаційної галузі України у 2010-2020 рр.

Примітка: складено на основі [118].

Навний низхідний тренд кількості телекомунікаційних підприємств зумовлює виникнення додаткових ризиків в телекомунікаційній сфері, зокрема, що пов'язані зі складністю контролю за дотриманням положень нормативно-правових актів, впровадженням діджиталізації, зменшенням податкових платежів до бюджету, зниженням якості телекомунікаційних послуг тощо.

Важливо наголосити, що вітчизняні телекомунікаційні підприємства функціонують за умов олігополізації ринку, підтвердженням цього є те, що вагома частка обсягу телекомунікаційних послуг припадає лише на 7 великих телекомунікаційних підприємств. При цьому, цікаво, що кількість персоналу в телекомунікаційних підприємствах розподіляється за кожною категорією підприємств майже рівномірно. Динаміка кількості телекомунікаційних підприємств і їх працівників за 2012-2021 рр. наведена на рисунку 2.2. Враховуючи встановлену тенденцію падіння кількості зайнятих працівників, при стабільній кількості підприємств, вважаємо доцільним проаналізувати матеріальну мотивацію найманих працівників.

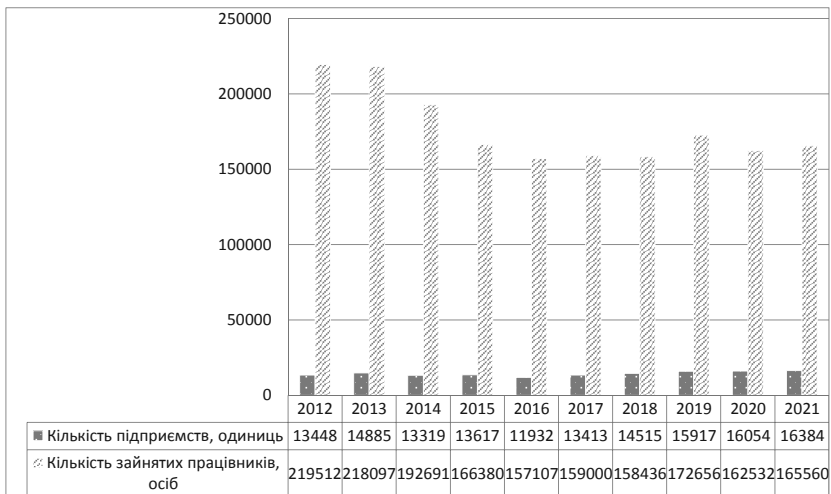


Рис. 2.2 Динаміка кількості телекомунікаційних підприємств і їх працівників за 2012-2021 рр.

Примітка: складено на основі [118].

Дослідження динаміки витрат на оплату праці в телекомунікаційних підприємствах за 2011-2021 рр. представлено у таблиці 2.3.

Таблиця 2.3

Динаміка витрат на оплату праці в телекомунікаційних підприємствах

Рік	Сфера телекомунікацій			Середньомісячна заробітна плата по Україні, грн	Відношення середньомісячної заробітної плати у сфері телекомунікацій до середньої заробітної плати по Україні, %
	Загальні витрати на оплату праці, тис. грн	Середньомісячна заробітна плата, грн	Темп росту середньомісячної заробітної плати, %		
2011	8854083,0	3188,77	113,00	2648	120,42
2012	9980373,3	3788,85	118,82	3041	124,59
2013	10625697,7	4060,00	107,16	3282	123,71
2014	10810353,8	4675,17	115,15	3480	134,34
2015	12215256,1	6118,15	130,86	4195	145,84
2016	14513159,7	7698,13	125,82	5183	148,53
2017	18717913,1	9810,23	127,44	7104	138,09
2018	22437161,7	11801,38	120,30	8865	133,12
2019	26592278,9	13986,87	118,52	10497	133,25
2020	36971461,3	17844,47	127,58	11591	153,95
2021	42716945,8	21901,81	122,74	14014	156,28

Примітка: розраховано авторами на основі [118]

За представленими даними у таблиці 2.3 продовж 2011-2021 років спостерігалось поступове зростання середньомісячної заробітної плати в телекомунікаційних підприємствах відповідно до темпів зростання середньомісячної заробітної плати в країні. Дане зростання середньомісячної заробітної плати за досліджуваний період складає у межах 15 – 25% щорічно. При цьому рівень середньомісячної заробітної плати у телекомунікаційних підприємствах вищий за аналогічний рівень середньої заробітної плати по Україні на 20-40% у 2011-2019 роках і на 55% за 2020 та 2021 роки. Все це вказує на високе матеріальне заохочення працівників в телекомунікаційних підприємствах. Отже, на наш погляд, скорочення чисельності працівників пов'язано з вивільненням частини трудових ресурсів у зв'язку з активним розвитком штучного інтелекту і впровадженням цифрових трансформацій.

Наступним етапом дослідження розвитку управління ризиками телекомунікаційних підприємств став аналіз динаміки показників телекомунікаційних підприємств зрівняно із іншими підприємствами економіки України за 2010-2021 роки. (табл. 2.4).

Таблиця 2.4

Аналіз динаміки показників телекомунікаційних підприємств зрівняно із іншими підприємствами економіки України за 2010-2021 роки

Рік	Загальна кількість підприємств, од	Кількість телекомунікаційних підприємств	Частка телекомунікаційних підприємств, %	Загальна кількість найманих працівників, осіб	Кількість найманих працівників телекомунікаційних підприємств, осіб	Частка працівників телекомунікаційних підприємств, %
2010	378810	13189	3,48	7836443	230998	2,95
2011	375695	14372	3,83	7712429	228799	2,97
2012	364935	13448	3,69	7577595	216181	2,85
2013	393327	14885	3,78	7285562	214593	2,95
2014	341001	13319	3,91	6192987	189583	3,06
2015	343440	13617	3,96	5778120	162275	2,81
2016	306369	11932	3,89	5713871	154171	2,70
2017	338256	13413	3,97	5714585	155782	2,73
2018	355877	14515	4,08	5870601	155069	2,64
2020	373897	16054	4,3	7379539	162532	2,2
2021	370834	16384	4,42	7368718	165560	2,2

Примітка: розраховано авторами на основі [118]

Представлені дані у таблиці 2.4 є стабільними упродовж досліджуваних 2010-2021 років. Так, з 2010 року частка телекомунікаційних підприємств поступово збільшилась з 3,48 % до 4,42 % у 2021 році. Частка найманих працівників в телекомунікаційних підприємствах, за цей період, поступово зменшилась, а саме з 2,95 % у 2010 році до 2,2 % у 2021 році.

Розвиток управління ризиками в телекомунікаційних підприємствах опирається на всебічне дослідження їх фінансових результатів. Тому, доцільно проаналізувати доходність і прибутковість телекомунікаційних послуг та

частку прибутків телекомунікаційних підприємств у загальних фінансових результатах діяльності підприємств країни. Проаналізовано дані показники за основними видами послуг, які надають телекомунікаційні підприємства споживачам. Так, у 2016-2020 роках телекомунікаційні підприємства демонстрували динамічний розвиток, а їх доходи мали висхідні тренди (рис. 2.3).

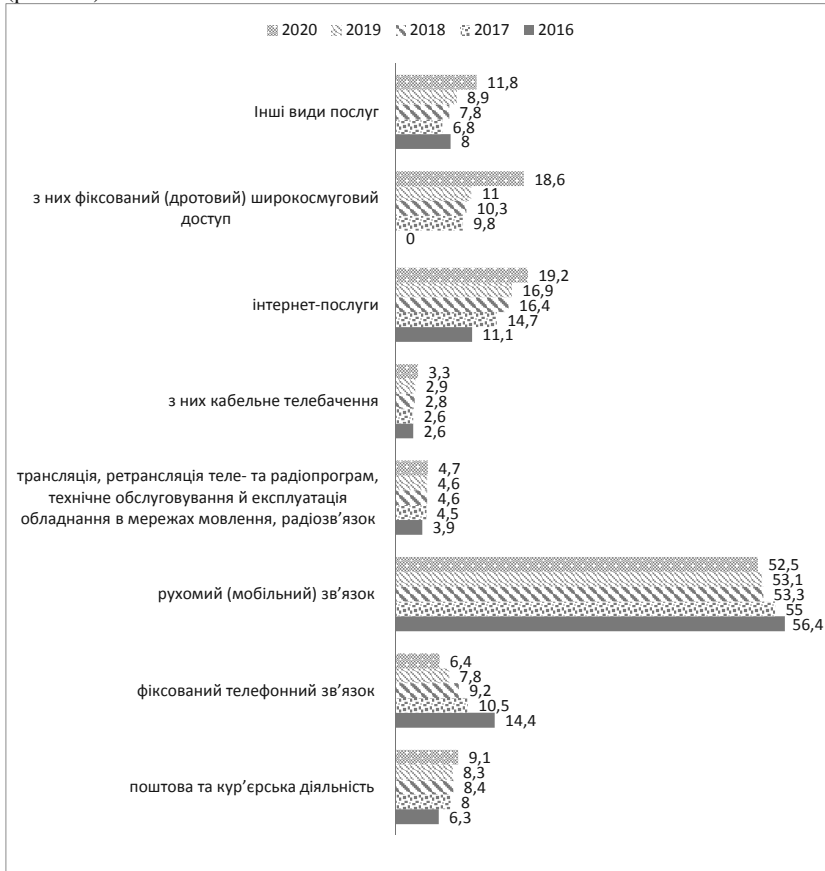


Рис. 2.3. Динаміка структури доходів телекомунікаційних підприємств України у 2016-2020 рр.

Примітка: розраховано авторами на основі [118]

Водночас, сукупний обсяг доходів телекомунікаційних підприємств становив у 2020 році вже 71598,5 млн. грн.

Стабільними є й висхідні тренди доходів від надання інтернет-послуг; трансляції, ретрансляції теле- та радіопрограм, технічного обслуговування й експлуатації обладнання в інформаційно-комунікаційних мережах мовлення; поштової та кур'єрської діяльності.

Всі ці напрями реалізуються в рамках Стратегії цифрового розвитку України і задач поставлених Міністерством цифрових трансформацій світового розвитку даної галузі і відповідно до державного регулювання України [62, 92]. На рисунку 2.3 видно, що обсяги доходів від послуг рухомого (мобільного) зв'язку протягом досліджуваного періоду займають найбільшу частку у загальній структурі доходів телекомунікаційних підприємств.

У 2020 році вони займали 52,5 %. Водночас, попит на послуги з фіксованого телефонного зв'язку з кожного роком знижується. Так у 2016 році, частка сукупного доходу від цього виду послуг склала 14,4 %, у 2020 році цей показник знизився до 6,4 %.

Аналіз доходів і витрат телекомунікаційних підприємств за 2017-2021 роки представлено у таблиці 2.5.

Таблиця 2.5

Аналіз доходів і витрат телекомунікаційних підприємств
за 2017-2021 роки

Показник	2017 рік	2018 рік	2019 рік	2020 рік	2021 рік	Темп росту 2021 до 2017 рр.
Доходи						
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	138187,4	165744,1	197363,0	217306,6	270768,5	195,94
Інші операційні доходи	13834,3	13469,9	11119,7	13457,5	12427,2	89,83
Інші доходи	4899,4	7107,3	8976,2	6153,4	7584,2	154,80
Разом чисті доходи	156921,1	186321,4	217459,1	236937,4	290780,0	185,30
Витрати						
Операційні витрати	133288,1	157727,3	179174,4	198927,2	242309,0	181,79
Інші витрати	8437,6	10413	13445,7	21029,2	14468,4	171,48
Витрати усього	144891,8	171645,3	196841,8	222428,2	263523,0	181,88
з них собівартість реалізованої продукції (товарів, робіт, послуг)	94435,5	112759	134477,3	153380,1	193418,9	204,82
Чистий прибуток (збиток)	12029,3	14676	20617,3	14509,2	27257,0	226,59

Примітка: розраховано авторами на основі [118]

Нарощення сукупних доходів від надання телекомунікаційних послуг, що зумовлено зростанням попиту на них, пояснюється наступним:

забезпечення якісного мобільного зв'язку через розвиток телекомунікаційних мереж по усій території нашої країни;

зростання клієнтського попиту на мультимедійні конвергентні сучасні телекомунікаційні послуги;

високий рівень затребуваності сучасних інформаційно-комунікаційних технологій для діджиталізації бізнес-процесів широкого кола підприємств з різних галузей;

розповсюдження і перевод деяких бізнесових аспектів підприємств у віртуальне середовище.

Представлені показники доходів і витрат телекомунікаційних підприємств (табл. 2.5) підтверджують позитивну динаміку розвитку ефективності діяльності даних підприємств. Так, упродовж досліджуваного періоду з 2017 року чистий дохід від реалізації продукції (товарів, робіт, послуг) телекомунікаційних підприємств збільшився практично у два рази, але при цьому операційні доходи скоротились. У 2017-2021 роках також збільшили і витрати підприємств даної сфери, однак ці витрати були оправдані для отримання додаткових доходів і у 2021 році чистий прибуток зріс майже на 127%.

Динаміка рівня рентабельності телекомунікаційних підприємств України у 2015-2021 рр. продемонстрована на рисунку 2.4.

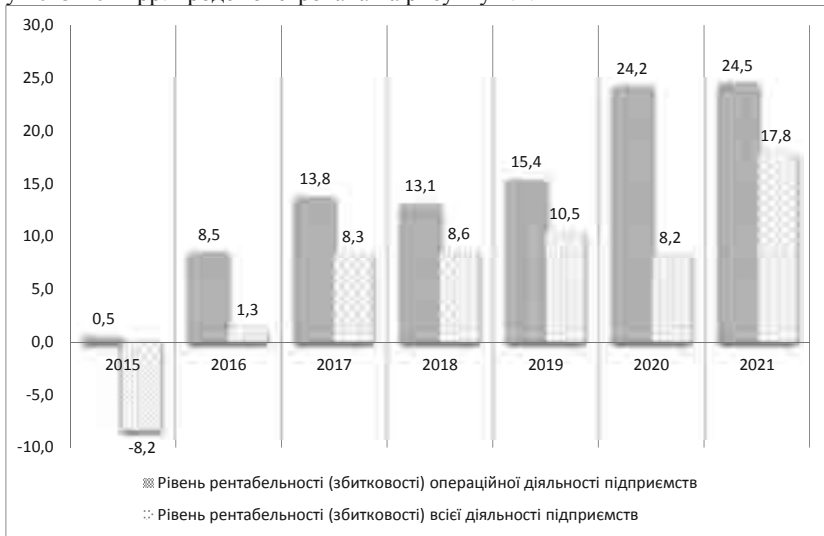


Рис. 2.4. Динаміка рівня рентабельності телекомунікаційних підприємств України у 2015-2021 рр.

Примітка: розраховано авторами на основі [118]

Треба зазначити, що у сукупності, у 2015 року телекомунікаційні підприємства були збитковими. У 2015 році рівень збитковості склав 8,2%, у 2021 році цей показник набув прибутковості і рентабельність

телекомунікаційних підприємств значно зростає до рівня 17,8%. Результат проведеного дослідження говорить про статистичну пропорцію між прибутковими телекомунікаційними підприємствами і збитковими. Так, наприклад за досліджуваний період 71,6 % телекомунікаційних підприємств були прибутковими.

Разом з проаналізованими показниками доцільно провести оцінку фінансової незалежності телекомунікаційних підприємств. Узагальнені результати даного напрямку дослідження за 2017-2021 роки, наведені у таблиці 2.6 та продемонстровано на рисунку 2.5.

Таблиця 2.6

Аналіз фінансової незалежності телекомунікаційних підприємств за 2017-2021 роки

Показник	Рік				
	2017	2018	2019	2020	2021
Індекс автономії	0,414	0,088	0,191	0,226	0,263
Індекс покриття власним капіталом позикового капіталу	0,705	0,097	0,346	0,292	0,356

Примітка: розраховано на основі [118]

Треба зазначити, що на телекомунікаційних підприємствах України спостерігається зниження фінансової незалежності.

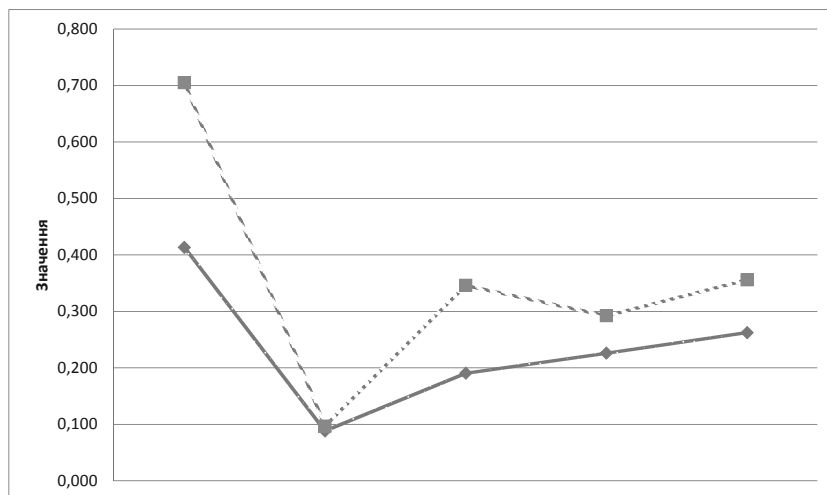


Рис.2.5. Динаміка фінансової незалежності телекомунікаційних підприємств України у 2017-2021 роки

Примітка: розраховано на основі [118]

Про це свідчать показники – індекс автономії і індекс покриття власним капіталом. Станом на 2021 рік порівняно з 2017 роком індекс автономії знизився більше ніж на третину, а індекс покриття власним капіталом позикового капіталу відповідно знизився майже вдвічі.

Узагальнюючи отримані результати дослідження, щодо функціонування телекомунікаційних підприємств України, можна стверджувати, що вони набувають перспективного і важливого значення для України і є прибутковими. У процесі аналізу офіційних статистичних даних та вивчення аналітичних матеріалів стану телекомунікаційних підприємств встановлено, що їх послуги користуються високим попитом, що зумовлено зростанням рівня їх доходності.

Вітчизняні телекомунікаційні підприємства мають позитивні тенденції ефективної діяльності і рухаються до світової інтегративної розвинутої системи цифрових трансформацій. Цьому сприяє розвиток глобальної мережі інтернету, організація впровадження широкосмугового та високошвидкісного доступу до нього для бізнесу і населення.

Треба відзначити, що будь-яка сучасна соціально-економічна організація діяльності суб'єктів господарювання різних форм власності та населенням практично неможлива без сучасних інформаційно-телекомунікаційних послуг. При цьому це стосується багатьох сфер: охорони здоров'я, освіти, сільського господарства, торгівлі, фінансів, управління комунальним господарством.

Телекомунікаційні послуги виступають необхідним посередником обслуговування таких важливих сфер життєдіяльності, як банківська діяльність, охорона та безпека, моніторинг транспорту та логістика, промисловість, сільське господарство, енергетика тощо.

Згідно плану заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки наша країна впроваджує наступні напрями цифрових трансформацій, які безпосередньо стосуються телекомунікаційних підприємств [92]:

- нормативно-правове та організаційно-методичне забезпечення розвитку;
- розвиток пріоритетних напрямів цифровізації і телекомунікаційних послуг, зокрема;

- виробництво і розвиток експорту цифрових технологій;
- цифровізація пріоритетних та соціально-орієнтованих сфер життєдіяльності;

- розвиток цифрових компетенцій, грамотності та навичок громадян;
- розвиток цифрових інфраструктур взаємодії держава-бізнес-населення.

Отже, в цілому телекомунікаційні підприємства України мають позитивні тенденції та перспективи, а саме в розвитку мобільного зв'язку в країні і за її межами, доступу до мережі Інтернету, забезпечення відкритості інформації та організацію цифровізації важливих соціально-орієнтованих сфер життєдіяльності – охорони здоров'я, освіти, логістики, державного регулювання.

Проте, в телекомунікаційних підприємствах є і багато проблемних аспектів, які потребують вирішення задля досягнення стратегічного розвитку і ефективності.

Основними проблемами телекомунікаційних підприємств вважаються [90]: нерівномірність забезпечення споживачів телекомунікаційними послугами особливо в сільській, гірській місцевостях, в тому числі загальнодоступними телекомунікаційними послугами широкосмугового доступу до Інтернету; ресурсна обмеженість в умовах кризових ситуацій і нестабільності ринкового оточення; насиченість ринку і високі якісні затребування споживачів; недостатня ефективність управління ризиками телекомунікаційною мережею загального користування України.

Опираючись на проведені дослідження, можна стверджувати, що розвиток управління ризиками в телекомунікаційних підприємствах, пов'язаний з ресурсними обмеженнями, тобто важливою умовою є отримання прибутків і ефективності їх діяльності, оскільки розвиток управління ризиками істотно залежить від кількості та обсягів наявних ресурсів – інтелектуальних, енергетичних, матеріальних, фінансових та інформаційних.

Розвиток управління ризиками в телекомунікаційних підприємствах у високо конкурентному середовищі залежить від гостроти конкуренції та вимог споживачів до якості і вартості телекомунікаційних послуг, які надаються. Тому, основними індикативними параметрами розвитку управління ризиками повинні бути мобільність, гнучкість та унікальність продукту, а стратегії розвитку управління ризиками мають враховувати основні вимоги внутрішнього та глобального телекомунікаційних ринків. Розвиток управління ризиками, внаслідок глобалізації ринків, має враховувати, також, композицію побудови інфраструктури та комунікацій, логістичних ланцюгів та необхідності формування єдиних інформаційно-комунікативних мереж автоматизації та діджиталізації економічної діяльності. Розвиток управління ризиками в телекомунікаційних підприємствах залежить від безпекових заходів та зовнішньополітичного оточення, що пов'язано з існуючими можливими кібератаками на ресурси, інфраструктурні системи та технології, використанням не сумлінних інструментів конкурентної боротьби та цифровізації великих даних, ресурсів і інформації.

2.2. Ключові чинники впливу на розвиток управління ризиками телекомунікаційних підприємств

Розвиток управління ризиками в телекомунікаційних підприємствах залежить від чіткого виявлення впливу та взаємозв'язків різноманітних чинників на ці процеси, коли визначені кількісні параметри ризиків і коли менеджер, який ухвалює управлінські рішення, може контролювати поточний стан процесів і затверджувати відповідні заходи опираючись на об'єктивну інформацію. Оскільки ідеальних рішень щодо розвитку управління ризиками поки що не існує, усі ризикові явища та процеси повинні безперервно вивчатися

для виявлення слабких місць і недоліків, для розробки прийомів та методів, спрямованих якщо не на повне усунення, то принаймні на зменшення кількості цих слабких місць та неефективності. Складність, невизначеність та нестабільність умов функціонування телекомунікаційних підприємств, що було підтверджено даними у підрозділі 2.1, хаотичність зміни чинників, що їх формують, призвели до загострення прояву кризових процесів та зумовили виникнення економічних деформацій в телекомунікаційних підприємствах.

Розуміння керівниками й менеджерами внутрішніх можливостей телекомунікаційних підприємств створює передумови для розвитку управління ризиками та розробки відповідних напрямів активізації та стратегічних орієнтирів, адекватних викликам зовнішнього середовища. Виходячи з цього, можливості телекомунікаційних підприємств протистояти негативному впливу чинників значною мірою визначаються рівнем їх внутрішньої стійкості до ризиків, тобто, спроможності телекомунікаційних підприємств протистояти різного роду ризикам, що дозволяє визначити їх потенційну здатність досягти запланованих результатів, забезпечити сталий поступ за несприятливого впливу будь-яких ризиків в умовах нечіткого середовища.

З метою оцінки внутрішньої стійкості до ризиків телекомунікаційних підприємств визначимо основні параметри та сформуємо відповідну систему індикаторів оцінки. Для формування системи показників оцінки впливу ключових чинників на розвиток управління ризиками телекомунікаційних підприємств було залучено експертів – керівників та фахівців телекомунікаційних підприємств. В експертну групу увійшли 23 фахівця провідних телекомунікаційних підприємств м. Києва та Київської області, з них 73% становили керівники інституційного рівня та 27% – керівники управлінського рівня. Середня вікова категорія експертів – 48 років, серед них – 12 жінок та 11 чоловіків, зі стажем роботи на керівній посаді до 3 років – 23%, 3-5 років – 37% та понад 5 років – 40%. Розподіл за рівнем освіти свідчить, що з числа експертів – 80% складають керівники з повним вищим рівнем освіти, 15% – з неповним вищим рівнем освіти та 5% – з середнім спеціальним. Кожному респонденту було запропоновано заповнити анкету, в якій необхідно було висловити власну думку щодо включення показників у систему, на основі яких можливе встановлення „слабких сигналів”, які можуть вплинути на порушення стійкості до ризику телекомунікаційних підприємств (додаток У).

Експертне опитування проводилося за методом Делфі. Даний метод є одним із найпоширеніших методів анкетування. Згідно з методом Делфі, кожен експерт отримує спеціально розроблену анкету з питаннями, яку заповнює незалежно від інших. Відповіді експертів підсумовують та разом із узагальненими безособовими аргументами на користь тих чи інших оцінок повертають експертам для уточнення чи зміни, якщо вони знайдуть це необхідним, своїх первісних відповідей [107, 116]. Перевагою застосування методу Делфі у межах нашого дослідження є забезпечення незалежності думок фахівців, що надає можливість через кількісну форму, сформувати систему показників. На основі результатів анкетування було встановлено, що

основними параметрами оцінки ризикостійкості телекомунікаційних підприємств є такі напрями: фінанси, персонал, матеріально-технічна база, маркетинг, інновації, за кожним з яких визначено основні індикатори оцінки та сформовано групи чинників впливу (рис. 2.6).

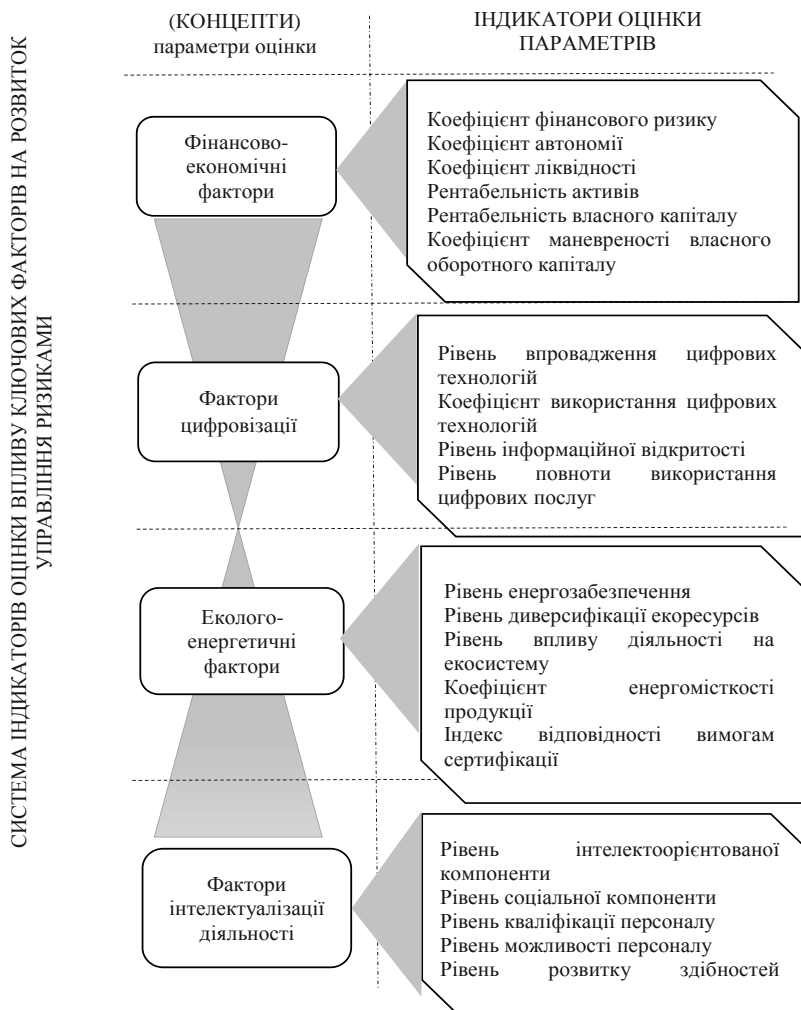


Рис. 2.6. Система індикаторів оцінки впливу ключових чинників на розвиток управління ризиками в телекомунікаційних підприємствах

Примітка: розроблено на основі [64, 172]

Водночас, експерти акцентували, що розроблена система індикаторів оцінки ключових чинників впливу на розвиток управління ризиками телекомунікаційних підприємств, на відміну від існуючих, повинна враховувати галузеву специфіку за концептами (фінансово-економічні чинники, чинники цифровізації, еколого-енергетичні чинники, чинники інтелектуалізації діяльності), що дозволить на основі встановленого рівня внутрішньої ризикостійкості до вказаних груп чинників визначити розвиток та можливості досягнення високих економічних результатів телекомунікаційними підприємствами.

Апробацію, сформованої системи індикаторів оцінки впливу ключових чинників на розвиток управління ризиками, було здійснено на телекомунікаційних підприємствах, а саме: ПрАТ „Київстар”, ПрАТ „ВФ Україна”, АТ „Укртелеком”, ТОВ „Lifese1”. За результатами апробації зроблено висновок, що розвиток управління ризиками зазначених підприємств гальмується через недостатнє використання значної частини ресурсного та інтелектуального потенціалів та порушення стійкості їх економічного функціонування, що актуалізує питання деталізованого аналізу параметрів впливу ключових чинників. Проведені розрахунки індикаторів оцінки концепту „Фінансово-економічні чинники” (додаток Ф1) впливу на розвиток управління ризиками дозволили дійти висновку, що в цілому практично для всіх телекомунікаційних підприємств характерне погіршення значень індикаторів оцінки фінансової складової внутрішньої стійкості до кризи.

З метою детального аналізу цього концепту було розраховано індикатори, що характеризують ліквідність та платоспроможність, їх фактичні значення були зіставлені з нормативними. Аналіз результатів проведених розрахунків на телекомунікаційних підприємствах (рис. 2.7) дозволяє зробити висновок, що значення коефіцієнта маневреності власного оборотного капіталу на досліджених телекомунікаційних підприємствах перебуває на рівні нижче нормативного значення (0,1), що свідчить про недостатність власних фінансових ресурсів для фінансування необоротних активів та частини оборотних. Проблеми забезпечення фінансової стійкості характерні для трьох підприємств з чотирьох досліджених, а саме: ПрАТ „Київстар”, ПрАТ „ВФ Україна”, ТОВ „Lifese1”, оскільки значення коефіцієнта маневреності власного оборотного капіталу має негативне значення. Для вирішення цієї проблеми, даним телекомунікаційним підприємствам необхідно розробити заходи щодо збільшення частки власних коштів. Аналізуючи значення коефіцієнта автономії (що показує потенційний рівень свободи при прийнятті рішень, розподілі доходів, а також можливості залучення додаткових коштів під потреби підприємства) на телекомунікаційних підприємствах, можна зробити висновок про те, що підвищення коефіцієнта автономії у 2020 році АТ „Укртелеком” та ТОВ „Lifese1” свідчить про те, що дані підприємства все більше покладаються на власні джерела фінансування, а також покращення їх фінансового стану. Але саме у ТОВ „Lifese1” показник фінансового ризику більше 1 (нормативне значення < 1), що свідчить про значні фінансові ризики.

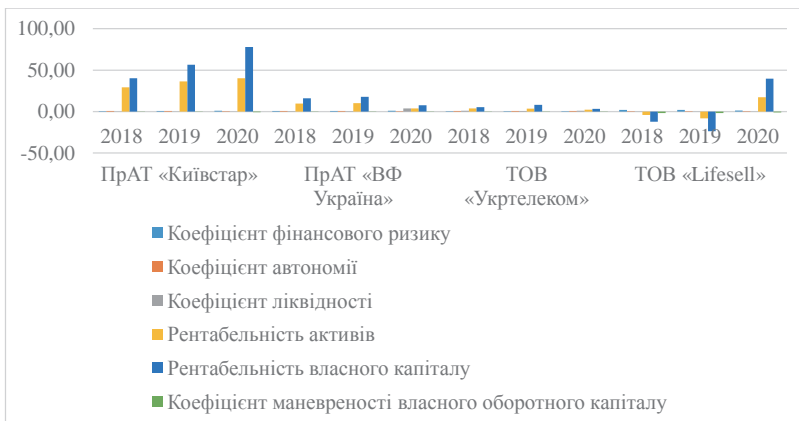


Рис. 2.7 Значення індикаторів оцінки концепту „Фінансово-економічні чинники” досліджуваних телекомунікаційних підприємств за 2018-2020 рр.
Примітка: складено авторами на основі розрахунків додатку Ф1.

Як відомо, для досягнення сучасних бізнес-компетенцій при розвитку управління ризиками, керівникам телекомунікаційних підприємств необхідно швидко реагувати на зміни ринку та здійснювати заходи для подальшого впровадження телекомунікаційних мереж наступного покоління. Саме тому нами було виокремлено таку концепту впливу як „Чинники цифровізації”, аналіз якої дозволяє зробити висновки щодо забезпечення розвитку мультисервісних телекомунікаційних транспортних мереж для задоволення потреб споживачів телекомунікаційних послуг. Для розрахунку були використані індикатори, графічне зображення яких представлено на рисунку 2.8.

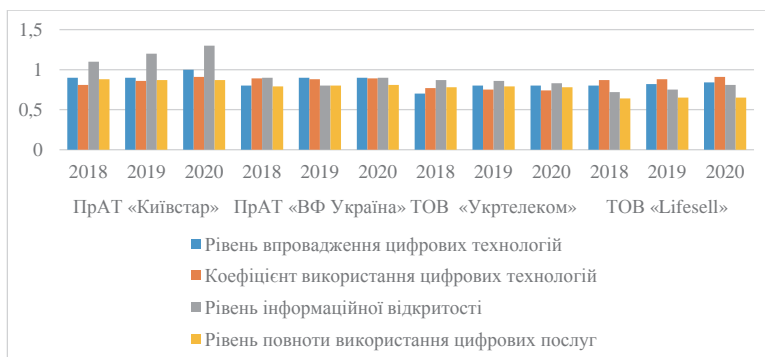


Рис. 2.8. Значення індикаторів оцінки концепту „Чинники цифровізації” досліджуваних телекомунікаційних підприємств за 2018-2020 рр.
Примітка: складено автором на основі розрахунків додатку Ф2.

Значення індикаторів концепти „Чинники цифровізації” дозволили зробити висновки, що досліджуваним підприємствам необхідно використовувати найбільш ефективні технології у сільській, гірській місцевості і депресивних регіонах. Це дозволить уникнути ризику зниження процесів цифровізації в діяльності телекомунікаційних підприємств, котрі в свою чергу спрощують роботу з масивами інформації, підвищують рівень прозорості, збільшують ємність і пропускну спроможність мереж та надають можливість вчасно приймати оптимальні управлінські рішення щодо забезпечення оптимізації витрат, створення комфортних умов для споживачів продукції та сформуванню позитивного іміджу підприємства.

Також у процесі дослідження, було з'ясовано чинники та межі зміни пропорцій між економічним зростанням та енергоспоживанням, що підтверджують, що вагомим чинником впливу на розвиток управління ризиками телекомунікаційних підприємств є еколого-енергетичні чинники, що, в свою чергу, знайшло відображення в системі індикаторів оцінки впливу ключових чинників на розвиток телекомунікаційних підприємств. Значення показників по цьому концепту відображено на рисунку 2.9.



Рис. 2.9. Значення індикаторів оцінки концепту „Еколого-енергетичні чинники” досліджуваних телекомунікаційних підприємств за 2018-2020рр.

Примітка: складено авторами на основі розрахунків додатку Ф3.

В процесі діагностики, було зроблено висновок, що досліджувані телекомунікаційні підприємства мають низькі показники по концепту „Еколого-енергетичні чинники”, що передбачає оновлення і модернізацію телекомунікаційної мережі, впровадження технологічних і продуктових нововведень, які зможуть забезпечувати відповідність міжнародним стандартам енергозбереження та охорони здоров'я (стандарти e-health), в результаті якого можна відзначити поліпшення показників ефективності функціонування і пріоритет потенціалу підприємства.

Практика телекомунікаційних підприємств щодо управління ризиками та їх оцінки свідчить, що найбільш цінним активом стає інтелектуальний

потенціал телекомунікаційних підприємств, який надає можливість телекомунікаційним підприємствам накопичити міцні конкурентні переваги на мінливому конкурентному ринку товарів та послуг в даний час та пристосуватись до конкурентних змін у майбутньому. За результатами експертного оцінювання, як зазначалося раніше, було виокремлено індикатори оцінки концепту „Чинники інтелектуалізації діяльності” телекомунікаційних підприємств, коливання яких за 2018-2020 рр. графічно зображено на рисунку 2.10.



Рис. 2.10. Значення індикаторів оцінки концепту „Чинники інтелектуалізації діяльності” досліджуваних телекомунікаційних підприємств за 2018-2020 рр. Примітка: складено авторами на основі розрахунків додатку Ф4.

Аналізуючи дані, наведені на рисунку 2.10, зазначимо, що майже всі визначені підприємства активно оновлюють інтелектуалі ресурси та технології, що виступають міцним ядром щодо розвитку управління ризиками телекомунікаційних підприємств. Також зазначимо, що АТ „Укртелеком” значно знизило ефективність управління за кожною складовою критерією оцінки.

З огляду на те, що ми використовували широкий спектр індикаторів, які мають бути враховані щодо рівня впливу чинників на розвиток управління ризиками телекомунікаційних підприємств, доцільно визначити інтегральний показник рівня внутрішньої стійкості до впливу чинників на розвиток управління ризиками (KFDR), який формується з урахуванням локальних інтегрованих оцінок за кожним параметром впливу чинників, відповідно: фінансово-економічні чинники, чинники цифровізації, еколого-енергетичні чинники, чинники інтелектуалізації діяльності.

Такий підхід дозволить визначити стан окремих параметрів впливу, з метою ідентифікації „вузьких місць” у діяльності телекомунікаційних підприємств, що сприятиме деталізації процесу розробки комплексу заходів щодо мінімізації чи нівелювання ризиків за певними параметрам впливу чинників на розвиток управління ризиками.

Для інтегрованої оцінки параметрів впливу чинників на розвиток управління ризиками варто використати наступний показник:

$$K_j = \sum_{k=1}^n \mathcal{L}_k [1 - \gamma_{of}]^{-l}$$

де: K_j – інтегрована оцінка j -го параметра впливу чинника на розвиток управління ризиками;

\mathcal{L}_k – значимість k -го індикатора оцінки j -го параметра впливу чинника на розвиток управління ризиками;

γ_{of} – стандартизоване значення k -го індикатора оцінки j -го параметра впливу чинника на розвиток управління ризиками, який розраховується за формулою:

$$\gamma_{of} = (\gamma_i - \gamma_{\min}) / (\gamma_{\max} - \gamma_{\min}) \quad (2.2)$$

де: γ_i – фактичне значення i -го індикатора оцінки j -го параметра фінансово-економічних чинників, чинників цифровізації, еколого-енергетичних чинників, чинників інтелектуалізації діяльності у k -му періоді, коеф.;

$\gamma_{\max}, \gamma_{\min}$ – відповідно максимальне та мінімальне значення i -го індикатора оцінки j -го параметра фінансово-економічних чинників, чинників цифровізації, еколого-енергетичних чинників, чинників інтелектуалізації діяльності у k -му періоді, коеф.

З метою діагностики внутрішніх можливостей щодо підвищення розвитку управління ризиками, на основі використання вищевказаних формул (2.1 та 2.2) розраховано інтегровані показники параметрів, що описують ключові чинники впливу на розвиток управління ризиками за концептами фінансово-економічних чинників, чинників цифровізації, еколого-енергетичних чинників, чинників інтелектуалізації діяльності. Результати проведених розрахунків наведено у таблиці 2.7.

Таблиця 2.7

Значення інтегрованих оцінок внутрішніх можливостей щодо підвищення розвитку управління ризиками телекомунікаційних підприємств (за концептами) у 2019-2020 роках, (коеф.)

Назва підприємства	Концепти впливу ключових чинників на розвиток управління ризиками							
	Фінансово-економічні чинники		Чинники цифровізації		Еколого-енергетичні чинники		Чинники інтелектуалізації діяльності	
	2019р.	2020р.	2019р.	2020р.	2019р.	2020р.	2019р.	2020р.
ПрАТ „Київстар”	0,771	0,706	0,872	0,896	0,415	0,488	0,647	0,743
ПрАТ Україна” „ВФ	0,682	0,692	0,816	0,837	0,455	0,373	0,634	0,741
АТ „Укртелеком”	0,68	0,597	0,766	0,732	0,464	0,523	0,437	0,329
ТОВ „Lifesell”	0,453	0,538	0,782	0,812	0,321	0,354	0,611	0,701
Середнє значення	0,647	0,633	0,809	0,819	0,414	0,435	0,582	0,629

Примітка: складено авторами на основі розрахунків

Розглядаючи результати представлених вище інтегрованих оцінок, слід відмітити, що максимальне значення характерно для концепту „Чинники цифровізації” (0,819). При цьому найбільше значення цієї інтегрованої оцінки відзначається у ПрАТ „Київстар” – 0,896, а найменше в АТ „Укртелеком” – 0,732.

Слід відмітити, що найменше значення отримано за концептом „Еколого-енергетичні чинники” (0,414). Якщо керівники підприємств звернуть увагу на цей індикатор, то в процесі впровадження новітніх технологій, будуть враховувати захист довкілля від негативного впливу діяльності телекомунікаційних підприємств. А це в свою чергу, є одним із стійких напрямів розвитку телекомунікаційних підприємств за рахунок виробництва і пропозиції ринку нових інтернет-послуг і власних пакетних (конвергованих) телекомунікаційних послуг.

Графічна інтерпретація проведених розрахунків представлена на рисунку 2.11.

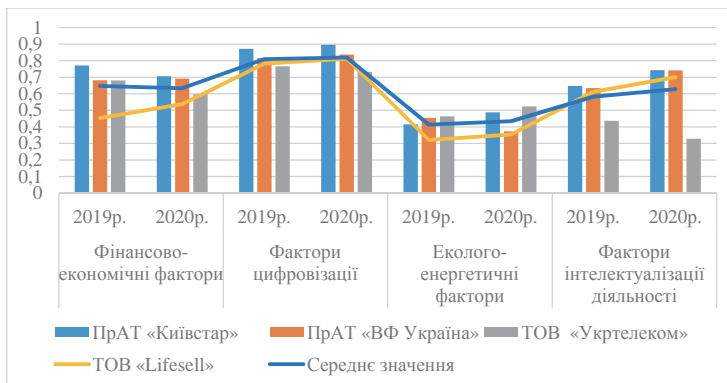


Рис. 2.11. Графічне зображення інтегрованих оцінок внутрішніх можливостей щодо підвищення розвитку управління ризиками телекомунікаційних підприємств (за концептами) у 2019-2020 роках

Примітка: складено авторами на основі таблиці 2.7.

Аналіз даних дозволяє зробити висновок, що за умови розробки дієвих заходів щодо підвищення ефективності фінансової діяльності та активізації цифровізації, підприємства зможуть підвищити значення даних інтегрованих оцінок внутрішньої можливості.

Водночас, переконуємось, що рівень внутрішніх можливостей активізації розвитку управління ризиками телекомунікаційних підприємств в цілому залишається на середньому рівні.

Жодне телекомунікаційне підприємство досліджуваної сукупності не досягає високого чи достатнього рівня стійкості до кризи.

При цьому слід зазначити, що в 2020 році намітилася позитивна тенденція підвищення рівня внутрішньої стійкості до ризиків: рівень нижче середнього був характерний тільки для АТ „Укртелеком”.

Узагальнюючи вище проведені розрахунки, розроблено блок-схему оцінок внутрішніх можливостей підвищення розвитку управління ризиками телекомунікаційних підприємств (рис. 2.12), що дозволяє чітко структурувати весь діагностичний процес, починаючи з визначення значення інтегрованих оцінок за концептами (фінансово-економічні чинники, чинники цифровізації, еколого-енергетичні чинники, чинники інтелектуалізації діяльності), а також оцінити фактичний рівень внутрішньої стійкості до ризиків, шляхом інтегрування до єдиної мети, завдань та об'єктів окремих етапів діагностики.

Таким чином, результати проведеної діагностики впливу чинників на розвиток управління ризиками свідчать, що його активізацію можна вважати ключовим аспектом діяльності телекомунікаційних підприємств.

З огляду на системний характер розвитку управління ризиками телекомунікаційних підприємств актуалізується питання оцінки внутрішніх можливостей щодо його активізації та гармонізації.

Така діагностика дозволить правильно визначити вектор управлінських рішень щодо подальшого розвитку управління ризиками телекомунікаційних підприємств.

Проведена діагностика ключових чинників впливу на розвиток управління ризиками телекомунікаційних підприємств дозволяє зробити наступні висновки.

Зважаючи на необхідність визначення ключових чинників впливу на розвиток управління ризиками та оцінки можливостей досягнення високих економічних результатів телекомунікаційних підприємств доцільно розробляти анкету та здійснювати опитування керівників та фахівців телекомунікаційних підприємств.

За результатами анкетування, варто формувати систему індикаторів оцінки впливу ключових чинників на розвиток управління ризиками, яка, на відміну від існуючих, має враховувати галузеву специфіку сфери телекомунікацій за концептами (фінансово-економічні чинники, чинники цифровізації, еколого-енергетичні чинники, чинники інтелектуалізації діяльності) та дозволяє на основі встановленого рівня внутрішньої ризиковості діяльності визначити внутрішні здібності забезпечення розвитку управління ризиками телекомунікаційних підприємств та можливості досягнення високих економічних результатів їх діяльності.

Встановлено, що на сучасному етапі поступу телекомунікаційних підприємств існує досить велика кількість проблем, пов'язаних із забезпеченням розвитку управління ризиками, з проміж них варто виокремити розбалансованість бізнес-процесів, не достатня ефективність використання ресурсного та інтелектуального потенціалу, низький рівень врахування еколого-енергетичних чинників тощо.

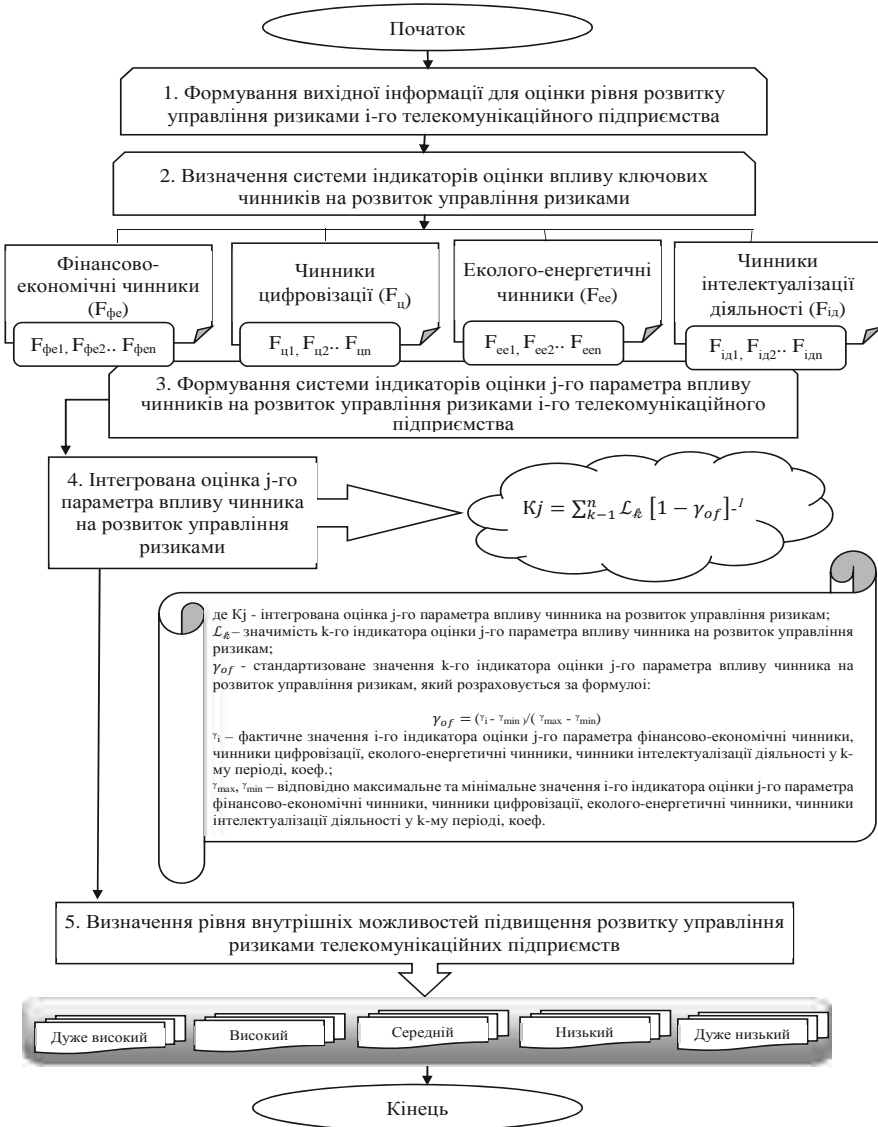


Рис. 2.12. Блок-схема визначення внутрішніх можливостей підвищення розвитку управління ризиками телекомунікаційних підприємств

Примітка: розроблено з використанням [105, 110, 111, 114]

2.3. Ефективність розвитку управління ризиками телекомунікаційних підприємств

Вищеозначені дослідження підтверджують особливу актуальність діагностики ефективності розвитку управління ризиками на підприємствах. Так, розглядаючи характерні ризики телекомунікаційних підприємств, доцільно акцентуватись на ризиках інформаційно-комунікаційних технологій, що пов'язані із надійністю та якістю білінгових систем, кібер-безпекою, захистом конфіденційної інформації, особливо персональних даних клієнтів підприємства. Означене, слід доповнити ризиками, зумовленими проведенням реструктуризації підприємств внаслідок поширених сьогодні процесів злиття та поглинання.

Водночас, нині, не можна оминати ризики, які стали вагомими для телекомунікаційних підприємств, воєнного та пост воєнного часу, зважаючи на те, що підприємства змушені функціонувати в жорстких умовах економічної кризи в наслідок жорсткої російської агресії. Втрати активів і ресурсів (кадрові, фінансові, матеріальні, територіальні (покриття), технологічні, інфраструктурні тощо) вимагають розробки нових підходів до формування системи управління ризиками в телекомунікаційних підприємствах задля забезпечення важливого компоненту життєстійкості й незламності населення та умов перемоги України – постійних комунікацій та надійного зв'язку. „У довоєнний період ринок стаціонарного ширококутного зв'язку в Україні був висококонкурентним (ННІ 0,12)” [156]. При цьому, „загальний дохід від фіксованого ширококутного доступу, наданого в Україні у 2020 р., становив 13,48 млрд грн.” [118]. Нині телекомунікаційний ринок зазнав значних трансформацій. Незважаючи на порівняно високу рентабельність телекомунікаційних послуг і продуктів, для підприємств відчутним є зростання операційних витрат.

Нині, на функціонування телекомунікаційних підприємств здійснюють вплив наступні чинники: нестабільність умов зовнішнього середовища, що пояснюється воєнними діями; значні руйнування енергетичної інфраструктури; знищення телекомунікаційної інфраструктури, розкрадання ворогом приміщень, обладнання; необхідність термінового відновлення чи заміни ширококутного покриття на деокупованих територіях тощо.

Зокрема, лише „станом на 1 червня 2022 року телекомунікаційно-цифровий сектор України зазнав збитків від війни на 0,7 млрд. доларів США. З них – на 0,6 млрд. доларів було завдано шкоди операторам стаціонарного та мобільного зв'язку. Оцінка шкоди завдана українським провайдером стаціонарного ширококутного зв'язку становила 0,3 мільярда доларів США; для мобільних провайдерів – 0,2 мільярда доларів США. Завдана шкода включає вартість пошкоджених і зруйнованих інтернет-ліній через військові дії на тимчасово непідконтрольних уряду територіях, а також пошкодженої інфраструктури на тих територіях, які були повернуті під контроль уряду до 1 червня 2022 року. Загалом 1 767 269 стаціонарних ліній були пошкоджені або зруйновані, що обмежило доступ місцевого населення до ширококутного

інтернету та телекомунікаційних послуг. Накопичені збитки українських провайдерів стаціонарного широкопasmового зв'язку становлять не менше 0,05 мільярда доларів США; для провайдерів мобільного зв'язку вони становлять 0,1 мільярда доларів США. Ці збитки є нижньою оцінкою економічної доданої вартості (прибутку), втраченої внаслідок вторгнення. Вони відображають втрачений прибуток інтернет-провайдерів (ISP) протягом перших трьох місяців війни та періоду відновлення послуг протягом 18 місяців. За оцінками, 22 % доходів інтернет-провайдерів були втрачені через втрату абонентів і неоплачене надання послуг. Оператори мобільного зв'язку постраждали ще сильніше в короткостроковій перспективі (перші три місяці), оскільки неоплачене надання послуг і втрата абонентів на тимчасово невідконтрольних урядом територіях вже проявилися в березні й тривали до кінця травня. Витрати інтернет-провайдерів також збільшилися через видалення уламків, незаплановані ремонтні роботи, витрати на переїзд персоналу і багато чого іншого. Оцінка збитків є консервативною, оскільки вона враховує лише частину, що стосується норми прибутку (17 відсотків в середньому для європейських інтернет-провайдерів) із 22 відсотків втраченого доходу" [156].

Водночас, варто враховувати: реалізацію принципово нових технологічних рішень; невпинну інтеграцію до західноєвропейського інфо-комунікаційного ринку, формування єдиного цифрового простору з ЄС тощо. За означених нових економічних реалій життєво важливим є завчасне виявлення й об'єктивна діагностика ефективності розвитку управління ризиками в телекомунікаційних підприємствах та формування адаптивної системи управління ризиками із використанням проактивних методів їх мінімізації та нівелювання. Цікаво, що зарубіжні телекомунікаційні підприємства здійснюють безперервне управління ризиками на превентивній, антиципативній основі за слабкими сигналами загроз. Настання відчутних змін в динамічному середовищі телекомунікаційного підприємства теж відбувається не водночас, фактично перед такими змінами завжди проявляються сигнали раннього попередження, слабкі сигнали. Адекватна ідентифікація яких може завчасно попередити про загрози та ризики, що наближаються. Вплив ризикових процесів на функціонування телекомунікаційних підприємств спричиняє негативні наслідки їх фінансового стану: низька обіговість активів, незбалансованість грошових потоків, наявність значної частки дебіторської та кредиторської заборгованості у складі оборотних активів та поточних зобов'язань відповідно, висока собівартість послуг і продуктів, недостатня ліквідність та платоспроможність тощо.

Для виживання в сьогоdnішніх економічних реаліях телекомунікаційним підприємствам необхідна наявність результативного своєчасного управління ризиками, що дасть змогу стежити за ринковими тенденціями, здійснювати глибоку експертизу діяльності конкурентів та оперативно реагувати на нові виклики та загрози сьогоdnення. До найбільш розповсюджених чинників, що пояснюють необхідність пошуку телекомунікаційними підприємствами нових підходів до діагностики ефективності розвитку управління ризиками на

підприємствах та активізації цих процесів можна віднести: „генерування нових конкурентних переваг; прагнення збільшення капіталізації підприємства, зокрема з допомогою розміщення акцій на світових фондових біржах; розвиток нових послуг та тарифних схем; зростання абонентської бази операторів та ускладнення розрахунків” [149 с. 69]. Водночас, зауважимо, що окрім операційних бізнесових ризиків для телекомунікаційних підприємств знаковими вважаються й інвестиційні ризики, що зумовлено гостротою конкурентної боротьби у сфері телекомунікацій, що змушує здійснювати вагомі додаткові інвестиції в інноваційні проекти щодо закупівлі сучасного обладнання та розвитку новітніх технологій. До таких новітніх технологій відносять: хмарні технології, широкосмуговий доступ до Інтернету, цифрове медіа та телебачення, послуги інтелектуальної мережі зв'язку, діджиталізацію бізнес-процесів з використанням елементів штучного інтелекту, організація відео конференцій, впровадження трафіку віртуальних мереж тощо. Наголосимо, що ключовим рішенням щодо подолання наслідків настання кризових явищ та прояву ризиків стало масове скорочення інвестиційних програм телекомунікаційними підприємствами. Аналіз статистичних даних провідних міжнародних організацій, які займаються систематизацією аналітичних показників розвитку галузі технологій та зв'язку різних країн світу та визначенням найбільш актуальних ризиків її функціонування, свідчить про існування певних проблем та тенденцій даної галузі. Відповідно даних Technology and Communications Industry Report [195], топовими ризиками інформаційно-комунікаційної галузі є зростання конкуренції, втрата репутації бренду компанії, невідповідність інноваційним потребам клієнтів, втрата професійних кадрових ресурсів, кіберзлочини, часова нерівномірність економічних циклів, втрата інтелектуальної власності, нестабільність нормативно-правової бази, недосконалість інформаційних технологій та порушення ланцюгів постачань продуктів. Зазначені ризики було структуровано за ступенем їх впливу (від 1 до 10 місця) (табл. 2.8).

Джерелом наведеної інформації є результати опитування респондентів різних країн, яким було запропоновано обрати 10 найбільш вагомих ризиків для їх власних компаній із 53 ризиків загального переліку [105].

Найбільш актуальними було виявлено ризики зростання конкуренції, втрати репутації бренду та невідповідності інноваційним потребам клієнтів.

Слід зазначити, що конкуренція як невід'ємний атрибут ринкових відносин активізує розвиток інноваційного потенціалу підприємств, стимулює продуктивність їх діяльності та економічне зростання.

Поруч з цим, ризик зростаючої конкуренції може привести до припинення діяльності недостатньо капіталізованих та фінансово нестійких компаній, що обумовлено наявністю конкурентів з боку іноземних компаній, стрімким розвитком технологій, зміною тарифної політики тощо. З огляду на це більшість телекомунікаційних підприємств розглядають конкуренцію як пріоритетний ризик сучасності, який в цілому займає перше місце в галузі.

Слід зазначити, що ризик невідповідності інноваційним потребам клієнтів є доволі актуальним для вітчизняних телекомунікаційних підприємств, які демонструють недостатній рівень інноваційної активності. Це зумовлено існуванням низки чинників, серед яких можна виділити

Таблиця 2.8

Ризики телекомунікаційних підприємств

Місце	Сфера технологій та зв'язку (<i>Technology and Communications Industry</i>)	Сфера технологій (<i>Technology</i>)	Сфера комунікацій (<i>Communications</i>)
1	Технологічні ризики (недосконалість ІКТ)	Виробничі ризики (порушення ланцюгів постачань продуктів, ризик часової нерівномірності економічних циклів)	Підприємницькі ризики (зростання конкуренції, втрата репутації бренду)
2	Ризики діджиталізації	Кібер- ризики (кіберзлочинність)	Ризик втрати професійних кадрових ресурсів та інтелектуальної власності
3	Виробничі ризики (порушення ланцюгів постачань продуктів, ризик часової нерівномірності економічних циклів)	Технологічні ризики (недосконалість ІКТ)	Ризики діджиталізації
4	Підприємницькі ризики (зростання конкуренції, втрата репутації бренду)	Підприємницькі ризики (зростання конкуренції, втрата репутації бренду)	Виробничі ризики (порушення ланцюгів постачань продуктів, ризик часової нерівномірності економічних циклів)
5	Кібер- ризики (кіберзлочинність)	Інвестиційні ризики	Технологічні ризики (недосконалість ІКТ)
6	Інвестиційні ризики	Адміністративно-нормативні ризики (ризик злиття та поглинання підприємств, ризик банкрутства)	Інноваційні ризики (невідповідність інноваційним потребам клієнтів)
7	Ризик втрати професійних кадрових ресурсів та інтелектуальної власності	Юридичні ризики (нестабільність нормативно-правової бази, ризик корпоративної відповідальності)	Кібер- ризики (кіберзлочинність)

8	Інноваційні ризики (невідповідність інноваційним потребам клієнтів)	Ризик втрати професійних кадрових ресурсів та інтелектуальної власності	Інвестиційні ризики
9	Адміністративно-нормативні ризики (ризик злиття та поглинання підприємств, ризик банкрутства)	Інноваційні ризики (невідповідність інноваційним потребам клієнтів)	Юридичні ризики (нестабільність нормативно-правової бази, ризик корпоративної відповідальності)
10	Юридичні ризики (нестабільність нормативно-правової бази, ризик корпоративної відповідальності)	Ризики діджиталізації	Адміністративно-нормативні ризики (ризик злиття та поглинання підприємств, ризик банкрутства)

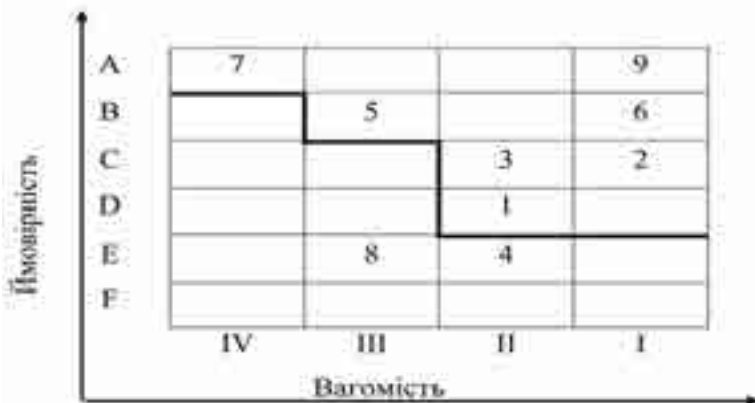
Примітка: сформовано з використанням [105].

фінансові (нестача власних фінансових ресурсів, значні витрати на освоєння інновацій, тривалість окупності нових телекомунікаційних продуктів, брак коштів у замовників) – 39%; інформаційні (дефіцит інформації щодо нового обладнання чи телекомунікаційних технологій, відсутність даних щодо існуючих тенденцій розвитку телекомунікаційних ринків, проблеми зі знаходженням зацікавлених учасників щодо партнерства у сфері інноватики) – 19%; ринкові (домінування окремих підприємств на ринку окремих телекомунікаційних послуг, низький попит на інноваційні продукти чи телекомунікаційні технології, високі економічні та фінансові ризики при освоєнні нововведень на телекомунікаційному підприємстві) – 27%; інші (немає необхідності у швидкому впровадженні інновацій, недосконалість нормативного поля у сфері підтримки телекомунікаційних підприємств, нестача або відсутність досвідчених кваліфікованих спеціалістів для освоєння інновацій) – 15% [105].

Використовуючи кваліфікаційну матрицю ризиків досліджуваних телекомунікаційних підприємств, здійсненої на основі запропонованої мультимодульної карти ризиків за допомогою обрахування коефіцієнту конкордації розраховано, що найвпливовішим ризиком є технологічні, на що вказало 93 % опитаних респондентів (керівників та спеціалістів 17 телекомунікаційних підприємств) (рис. 2.13).

Наступними є ризики діджиталізації – узгодженість думок 64% опитаних респондентів. Вагомість впливу виробничого та підприємницького ризиків склали 51% і 45% відповідно.

За останній часовий період досить гостро вип'ятилась проблема загрози кібер-ризиків, що пояснюється процесами глобалізації, інтеграції та діджиталізації, що відмітили 38% респондентів, також вагомих вплив несуть на діяльність телекомунікаційних підприємств інвестиційні ризики – 25% респондентів підтвердили цей тренд загроз.



*Рис.2.13. Мультимодульна карта ризиків телекомунікаційних підприємств
Примітка: побудована з використанням [4, 140, 154]: 1- технологічні ризики; 2- ризики діджиталізації; 3- виробничі ризики; 4 – підприємницькі ризики; 5 – кібер-ризики; 6 - інвестиційні ризики; 7 – адміністративно-нормативні ризики; 8 – юридичні ризики.*

Так, „вразливість інформаційних інфраструктур сягає – 40% за похибками у налаштуванні, 27% становлять помилки у програмному кодї та 20% ризики відсутності або несвочасність оновлень безпекових програм” [87]. Мінімальний безпосередній вплив на діяльність телекомунікаційних підприємств здійснюють адміністративно-нормативні та юридичні ризики. Таким чином, за сучасних умов функціонування телекомунікаційних підприємств, з урахуванням існуючих трендів економічного розвитку національної економіки, особливої важливості набуває проблема захисту телекомунікаційних підприємств від негативних впливів бізнес-середовища, вирішення якої вимагає їх відповідної адаптації до існуючих глобальних та локальних суспільно-політичних і економічної невизначеностей. Це є можливим за умови ефективності розвитку управління ризиками телекомунікаційних підприємств та результативного використання ними методів управління різноманітними ризиками.

Враховуючи останні виклики й кризові процеси (масовані несанкціоновані руйнівні втручання у цифрову та комунікаційну інфраструктуру, у функціонування комп’ютерних, інфо-комунікаційних, мобільних мереж, що вип’ятили неготовність та вразливість вітчизняних телекомунікаційних підприємств та їх хиткість до ефективного протистояння потужним кібератакам), телекомунікаційні підприємства, їх партнери (замовники програмного забезпечення, користувачі ІТ-послуг) готові додатково інвестувати в безпекові системи та у захист своїх цифрових даних (впровадження антивірусних програм, апаратне забезпечення, ефективний програмно-апаратний захист, додаткові організаційні заходи, убезпечення

цифрових комунікацій тощо) від деформацій, знищення, пошкодження чи викрадення, що вважаємо на часі.

У процесі розвитку управління ризиками, телекомунікаційні підприємства мають вирішувати гострі питання щодо відбору персоналу для розробки та впровадження ІТ-послуг і ІТ-продуктів, забезпечення своєчасності виконання різних проєктів, дієвих способів усунення помилок щодо формування програмних кодів, різноманітних збоїв у програмному забезпеченні тощо. Все це генерує додаткові ризики (табл. 2.9).

Вибір та використання різноманітних методів управління ризиками на телекомунікаційних підприємствах залежить від їх фінансового стану та ресурсних можливостей. Нині, широке застосування методів управління ризиками в телекомунікаційних підприємствах поки не спостерігається і часто зводиться до диверсифікації, страхування та формування резервів і запасів, тобто самострахування.

Таблиця 2.9

Ризики та методи управління ними в телекомунікаційних підприємствах

Блок	Ризик	Методи управління ризиками	Види інструментарію
Інвестиційні ризики	Ризик розробки продукту неналежної якості	Розподіл ризиків Прогнозування та ухилення від ризикових подій	формування партнерських відносин, юридичні, договірні методи, формування резервів, моніторинг, контроль
	Ризик недотримання встановлених строків розробки продукту	Отримання фінансових гарантій Самострахування	
	Ризик перевищення бюджету витрат	Лімітування Диверсифікація	
	Юридичний ризик, адміністративно-нормативні ризики	Хеджування Страхування	
Операційні ризики	Технологічні ризики ризики діджиталізації	Диверсифікація Страхування	Формування резервів, моніторинг, контроль
	виробничі ризики	Превенція ризиків	
	підприємницькі ризики	Диверсифікація Самострахування	
	адміністративно-нормативні ризики	Прогнозування та ухилення від ризикових подій	

Примітка: сформовано за [75].

Процес формування резервів і запасів є доволі складним, вимагає додаткового інформаційного забезпечення та аналітичної роботи. Саме тому, як правило, резервування здійснюється в межах великих підприємств [75], а малі телекомунікаційні підприємства обмежуються більш простими методами

управління ризиків. Використання телекомунікаційними підприємствами ключових методів управління ризиком та оцінка їх результативності за роками продемонстрована у таблиці 2.10.

Таблиця 2.10

Використання телекомунікаційними підприємствами ключових методів управління ризиком та оцінка їх результативності за роками (%).

Методи управління ризиком	2016 – 2018 рр.		2019 – 2021 рр.	
	використання методу	результативність методу	використання методу	результативність методу
Диверсифікація	56	76	78	65
Лімітування	34	34	42	42
Самострахування (формування резервів)	51	86	69	77
Превенція ризиків	26	45	34	42
Хеджування	18	23	24	32
Страхування	69	86	82	78
Отримання фінансових гарантій	17	76	26	87
Прогнозування та ухилення від ризикових подій	23	34	32	28
Розподіл ризиків (формування партнерських відносин, юридичні, договірні методи)	15	37	29	46

Примітка: сформовано за [75].

Як переконуємось, переважно, телекомунікаційні підприємства обирають та використовують методи управління ризиками:

пасивно, тобто реакція підприємства на ризикові явища відбувається незалежно від моменту його настання або зовсім млява реакція на окремі ризикові процеси, при цьому мало відчутний вплив спектру загроз на вибір та використання методів управління ризиків;

реактивно, тобто реакція підприємства на ризикові явища відбувається після їх настання, зовнішнє середовище вважається постійним джерелом загроз, викликів, які впливають на вибір та використання методів управління ризиків;

активно, тобто реакція підприємства на ризикові явища відбувається у момент, коли воно настає при високому впливі чинників зовнішнього середовища на вибір та використання методів управління ризиків.

Таким чином, дослідження методів провідних телекомунікаційних вітчизняних підприємств за 2016-2021 роки демонструють, що ключовими чинниками недосконалості їх системи управління ризиками слід вважати неадекватність та несвоєчасність вибору використання методів управління ризиків, що не дає змогу своєчасно ухвалювати відповідні управлінські заходи.

Переважно, телекомунікаційні підприємства, не мають достатнього досвіду щодо вибору та використання методів управління ризиків, водночас, наголосимо на позитивних аспектах їх практики: активне використання методів ідентифікації, діагностики та ранжування ризиків; своєчасне інформування акціонерів і партнерів про причини та обсяг можливих втрат; розробка адаптаційних заходів для пристосування до нових реалій сьогодення тощо.

На часі використання проактивних методів управління ризиками в телекомунікаційних підприємствах.

Оцінка рівня організації управління ризиками досліджуваних телекомунікаційних підприємств (табл. 2.11) продемонструвала найвищий рівень організації у ПрАТ „Київстар”.

Таблиця 2.11

Оцінка рівня організації управління ризиками телекомунікаційних підприємств

Показник оцінки організації управління ризиками	ПрАТ „Київстар”		ПрАТ „ВФ Україна”		ТОВ „Lifesell”		АТ „Укртелеком”	
	2019	2020	2019	2020	2019	2020	2019	2020
Коефіцієнт нейтралізації складних ризиків (<i>Кнсп</i>)	0,73	0,75	0,69	0,62	0,52	0,65	0,55	0,51
Коефіцієнт адаптації інструментів управління ризиками до специфіки підприємства (<i>Каір</i>)	0,68	0,70	0,66	0,71	0,62	0,72	0,46	0,41
Коефіцієнт автоматизації (цифровізації) оцінки ризиків (<i>Каор</i>)	0,55	0,64	0,52	0,57	0,51	0,52	0,45	0,53
Коефіцієнт організаційної відповідальності за управління ризиками (<i>Корв</i>)	0,70	0,78	0,68	0,76	0,54	0,71	0,56	0,63
Коефіцієнт розвитку культури проактивного управління ризиками (<i>Ктур</i>)	0,62	0,65	0,65	0,65	0,62	0,71	0,62	0,68
Інтегральний показник (<i>Коур</i>)	0,656	0,704	0,640	0,662	0,562	0,662	0,528	0,552

Позитивна динаміка і найвище значення інтегрального показника рівня організації управління ризиками у ПрАТ „Київстар” (0,704 у 2020 р.) корелює з найвищими серед досліджуваних підприємств обсягами чистого доходу від реалізації і чистого прибутку. Певний стрибок в організації управлінні ризиками притаманний ТОВ „Lifesell” (0,562 у 2019 р. і 0,662 у 2020 р.), що виводить дане підприємство на рівень організації управління ризиками вище середнього. Зазначимо, що у 2020 р. ТОВ „Lifesell” пододало збитковість минулих років і досягло чистого прибутку в обсязі 2586680,0 тис. грн. На аналогічному рівні вище середнього (0,640 у 2019 р. і 0,662 у 2020 р. залишається організація управління ризиками у ПрАТ „ВФ Україна”.

І стабільно середній рівень підтримує АТ „Укртелеком”, незважаючи на падіння чистого прибутку у 2020 р. майже вдвічі.

Аналіз показав, що найменш розвинутими для досліджених підприємств виявились управлінські аспекти, пов’язані з цифровізацією оцінки і прогнозування ризиків на основі сучасних інтегрованих програмних рішень, а також рівень розвитку корпоративної культури „проактивного управління ризиками”. Натомість у всіх підприємств окрім АТ „Укртелеком” ефективно розвивається адаптація інструментів управління ризиками до специфіки бізнес-процесів та підвищується їх інноваційність.

Апробацію запропонованих підходів у п.1.3, проведено на основі 4 досліджуваних у роботі підприємств, згрупованих у кластери методом к-середніх. Типологію кластера запропоновано визначати на основі врахування таких критеріїв, як рівень економічної стійкості підприємства (враховано 4 рівня: низький, середній, вище середнього, високий) та рівень організації управління ризиками (враховано 3 рівня: реактивний, стандартний, прогресивний). Типологія запропонованих у роботі кластерів телекомунікаційних підприємств для визначення рівня розвитку управління ризиками представлена у таблиці 2.12.

Таблиця 2.12.

Типологія кластерів телекомунікаційних підприємств для визначення рівня розвитку управління ризиками

Рівень організації управління ризиками	Рівень економічної стійкості з урахуванням фінансово-економічних, цифровізаційних, інтелектуалізаційних та ринкових чинників ризиків			
	1.Низький ($0,01 \leq E_{стр} \leq 0,25$)	2.Середній ($0,26 \leq E_{стр} \leq 0,50$)	3.Вище середнього ($0,51 \leq E_{стр} \leq 0,75$)	4.Високий (0,76 $\leq E_{стр} \leq 1$)
Реактивний ($0,10 \leq Коур \leq 0,40$)	А 1	А 2	А 3	А 4
Стандартний ($0,41 \leq Коур \leq 0,70$)	В 1	В 2	В 3	В 4
3.Прогресивний ($0,71 \leq Коур \leq 1$)	С 1	С 2	С 3	С 4

На основі запропонованого науково-методичного підходу було розраховано коефіцієнт ефективності розвитку управління ризиками і визначено рівень ефективності (табл.2.13).

Таблиця 2.13

Визначення ефективності розвитку управління ризиками телекомунікаційних підприємств

Найменування показника	ПрАТ „Кіівстар”		ПрАТ „ВФ Україна”		ТОВ „Lifesell”		АТ „Укртелеком”	
	рік							
	2019	2020	2019	2020	2019	2020	2019	2020
Інтегральний показник рівня організації управління ризиками (K_{oup})	0,656	0,704	0,640	0,662	0,562	0,662	0,528	0,552
Інтегральний показник рівня економічної стійкості з урахуванням факторів ризику ($E_{стп}$)	0,751	0,709	0,705	0,681	0,461	0,708	0,678	0,635
Відстань інтегрального показника управління ризиками у різні періоди t від його максимального значення (C_{t0})	0,221	0,228	0,278	0,286	0,265	0,271	0,304	0,311
Середнє значення відстані ($\overline{C_0}$)	0,862	0,941	0,867	0,851	0,604	0,763	0,597	0,626
Коефіцієнт ефективності розвитку управління ризиками (d_t)	0,744	0,758	0,679	0,664	0,561	0,645	0,491	0,503
Кластер підприємства	В3	С3	В3	В3	В2	В3	В3	В3
Рівень ефективності розвитку управління ризиками	Високий	Високий	Вище середнього	Вище середнього	Середній	Вище середнього	Середній	Середній

Як показали результати розрахунків, найвищий рівень розвитку управління ризиками і найменш „радикальний” фокус змін у стратегію ризик-менеджменту має ПрАТ „Київстар”. Означене підприємство має прогресивний рівень організації управління ризиками, найвищий серед досліджуваних підприємств рівень економічної стійкості і найкращий коефіцієнт ефективності розвитку управління ризиками.

Достатньо високий (за шкалою – „вище середнього”) рівень розвитку управління ризиками мають ПрАТ „ВФ Україна” (2 місце після ПрАТ „Київстар”) та ТОВ „Lifesell” (відповідно – 3 місце).

На даному етапі підприємства мають стандартний з елементами прогресивного рівень розвитку управління ризиками і достатньо підготовлені до застосування інноваційних механізмів управління ризиками. Середній рівень розвитку управління ризиками і, відповідно, найбільшу необхідність удосконалення стратегії ризик-менеджменту демонструє АТ „Укртелеком” (4 місце).

Таким чином, проведені дослідження показали, що провідні телекомунікаційні підприємства України, а саме ПрАТ „Київстар”, ПрАТ „ВФ Україна”, ТОВ „Lifesell” та АТ „Укртелеком” мають достатньо високий (вище середнього або середній) рівень розвитку управління ризиками, що засвідчує відповідний рівень ефективності. Найвищий рівень розвитку управління ризиками і найменш „радикальний” фокус змін у стратегію ризик-менеджменту має ПрАТ „Київстар”. Означене підприємство має прогресивний рівень організації управління ризиками і найвищий серед досліджуваних підприємств рівень економічної стійкості. Достатньо високий (за шкалою – „вище середнього”) рівень розвитку управління ризиками мають ПрАТ „ВФ Україна” (2 місце після ПрАТ „Київстар”) та ТОВ „Lifesell” (відповідно – 3 місце). На даному етапі підприємства мають стандартний з елементами прогресивного рівень розвитку управління ризиками, що відповідає середньому рівню підготовленості до застосування інноваційних механізмів зниження ризиків.

2.4. Ризикозахищеність телекомунікаційних підприємств в реаліях цифрової трансформації

Процеси цифрових трансформацій телекомунікаційних підприємств зазнають істотного впливу елементів невизначеності, чим зумовлюється високий ризик їх діяльності. Цей ризик стає особливо значним, оскільки багато важливих рішень приймаються в умовах неповної, неточної чи суперечливої інформації.

Наслідком прийняття рішень у реаліях цифрової трансформації є невизначеність результатів, тому доводиться ризикувати. З іншого боку, ризик викликаний спонтанним і суперечливим характером цифрових процесів, що відбуваються в складних соціально-економічних системах, які неможливо адекватно і вичерпно описати. Таким чином, ризик телекомунікаційних підприємств в реаліях цифрової трансформації слід розглядати як наслідок

прийняття рішень в умовах неповної, неточної чи суперечливої інформації, тобто в умовах невизначеності чи неповної визначеності.

Під ризиком цифрових трансформацій розуміють можливість (загрозу) втрати телекомунікаційним підприємством частини своїх ресурсів, недоотримання доходів чи виникнення додаткових витрат у результаті здійснення виробничо-збутової і фінансової діяльності, яка спирається на нові цифрові технології, нові продукти, нові способи їхньої реалізації тощо. Численні техногенні катастрофи, кількість яких зростає в міру розвитку цифрових технологій, підтверджують це.

При здійсненні цифрових трансформацій у телекомунікаційних підприємств виникає об'єктивна необхідність у розробці способів попередження, зниження чи компенсації можливих негативних наслідків цих специфічних ризиків. Для цього телекомунікаційні підприємства спочатку кількісно оцінюють величину ризику конкретного процесу цифрової трансформації (як ймовірності деструктивних наслідків, так і величини можливих втрат), виділяють і досліджують вплив і частку кожного з чинників ризику в загальному обсязі можливих втрат. Результати оцінки ризику враховують при ухваленні телекомунікаційними підприємствами рішень щодо вибору стратегії і тактики цифрового розвитку, плануванні науково-технічної, виробничо-збутової і фінансової діяльності, що пов'язана із цими процесами.

Ризик може проявлятися в тому, що новий (модернізований) продукт чи послуга вже в процесі впровадження виявляється непотрібним, тоді як на момент рішення про його розробку і впровадження, що спиралося на результати діагностики кон'юнктури ринку, потреб і запитів споживачів, напрямків і темпів розвитку НТП тощо, передбачалося, що попит на нього буде стійким. Ризик може проявлятися й у тому, що на даному ринку чи його сегменті новий продукт чи послуга можуть бути і не реалізованими у тих обсягах, які були розраховані на основі результатів маркетингових досліджень. Ухвалюючи рішення про проведення великомасштабної рекламної компанії нової продукції, зазвичай, не можна бути цілком упевненим у її ефективності. Так само, як і вибираючи варіанти цінової стратегії для проникнення на нові ринки, не можна з повною впевненістю стверджувати, що телекомунікаційне підприємство очікує успіх, оскільки конкуренти можуть відповісти адекватними діями. Як наслідок цих ситуацій – можливість отримання збитків чи недоотримання доходу. Впровадження цифрових трансформацій телекомунікаційними підприємствами завжди пов'язано з високим ризиком. Основні причини цього:

можливі різкі зміни економічної, політичної, соціальної, екологічної і інших складових середовища функціонування в процесі впровадження цифрових трансформацій;

зміни споживчих запитів;

несприйнятливості інноваційних цифрових трансформацій персоналом чи споживачами;

непередбачуваність дій конкурентів;

неадекватна оцінка власних можливостей;
прискорення темпів науково-технічного прогресу, цифрові технологічні і технічні прориви тощо.

У цих реаліях, телекомунікаційним підприємствам необхідно особливо ретельно прогнозувати і кількісно оцінювати ризик цифрових трансформацій з урахуванням усього комплексу чинників ризику з метою розроблення комплексу заходів, спрямованих на зниження, компенсацію чи запобігання можливим деструктивним наслідкам. Причому цю оцінку телекомунікаційним підприємствам доводиться вести в умовах інформаційного дефіциту, що вимагає специфічних методів оцінки ризику.

Оцінка ризику телекомунікаційних підприємств в реаліях цифрових трансформацій поділяється на два доповнюючих один одного види – якісна і кількісна.

Якісна оцінка має за мету визначення чинників ризику, що впливають на результати прийнятих рішень і виконуваних робіт, встановлення потенційних зон ризику й ідентифікацію ризиків.

Кількісна оцінка передбачає чисельне визначення розмірів ризику (ймовірностей виникнення втрат і їх величин).

При оцінці ризику часто виділяють ті їх види, що не пересікаються, для того щоб уникнути подвійного урахування.

Часто для кількісної оцінки ризику використовують імовірнісний підхід, відповідно до якого для того, щоб оцінити ризик, необхідно знати всі можливі наслідки конкретного рішення чи дії (або закон їхнього розподілу) і ймовірності цих наслідків.

Імовірності розвитку того чи іншого сценарію визначають:

об'єктивним методом (на підставі наявних даних про аналогічні проекти, що виконувалися в аналогічних умовах, розраховується частота, з якою відбуваються ті чи інші явища);

суб'єктивним методом (зокрема, шляхом експертної оцінки, коли група експертів висловлює припущення щодо конкретних результатів і ймовірностей їхнього виникнення).

Імовірнісний підхід для оцінки ризику передбачає використання таких критеріїв:

очікуване значення результату, яке розраховується як середньозважене за ймовірностями величин усіх можливих результатів (як результат звичайно використовують запланований прибуток (дохід) конкретного процесу цифрової трансформації або можливі втрати);

мінливість чи розкид можливих результатів, що розраховується як корінь квадратний із середньозваженого квадратів відхилень можливих результатів від їх очікуваного значення (середньоквадратичне чи стандартне відхилення).

Іноді виникають ситуації, коли корисним виявляється розрахунок такого критерію, як відносний ризик (величина ризику, що припадає на одиницю результату), щоб перевірити, чи компенсується підвищений ризик підвищеним доходом. Показник даного критерію розраховується як результат від ділення

середньоквадратичного відхилення на очікуване значення результату (у статистиці йому відповідає коефіцієнт варіації).

Слід відзначити, що використання критерію відносного ризику можливе лише у випадку, якщо очікувані значення результатів за варіантами порівнянні. В іншому випадку даний критерій не застосовується.

Для оцінки ризику цифрових трансформацій, телекомунікаційні підприємства використовують різні методи, серед яких найбільше поширення одержали статистичний метод (у тому числі метод статистичних випробувань чи метод Монте-Карло); аналітичний метод; метод використання дерева рішень та імовірнісного підходу; метод оцінки фінансової стійкості або оцінки доцільності витрат; метод експертних оцінок; нормативний метод; метод діагностики чутливості; метод використання аналогів та інші. Кожний з названих методів має свої переваги і недоліки і використовується в цілком конкретних ситуаціях; універсального методу, прийнятного для всіх випадків, не існує. В практичній діяльності, телекомунікаційні підприємства використовують декілька методів. Природно, отримані різними методами результати різняться, але дослідження розходжень між ними дозволяють виявити чинники, які враховуються в одних методах і відсутні в інших, що впливає на точність оцінки і достовірність результатів. Аналіз розходжень у результатах дасть змогу виявити існуючі тенденції розвитку майбутніх подій з погляду ризику тих чи інших процесів цифрових трансформацій. А це сприятиме більш точному прогнозуванню ступеня ризику конкретних проєктів цифрових трансформацій.

У деяких випадках телекомунікаційні підприємства використовують інші, більш специфічні методи, що включають у різних комбінаціях елементи теорії ігор, теорії оптимізації, факторного аналізу, теорії ймовірностей (у тому числі умовні ймовірності), комбінаторики, нечіткої логіки тощо.

Цікаво, що понад 90% телекомунікаційних підприємств, що впроваджували цифрові трансформації, істотно поліпшили показники своєї діяльності і зміцнили свої позиції на ринку.

Водночас, цифрові трансформації, в результаті яких підвищуються невизначеність, ризик і загрози, особливо гостро випинають проблематику виявлення можливостей ризикозахищеності телекомунікаційних підприємств, оскільки вони функціонують в кризових умовах конкурентного середовища, володіючи різної потужності цифровим потенціалом. Тому у кожного підприємства генеруються специфічні ризики та загрози, що притаманні лише конкретному підприємству.

Т. Андерсен та П. Шредер стверджують, що „нині, коли відбуваються корпоративні скандали і великі фінансові невдачі, підвищується актуальність ефективного управління ризиками”.

І. Кох обґрунтовує „застосування нечітких моделей для оцінки ризиків”. Підтримують такий підхід і Мамдані, Сугено, Цукамото.

А. Гріффін, наводить конкретні приклади „ефективних і помилкових дій корпорацій з управління ризиками”.

Т. Бедфорд і Р. Кук окреслюють „фундаментальні поняття невизначеності, її співвідношення з ймовірністю, межі з кількісною оцінкою невизначеності”.

„Ризикозахищеність підприємства – це забезпеченість життєво важливих інтересів і потреб системи підприємства від усього спектра зовнішніх і внутрішніх загроз, різних за своєю природою”. У контексті системного підходу, ризикозахищеність телекомунікаційного підприємства в реаліях цифрових трансформацій окреслюється, як „властивість системи, що забезпечує її сталість і стабільний цифровий розвиток в умовах виникнення різних видів ризиків внутрішнього і зовнішнього середовища.

Тобто, це така характеристика системи, яка дозволяє звести до мінімуму, а в кращому випадку, і повністю позбутися від негативних наслідків впливу ризиків різної природи”. Практично, ризикозахищеність телекомунікаційного підприємства в реаліях цифрових трансформацій демонструє спроможність підприємства успішно протидіяти ендегенним і екзогенним загрозам, можливість адекватно і швидко трансформувати свій організаційний дизайн й цифровий потенціал відповідно до динамічних реалій.

У розвиток такого підходу, управління ризикозахищеністю телекомунікаційного підприємства в реаліях цифрових трансформацій окреслюють, як багатоступінчастий комплексний процес, метою якого вважається зниження чи компенсація втрат на підприємстві за реалізації ризиків при освоєнні цифрових інновацій.

Наукові підходи до обґрунтування сутності, витоків генерування і різновидів ризиків цифрових трансформацій досить строкаті. Мета знаходження можливостей ризикозахищеності телекомунікаційного підприємства в реаліях цифрових трансформацій має дисонувати цільовій функції підприємства щодо генерування максимальних обсягів прибутку при гармонійному співвідношенні прибутку і ризику.

Концептуальні підходи щодо можливості ризикозахищеності телекомунікаційного підприємства в реаліях цифрових трансформацій зосереджені у такому: цифрові трансформації підприємства завжди супроводжуються ризиком як атрибутом невизначеності; на виникнення ризику та його значимість впливають чинники зовнішнього та внутрішнього середовища, тож доцільно вивчати зовнішні та внутрішні чинники виникнення ризиків цифрової трансформації; ризик може мати як деструктивний характер, тобто приносити збитки підприємству, так і позитивний, тобто підсилювати приховані можливості цифрового розвитку; незалежно від характеру прояву ризику необхідно ним управляти, використовуючи такі методи як, страхування, лімітування, диверсифікація, хеджування тощо.

Тож, зважаючи на означене щодо можливості ризикозахищеності, на рисунку 2.14 представлено конститутивні атрибути ризикозахищеності телекомунікаційного підприємства в реаліях цифрових трансформацій.



Рис. 2.14. Конститутивні атрибути ризикозахищеності телекомунікаційного підприємства в реаліях цифрових трансформацій

Види ризиків телекомунікаційного підприємства в реаліях цифрових трансформацій представлено на рисунку 2.15.

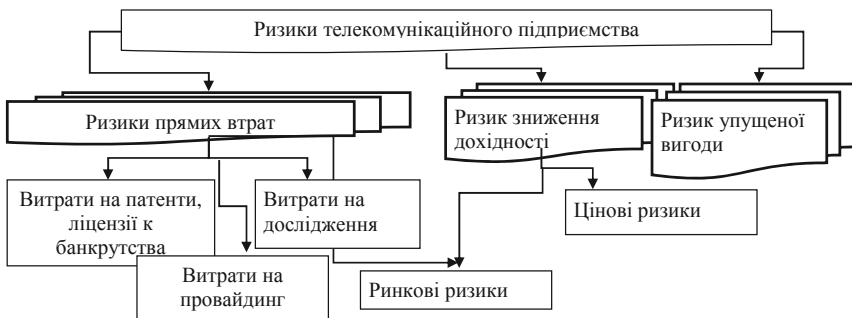


Рис. 2.15. Ризики телекомунікаційного підприємства в реаліях цифрових трансформацій

Система внутрішніх та зовнішніх чинників, що впливають на виникнення ризиків в телекомунікаційних підприємствах в реаліях цифрових трансформацій продемонстрована на рисунку 2.16.



Рис. 2.16. Система внутрішніх та зовнішніх чинників, що впливають на виникнення ризиків в телекомунікаційних підприємствах в реаліях цифрових трансформацій

За результатами експертних оцінок щодо ризиків внутрішнього середовища, з'ясовано (табл. 2.14), що гальмуючими чинниками цифрових трансформацій телекомунікаційних підприємств є: відсутність фінансових джерел для впровадження цифрових трансформацій (16 %), низька активність освоєння цифрових трансформацій (15 %), низькі ринкові можливості й альтернативи втілення цифрових трансформацій (14 %), відсутність стратегічного набору (12 %), низька організаційно-комунікаційна здатність щодо цифрових трансформацій (11 %), нерозвинутість організаційного дизайну та комунікаційних внутрішніх зв'язків (9 %), незацікавленість управлінської команди (7 %), відсутність спеціалістів з відповідними компетенціями (6 %), нерозвиненість інфраструктури цифрових трансформацій (5 %), низький рівень диверсифікації діяльності (3 %), високий рівень формалізації й централізації менеджменту (2 %).

Таблиця 2.14

Ризики внутрішнього середовища, що гальмують цифрові трансформації телекомунікаційних підприємств

Ризики	Вага ризиків
Відсутність фінансових джерел для впровадження цифрових трансформацій	0,16
Низька активність освоєння цифрових трансформацій	0,15
Низькі ринкові можливостей й альтернативи втілення цифрових трансформацій	0,14
Відсутність стратегічного набору	0,12
Низька організаційно-комунікаційна здатність щодо цифрових трансформацій	0,11
Нерозвинутість організаційного дизайну та комунікаційних внутрішніх зв'язків	0,09
Незацікавленість управлінської команди	0,07
Відсутність спеціалістів з відповідними компетенціями	0,06
Нерозвиненість інфраструктури цифрових трансформацій	0,05
Низький рівень диверсифікації діяльності	0,03
Високий рівень формалізації й централізації менеджменту	0,02

Таблиця 2.15

Ризики зовнішнього середовища, що гальмують цифрові трансформації телекомунікаційних підприємств

Ризики	Вага ризиків
Високі параметри кредитних ставок	0,19
Обтяжлива система оподаткування	0,17
Брак необхідної інфраструктури для трансферу технологій та відповідної інформаційно-аналітичної підтримки	0,15
Високий рівень конкурентної боротьби	0,12
Відсутність необхідності впровадження цифрових трансформацій	0,10
Зростання інфляційних процесів, що впливає на високу вартість матеріальних активів, технологій, енергоносіїв	0,09
Відсутність налагоджених зв'язків між наукою та виробництвом	0,08
Низька платоспроможність населення	0,05
Нерозвиненість мережі цифрової інфраструктури	0,03
Недостатнє державне стимулювання цифрових трансформацій	0,02
Неочікувані зміни керівництва та завдань цифрового розвитку, рейдерство	0,01

За результатами експертних оцінок щодо ризиків зовнішнього середовища (табл. 2.15), з'ясовано, що гальмуючими чинниками цифрових трансформацій телекомунікаційних підприємств є: високі параметри кредитних ставок (19 %), обтяжлива система оподаткування (17 %), брак необхідної інфраструктури для трансферу технологій та відповідної інформаційно-аналітичної підтримки (15 %), високий рівень конкурентної

боротьби (12 %), відсутність необхідності впровадження цифрових трансформацій (10 %), зростання інфляційних процесів, що впливає на високу вартість матеріальних активів, технологій, енергоносіїв (9 %), відсутність налагоджених зв'язків між наукою та виробництвом (8 %), низька платоспроможність населення (5 %), нерозвиненість мережі цифрової інфраструктури (3 %), недостатнє державне стимулювання цифрових трансформацій (2 %), неочікувані зміни керівництва та завдань цифрового розвитку, рейдерство (1 %).

Зважаючи, що ризик впливає на можливість здійснення руйнівних наслідків цифрового розвитку, і водночас може сприяти генеруванню додаткових можливостей, усі методи доцільно сегментувати на: методи зменшення рівня чинників ризику цифрових трансформацій; методи підсилення сприятливих можливостей ризикозахищеності (рис. 2.17).



Рис. 2.17. Методи ризикозахищеності телекомунікаційних підприємств в реаліях цифрових трансформацій

Дієвий стратегічний набір управління ризикозахищеністю телекомунікаційних підприємств в реаліях цифрових трансформацій має бути зорієнтований на гармонізацію співвідношення бажаного прибутку і величини ризику. Важливим інструментом для зменшення невизначеності та оптимізації такого співвідношення вважаємо розвиток інформаційно-аналітичної підтримки цифрового розвитку підприємств.

Розробка карти ризиків цифрових трансформацій телекомунікаційного підприємства та його ризик-профілю буде доцільною при: оцінці загроз і ризиків; формуванні стратегічного набору за показниками ризикозахищеності; прогнозуванні заходів на підтримку функціонування системи ризикозахищеності телекомунікаційного підприємства та необхідних витрат.

Прийняття управлінських заходів щодо забезпечення ризикозахищеності телекомунікаційних підприємств в реаліях цифрових трансформацій має опиратись на ключові принципи: не доцільно ризикувати на суму більшу власних активів; завжди потрібно розраховувати вплив наслідків ризику; не слід ризикувати великою сумою заради малих прибутків; позитивно ухвалюється рішення тільки при відсутності альтернатив, якщо є альтернативи, то слід ухвалювати превентивні дії щодо мінімізації ризиків (рис. 2.18).

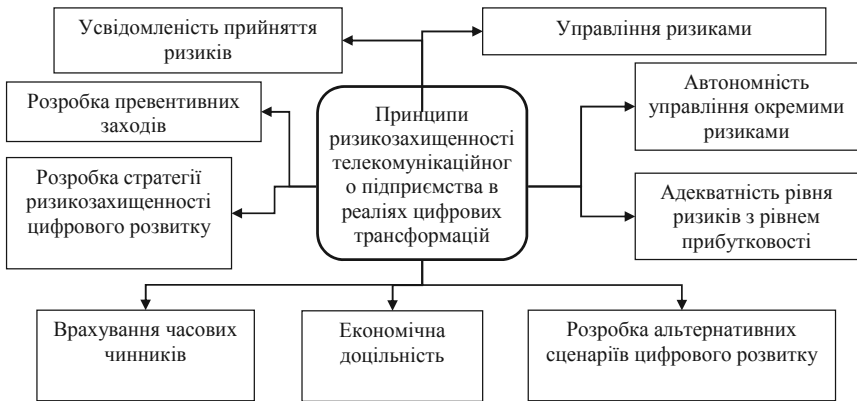


Рис. 2.18. Принципи ризикозахисності телекомунікаційних підприємств в реаліях цифрових трансформацій

Вказані принципи є загальними, тобто вони є сукупністю правил розробки заходів, яких доцільно притримуватись при різних сценаріях розвитку подій. Обов'язково, при формуванні і фільтрації стратегічного набору необхідно враховувати часові і ресурсні обмеження. На рисунку 2.19 подано механізм ризикозахисності телекомунікаційних підприємств в реаліях цифрових трансформацій.

Відповідно до обґрунтованих положень система заходів щодо ризикозахисності телекомунікаційних підприємств в реаліях цифрових трансформацій має включати:

постійний моніторинг і аналіз ризиків та ендогенних й екзогенних чинників й передумов здійснення цифрового розвитку підприємств;

розробка системи заходів щодо мінімізації зовнішньої уразливості цифрового розвитку телекомунікаційних підприємств;

підвищення гнучкості організаційного дизайну та формування структур, що займаються ризикозахисністю телекомунікаційних підприємств в реаліях цифрових трансформацій;

розробка превентивних заходів щодо мінімізації наслідків реалізації ризиків та появи перешкод для цифрового розвитку телекомунікаційних підприємств;

підготовка персоналу та розробка відповідних заходів щодо розподілу відповідальності і повноважень при настанні непередбачуваних чи кризових ситуацій.

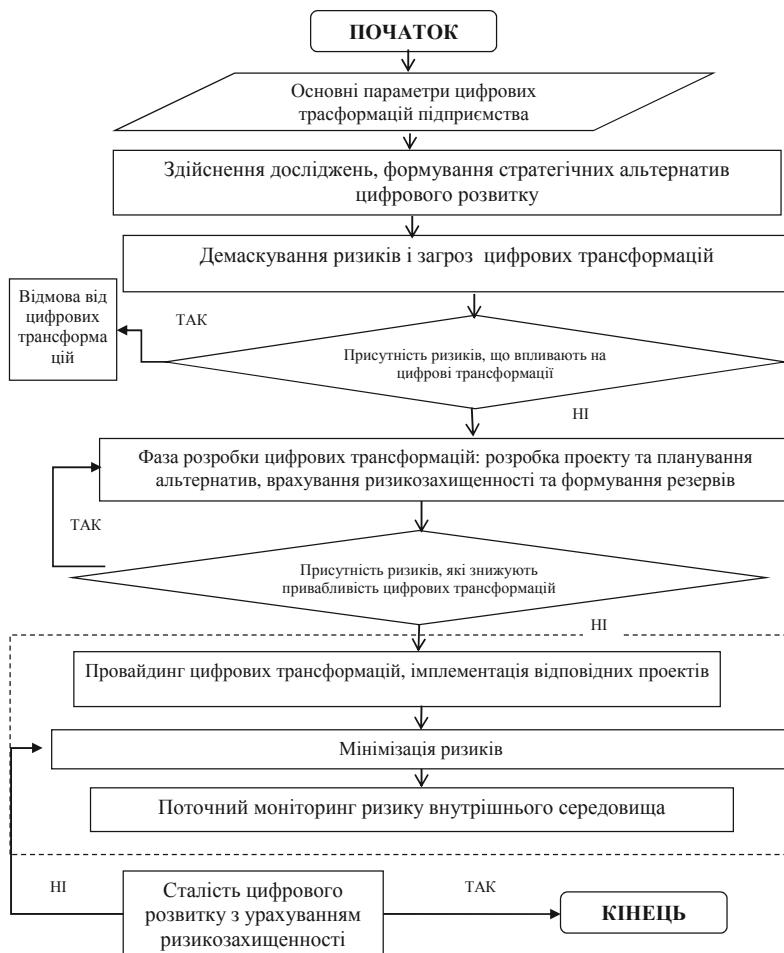


Рис. 2.19. Механізм ризикозахищеності телекомунікаційних підприємств в реаліях цифрових трансформацій.

Цифровий розвиток відбувається нерівномірно, демонструє висхідні та низхідні періоди, коливання кількісних та якісних економічних характеристик, конструктивні та руйнівні тренди і має розглядатися в певному часовому відтинку. Такий підхід до формування можливостей ризикозахищеності телекомунікаційних підприємств в реаліях цифрових трансформацій сприятиме їх цифровому розвитку, підвищенню їх конкурентоспроможності та нарощуванню ефективності.

РОЗДІЛ 3

ПРІОРИТЕТНІ НАПРЯМИ РОЗВИТКУ УПРАВЛІННЯ РИЗИКАМИ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ В РЕАЛІЯХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

3.1. Напрями активізації розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації

Останнім часом у вітчизняній та світовій економічній науці та практиці пошук напрямів активізації управління ризиками підприємств в реаліях цифрових трансформацій є вкрай актуальні. Цим проблемам присвячуються статті у науковій та популярній літературі, проводяться спеціальні тематичні семінари та конференції. Концептуальні підходи до активізації розвитку управління ризиками в підприємствах висвітлено в працях А.О. Старостіної [151], М.А. Дядюк [57], Н.В. Карасвої, С.В. Войтко, Л.В. Сорокіної [86], М.В. Боровик [14], К. Д. Семенової. К.І. Тарасової [146] та інших науковців. Методологія активізації розвитку управління ризиками в телекомунікаційних підприємств у пост воєнний період має базуватися на міжнародних стандартах, відомих моделях світових компаній та науковців з врахуванням загально-управлінських, загальних принципів ризик-менеджменту та специфічних для телекомунікаційних підприємств принципів. Аналіз міжнародних стандартів управління ризиками виконано в публікаціях вітчизняних вчених: О.М. Донець, Т.В. Савельєвої, Ю.І. Урецької [52], Т. В. Головач, А.Б. Грушевицької, В. В. Швид [30], Н Стрельбіцької [153]. Крім того, слід враховувати такі тенденції як – обов'язковість запровадження нових технологічних рішень телекомунікаційними підприємствами; поступова та невпинна інтеграція у західноєвропейський комунікативний простір та побудова єдиного цифрового ринку з ЄС тощо.

В працях науковців відсутні підходи до визначення поняття активізації розвитком управління ризиком на підприємстві, тому проаналізовано підходи до загального поняття „Активізація” (табл. 3.1). Виходячи з цього, поняття «активізації розвитком управління ризиками телекомунікаційних підприємств», визначимо як *«цільєспрямований вплив на розвиток управління ризиками телекомунікаційних підприємств з виключення або зниження негативних наслідків настання ризикових подій для прискорення досягнення підприємством стратегічної мети та завдань бізнес-комбінацій, процесів розвитку та підтримки»*. До основних напрямів активізації розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрових трансформацій можна віднести:

1. *Усвідомлення ризиків та їх загроз для досягнення мети функціонування підприємства та їх подальша ідентифікація* (ідентифікація активів, ідентифікація джерел ризиків, ідентифікація ризикових подій, ідентифікація заходів контролю, ідентифікація наслідків).

Таблиця 3.1

Підходи до трактування поняття „активація” в управлінні підприємством

Термін	Визначення
Активація (Activation) (менеджменту)	це час початку, коли повністю або частково запускається план забезпечення безперервності бізнесу (business continuity, BC), зв'язку з кризовими ситуаціями (crisis communication, CC), управлінням кризовими ситуаціями (KM) або плану аварійного відновлення (disaster recovery, DR) [176] https://www.bcmpeia.org/wiki/Activation
Активація (загальне, в управлінні)	або активувати, дієслово – означає привести в рух; зробити активним або більш активним [187]
Активація (стратегії)	це крок з визнання того, що перед впровадженням або виконанням чогось, людей потрібно переконати в бажанні внести зміни. Активація стратегії – це те, що відбувається між створенням стратегії та виконанням стратегії [177]
Управління активацією бренду (Brand Activation Management, BAM)	це те, як підприємство організовує та використовує всі наявні ресурси, необхідні для забезпечення узгодженості, частоти та адаптивності, необхідних для досягнення визнання та вдячності споживачів, а також співробітників, потенційних новобранців та громадськості в цілому [179]
Активація (як функція)	забезпечення зацікавленості всіх учасників процесу управління та ефективності їх дій [108]
Активація (як частина мотивації)	цілеспрямований вплив на сформовану систему мотивів організаційної поведінки менеджера [2]

Примітка: систематизовано авторами

2. Формулювання змісту декларації та настанов з ризик-менеджменту.

У самому спрощеному вигляді декларація відображає філософію телекомунікаційного підприємства щодо управління ризиками (відношення організації до ризиків; розмежування повноважень між суб'єктами ризик-менеджменту; персоналізація відповідальності тощо). Декларація містить викладення мети, завдань та принципів управління ризиками, а також опис методів ризик-менеджменту, використання яких суб'єктами управління є припустимим (наприклад: зниження можливості виникнення аварій; формування стабілізаційних (резервних) фондів для фінансування можливих втрат; страхування тощо) [112 с.62].

3. Формування організаційної структури управління ризиками та формалізація її діяльності (положення про структурний відділ, інструкції, плани тощо).

4. Визначення принципів управління ризиками

(принципи можуть бути закріплені в окремому документі або бути зафіксовані в декларації з ризик-менеджменту). Незалежно від форми формалізації (оформлення) принципів їх зміст повинен бути пов'язаний з механізмами управління ризиками.

Основні напрями активізації управління ризиками телекомунікаційних підприємств в реаліях цифрових трансформацій які можна представити у вигляді трикутника взаємопов'язані між собою, охоплюють стадії процесу

управління ризиками, співвідносяться до функцій менеджменту та є базою механізму управління ризиками телекомунікаційного підприємства (рис. 3.1).



Рис. 3.1. Трикутник напрямів активізації управління ризиками телекомунікаційних підприємств в реаліях цифрових трансформацій
Примітка: запропоновано авторами на основі [2, 36, 37, 44, 89].

Базисом трикутника напрямів активізації розвитку управління ризиками телекомунікаційних підприємств вважаємо визначення принципів управління ризиками підприємства. Ефективний і життєздатний розвиток управління ризиками телекомунікаційних підприємств повинен відповідати системі принципів, яка враховує загальні принципи управління ризиком та специфічні принципи ризик-менеджменту самих телекомунікаційних підприємств.

Принципи управління ризиками відображують:

- 1) розмежування повноважень (права, обов'язки, відповідальність) між суб'єктами ризик-менеджменту, а також визначення організаційної ієрархії;
- 2) порядок отримання інформації про ризики та умови їх позиціонування (динаміка надходження та особливості розподілу між суб'єктами управління);
- 3) особливості взаємодії між суб'єктами та об'єктами ризик-менеджменту, а також порядок взаємодії з основними партнерами організації;
- 4) дії при загостренні ризикової ситуації;
- 5) зміст підходів до управління ризиками, а також пріоритетність використання тих чи інших методів (механізмів) управління ризиками;
- 6) контроль за процесом та результатами управління [112 с.69].

Загальні принципи управління на підприємстві наведено у додатку. Фактично, принципи управління ризиком в телекомунікаційних підприємствах можна розділити на три основні групи. Принципи, що входять до складу першої групи, є загальними, що відносяться до системи управління в цілому. У другій

групі об'єднуються приватні принципи, що стосуються окремих частин і елементів системи управління. Принципи, складові третьої групи, регламентують порядок і правила управління конкретними видами діяльності або явищами (зокрема – ризиками). Принципи ризик-менеджменту – спеціальні принципи, що регламентують порядок і правила управління ризиками [144 с.26]. У вітчизняному законодавстві відсутні нормативні документи, що встановлюють регламент розробки та застосування системи управління ризиками в телекомунікаційних підприємствах. В результаті телекомунікаційні підприємства, самостійно формують концепцію побудови системи управління ризиками, спираючись у цій роботі на відомі світові стандарти, що містять найкращі практики. Насамперед це стандарт ISO/IEC Guide 73 „Управління ризиками – словник – настанови по використанню у стандартах” від 2002 та 2009 років [54]; цікавим вважаємо стандарт управління ризиками, що розроблений в COSO (The Committee of Sponsoring Organizations of the Treadway Commission), а саме модель COSO ERM (Enterprise Risk Management) [119, 182, 193] (додаток X), розроблений у 2004 році. У Європі широкого поширення набули стандарти управління ризиками FERMA [175, 192], створені в 2002 році Інститутом ризик-менеджменту (IRM) та Асоціацією ризик-менеджменту та страхування (AIRMIC) (додаток) . Слід також згадати ISO 31000:2009 [120] та ISO 31000:2018 [179, 53] „Управління ризиками. Принципи та рекомендації”, розроблений та доповнений Міжнародною організацією зі стандартизації (International Organization for Standardization), а також ISO/TR 31004:2013 „Управління ризиками – Керівництво з впровадження ISO 31000” [55]. У роботі О.М. Донець, Т.В. Савельсової, Ю.І. Урецької висвітлено важливість впровадження міжнародних стандартів в управлінні ризиками проєктно-орієнтованих підприємств, розроблено напрями та алгоритм опису ризиків на основі вимог провідних міжнародних стандартів з ризик-менеджменту [52]. У публікації Т.В. Головач, А.Б. Грушевицької, В.В. Швид досліджено теоретичні та практичні питання застосування ризик-менеджменту на підприємствах, функції та основні етапи ризик-менеджменту, основні міжнародні стандарти ризик-менеджменту [30]. Н. Стрельбіцька досліджує міжнародний стандарт управління ризиками ISO 31000: 2009, розглядає взаємозв'язок між принципами, системою і процесом управління ризиками та зміни у термінологічній базі [153].

Всі ці стандарти та рекомендації мало відрізняються, у них не розглядається специфіка бізнесу, але доступно та чітко виражаються основні поняття управління ризиками, ідеологія процесу управління та бажані стадії розробки та функціонування. Також, на жаль, лише декілька міжнародних стандартів виділяють принципи управління ризиками, якими слід керуватися для активізації розвитку управління ризиками в підприємствах (табл. 3.2).

Визначення сутності ризику та управління ним висвітлено в деяких нормативно-законодавчих актах України [131, 132, 133, 134, 135], але вони не містять перелік принципів, якими слід керуватися при активізації системи управління ризиками на підприємстві.

Принципи управління ризиками за міжнародними стандартами

Номер стандарту	Назва стандарту (англ.)	Назва стандарту (укр.)	Рік	Організація-розробник	Сутність стандарту	Принципи згідно із стандартом
COSO II ERM – Integrated Framework [119] COSO ERM [182 с.3]	Enterprise Risk Management – Integrated Framework Enterprise Risk Management – Integrating with Strategy and Performance	Інтегрована модель управління ризиками підприємства. Управління ризиками підприємства – інтеграція зі стратегією та продуктивністю	2004 2016 2016	Комітет організації-спонсорів Комісії Тредвея (The Committee of Sponsoring Organizations of the Treadway) США	Цей документ описує концептуальні основи управління ризиками підприємства, в якому містяться детальна інформація та рекомендації стосовно створення корпоративної системи ризик-менеджменту в рамках підприємства.	Виділяє шість принципів: 1) прозорій процесури; 2) зобов'язання на найвищому рівні; 3) оцінка ризиків; 4) належна обачність; 5) спільну діяльність (включаючи навчання); 6) моніторинг та огляд. Принципи є базою структури COSO ERM, яка складається з п'яти взаємопов'язаних компонентів: управління та культура; стратегія та постановка цілей; продуктивність; огляд і перегляд; інформація, комунікація та звітність
ISO 31000:2009 [120] ISO 31000:2018 [53]	Risk management – Principles and guidelines on Implementation	Управління ризиками. Принципи та рекомендації	2009 2018	Міжнародна організація зі стандартизації (International Organization for Standardization)	Основний стандарт з ризик-менеджменту. Містить принципи та загальні вказівки з виявлення ризиків та ефективного управління ними. Даний стандарт дає загальне розуміння того, як розробити, впровадити і підтримувати ефективну систему управління ризиками в рамках галузі підприємства тощо	1) інтегрованість; 2) структурованість і комплексність; 3) індивідуальність; (адаптованість та прозорість зовнішньому та внутрішньому контексту організації); 4) залученість (своєчасне залучення зацікавлених сторін призводить до покращення об'язаності та інформованого управління ризиками); 5) динамічність; 6) доступність інформації; 7) людські та культурні фактори; 8) постійне вдосконалення
ISO/TR 31004:2013 [55 с.10-20]	Risk management – Guidance for the implementation of ISO 31000	Управління ризиками – Керівництво з впровадження ISO 31000м	2013	Міжнародна Організація зі Стандартизації (International Organization for Standardization (ISO))	Цей стандарт сприяє ефективному впровадженню ISO 31000, а також забезпечує структурований підхід до переходу від існуючої практики управління ризиками до стандарту ISO 31000 з гнучкою перспективою адаптації до майбутніх змін; роз'яснення базових концепцій ISO 31000 з рекомендаціями та прикладами, 119 адаптованими до індивідуальних потреб користувачів; додаткове керівництво за принципами ISO 31000 та основи управління ризиками.	1) управління ризиками є невід'ємною частиною всіх організаційних процесів; 2) управління ризиками є частиною прийняття рішень; 4) управління ризиками чітко звертається до невизначеності; 5) управління ризиками є системним, структурованим і своєчасним; 6) управління ризиками базується на найкращій наявній інформації; 7) управління ризиками адаптивне; 8) управління ризиками враховує людські та культурні фактори; 9) управління ризиками є прозорим та інклюзивним; управління ризиками є динамічним, повторюваним і реагує на зміни; 10) управління ризиками сприяє постійному вдосконаленню організації

Примітка: складено авторами на основі [119; 182 с.3; 120; 53; 55 с.10-20]

В Україні принципи управління ризиками зафіксовані у «Положенні про організацію системи управління ризиками в надавачах фінансових послуг та небанківських фінансових групах» [136], де описані основні положення ризик-менеджменту, створення комплексної, адекватної та ефективної системи ризик-менеджменту з урахуванням особливостей фінансової діяльності, характеру, обсягів фінансових операцій, профілю ризиків та системної важливості фінансових установ, яка відповідає таким принципам: ефективність; своєчасність; структурованість; розподіл обов'язків; усебічність та комплексність; пропорційність; незалежність; конфіденційність; прозорість [136]. Підходи до принципи управління ризиками на підприємствах, наведені в працях вітчизняних науковців [86 с.60; 146, с.46-47; 147 с.17; 14 с.27; 112 с.63; 27 с.166-168] (додаток 3.4).

Опираючись на вказані дослідження, стверджуємо, що до найбільш важливих загальних принципів розвитку управління ризиками телекомунікаційних підприємств можна віднести:

1. *Принцип інтегрованості* передбачає розгляд управління ризиками як невід'ємної частини діяльності підприємства, який застосовується двома методами: при розробці моделі управління ризиками (включаючи підтримку в робочому стані та його поліпшення); під час реалізації процесу управління ризиками у прийнятті рішень і пов'язаної з цим діяльності.

2. *Принцип структурованості та комплексності* сприяє досягненню погоджених і співставних результатів. Послідовний підхід до управління ризиками під час прийняття рішень дає можливість підвищити ефективність діяльності підприємства та забезпечити результати, які можуть закріпити довіру до компанії та її успіх. Принцип структурованості передбачає чіткий розподіл функцій, обов'язків і повноважень з управління ризиками між усіма структурними підрозділами та працівниками підприємства, та їх відповідальність згідно з таким розподілом. Комплексність означає охоплення всіх видів діяльності підприємства на всіх організаційних рівнях та у всіх його структурних підрозділах, оцінка взаємного впливу ризиків. Для досягнення підприємством таких результатів необхідно, щоб у практичній діяльності всередині підприємства було закріплено врахування ризиків, які пов'язані з рішеннями, а також використання узгоджених критеріїв ризику.

3. *Принцип ефективності* означає процес управління, що забезпечує об'єктивну оцінку розміру ризиків підприємства та повноту заходів щодо управління ризиками з оптимальним використанням фінансових ресурсів, персоналу та інформаційних систем підприємства.

4. *Принцип незалежності* передбачає свободу від обставин, що становлять загрозу для неупередженого виконання підрозділом з управління ризиками та підрозділом контролю за дотриманням норм своїх функцій. Незалежність передбачає недопущення ситуації, коли винагорода працівників підрозділу з управління ризиками та підрозділу контролю за дотриманням норм, у тому числі їх керівників, пов'язана з фінансовими результатами бізнес-підрозділів.

5. *Принцип адекватної реакції та розумного прийняття* полягає у швидкій та ефективній реакції на зовнішні зміни в ризиковій ситуації, а також у прийнятті ризику лише у випадку його обґрунтованої необхідності.

6. *Принцип адаптованості* виражається через адаптацію моделі та процесу управління ризиками та відповідає зовнішньому та внутрішньому контексту підприємства, пов'язаний з його цілями. Кожен процес в управлінні ризиками необхідно адаптувати до його конкретної цілі. Структура і процес управління ризиками співвідносяться та налаштовуються з урахуванням зовнішнього і внутрішнього контексту організації, пов'язаного з її завданнями, цілями та політиками [27 с.167]. Адаптація необхідна для досягнення інтеграції з процесами прийняття рішень на підприємстві. Такі процеси прийняття рішень можливо буде необхідно змінити для приведення у відповідність зі структурованою моделлю управління ризиками.

7. *Принцип інклюзивності* передбачає належну та своєчасну залученість стейкхолдерів, що, в свою чергу, дозволяє враховувати їх знання, думку, а це призводить до підвищення освіченості та поінформованості щодо управління ризиками. Впроваджуючи цей принцип слід враховувати конфіденційність, безпеку та секретність. Наприклад, це може виражатись у обмеженні доступу до певної категорії документації. Дуже важливим аспектом при впровадженні принципу інклюзивності є його ефективність, саме на цьому етапі можна як вибудувати, так і зруйнувати довіру стейкхолдерів. Вони обов'язково повинні бути залучені у всі аспекти процесу управління ризиками.

8. *Принцип динамічності* полягає у наявності зміни ризиків в залежності внутрішнього та зовнішнього середовища самого підприємства. Управління ризиками дає змогу вчасно передбачати, виявляти й відповідно реагувати на зміни й події. Слід проводити моніторинг, відповідний аналіз та контроль прийняття управлінських рішень.

9. *Принцип доступності, надійності та релевантності інформації* означає, що вхідні дані для управління ризиками базуються на історичній та поточній інформації, а також на майбутніх очікуваннях та прогнозах. Особливу увагу в управлінні ризиками слід приділяти невизначеності та обмеженням, що пов'язані з інформацією та очікуваннями. Надійність та точність інформації необхідно постійно перевіряти на актуальність, своєчасність та надійність.

10. *Принцип врахування людських та культурних чинників* передбачає існування впливу на всі аспекти управління ризиками на кожному рівні й етапі людської поведінки й культури. Особливу увагу слід приділити здатності знаходити та реагувати на своєчасні попередження, надмірна увага чи байдужість до думок інших або нестача знань; упередженість через спрощені стратегії обробки інформації для вирішення складних завдань.

11. *Принцип постійного вдосконалення та результативності* базується на розумінні та необхідності постійного покращення процесу управління ризиками на основі накопичення досвіду та постійного навчання. Постійне покращення передбачає покращення інтеграції діяльності з управління ризиками в усі види діяльності підприємства; підвищення якості оцінювання ризиків; удосконалення моделі, наприклад, якості та доступу до інформації;

покращення швидкості прийняття рішень. До принципів, які притаманні й особливо важливі слід також виділити: модульність, багатокритеріальність оцінки, індивідуальність, своєчасність, конфіденційність, прозорість (табл. 3.3).

Таблиця 3.3

Додаткові специфічні принципи управління ризиками телекомунікаційних підприємств

Принцип	Характеристика принципу
Принцип модульності	тобто, можливість використання різних поєднань процедур управління ризиком телекомунікаційного підприємства у різних ситуаціях, що дозволяє врахувати специфіку конкретної ситуації та за необхідності налаштувати зазначену систему на вирішення індивідуальних потреб користувачів телекомунікаційних послуг
Принцип багатокритеріальності оцінки	різномірність складу системи та наявність специфічних бізнес процесів (операційних, процесів розвитку та підтримки) підприємства телекомунікацій, зокрема, означає, що кожен процес оцінюється з різних точок зору за унікальними критеріями, у тому числі й неформалізованими, що спричиняє виникнення додаткових складнощів при аналізі процесу прийняття рішень у сфері управління ризиком
Принцип індивідуальності	Урахування специфіки телекомунікаційних підприємств (операторів та провайдерів), розмірів, стадій життєвого циклу підприємства та інших факторів, які визначатимуть вплив ризику на бізнес-процеси
Принцип своєчасності	процес управління ризиками, що забезпечує своєчасне (на ранній стадії) виявлення, вимірювання, моніторинг, контроль, звітування та пом'якшення усіх видів ризиків на всіх організаційних рівнях
Принцип конфіденційності, безпеки та секретності	недопущення отримання інформації, що не підлягає оприлюдненню, особами, у яких немає повноважень на її отримання, управління ризиками не порушуючи політику конфіденційності підприємства телекомунікацій
Принцип прозорості	оприлюднення підприємством телекомунікацій інформації щодо системи управління ризиками та профілю ризику
Принцип максимізації (масштабність) та мінімізації	максимізація полягає у прагненні до врахування якомога більшої кількості сфер можливого виникнення ризиків на підприємстві телекомунікацій, а мінімізація. – у зменшенні спектра проявів ризиків і ступеня їх впливу
Принцип пропорційності	створення ефективної системи управління ризиками, що відповідає бізнес-моделі телекомунікаційного підприємства, його системі системній важливості, а також рівню складності операцій, що здійснюються телекомунікаційним підприємством.

Примітка: запропоновано авторами

Виходячи з цього, можна запропонувати систему принципів з урахуванням специфіки телекомунікаційних підприємств, яка включає загально-управлінські, загальні принципи ризик-менеджменту та додаткові специфічні для підприємств телекомунікацій принципи, використання яких сприятиме активізації управління ризиками в реаліях цифрових трансформацій (рис. 3.2).



Рис. 3.2. Система принципів управління ризиками телекомунікаційних підприємств в реаліях цифрових трансформацій

Примітка: розроблено авторами

Нині, успіх активізації розвитку управління ризиками в реаліях цифрових трансформацій багато в чому залежатиме від рівня цифрової зрілості телекомунікаційного підприємства, ступеня підтримки керівництва та кваліфікації персоналу. Активізація розвитку управління ризиками має бути центральним елементом стратегічного управління телекомунікаційного підприємства, яка базується на дотриманні *загально-управлінських, принципів ризик-менеджменту та специфічних принципів*, що сприятиме створенню нової філософії та культури ведення бізнесу та активізації розвитку управління ризиками в реаліях цифрових трансформацій задля досягнення підприємством поставленої мети.

Сьогодні, кризові деформації економічного простору, зумовлені воєнним станом, постковідними явищами, глобалізаційними й інтеграційними процесами пояснюють необхідність докорінних якісних перетворень щодо активізації розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрових трансформацій. Сьогодні до загальних труднощів

телекомунікаційних підприємств, додалися кадрові проблеми, пов'язані з залученням компетентного персоналу на військову службу, міграцією спеціалістів жінок за кордон; руйнування і розкрадання ворогом приміщень та обладнання тощо. Для того, щоб вистояти у ці непрості часи, телекомунікаційні підприємства, шукають і опробовують нові стратегії, технології, інструменти, методи управління ризиками що передбачають: гармонізацію організаційного дизайну, оптимізацію бізнес-процесів, зростання ринкової частки за рахунок злиття чи поглинання з іншими телекомунікаційними підприємствами, підвищення якості та розширення спектру телекомунікаційних послуг, входження до світових телекомунікаційних ринків, вдосконалення інформаційних і комунікаційних управлінських ланцюгів тощо. Проте, вітчизняні реалії сьогодення унеможливають це завдання, оскільки, більшість телекомунікаційних підприємств, опираються на застарілу фрагментарну концепцію розбудови системи управління ризиками, яка ґрунтується на пасивній чи реактивній основі, опираються на інтуїтивне управління ризиками. В додатку 1.3 наведено характеристику різних концепцій. Цікаво, що зарубіжні телекомунікаційні підприємства здійснюють безперервне управління ризиками на превентивній, антисипативній основі за слабкими сигналами загроз. Настання відчутних змін в динамічному середовищі телекомунікаційного підприємства теж відбувається не водночас, фактично перед такими змінам завжди проявляються сигнали раннього попередження, слабкі сигнали. Адекватна ідентифікація яких може завчасно попередити про загрози та ризики, що наближаються. Тому, на часі, формування нової парадигми антисипативного управління ризиками в телекомунікаційних підприємствах, яка передбачає перехід від невизначеності до зрілості й гнучкості що базується на вище обґрунтованих принципах й враховує „слабкі сигнали”. І. Ансоф [3] трактує слабкий сигнал, як „один із інструментів управління”, вказуючи, що „це ранній сигнал, який важко відмітний від природних або нав'язаних шумів, можливо несе в собі ознаки настання важливих подій, а можливо й ні [3]. Тобто він окреслює слабкий сигнал як особливий інструмент управління невизначеностями.

Мельник О. Г., Адамів М. Є. наголошують, що, „управління по слабких сигналах можна сприймати як механізм попередньої адаптації до середовища або як антисипативне управління” [106]. Акцентуємо, що нові наукові підходи до формування управління ризиками мають будуватись на підґрунті передбачення, прогнозування настання різноманітних ризикових явищ, що зумовлюють зміни, тобто на підґрунті антиципації. „Антиципація” у дослівному перекладі з латини (*anticipatio*) означає – передбачення, уявлення предмета або явища в свідомості людини до того, як вони на практиці будуть сприйняті або реалізовані” [12]. У наявних наукових та спеціалізованих виданнях знаходимо близькі до окресленого вище поняття антиципація, розглянемо їх. „Антиципація – це: передбачення, випередження, завчасне розпізнавання можливого розвитку подій; передчасне настання будь-якого явища, яке повинне настати пізніше” [85]. „Антиципація – це: передчуття,

передбачення, сподівання, побоювання; передчасність наступу” [96]. „Антисипація – це: здатність людини уявити собі можливий результат дії до його здійснення, а також можливість його мислення уявити спосіб вирішення проблеми до того, як вона реально буде вирішена (інтуїція); здатність організму людини або тварини підготуватися до реакції на будь-яку подію до його настання” [1]. „Антисипація – це передчуття, передбачення, сподівання, короткочасне прогнозування розвитку подій в майбутньому” [8]. „Антисипація – це: передбачення, здогад, прогноз; передчасне настання якогось явища, дії; заздалегідь складене уявлення про що-небудь” [16]. „Антисипація – це: завчасна дія, яка бере до уваги чи передбачає подію, що відбудеться пізніше; погляд вперед; використання безготівкових грошей (які ще не є доступними); візуалізація майбутньої події; об’єкт або форма, що передбачає подальші явища; раннє звучання одного чи декількох тонів подальшого акорду, що формують тимчасовий дисонанс” [191]. „Антисипація – це: передбачення можливого розвитку подій; передчасне настання певного явища” [59]. Тобто, переважно дослідники, антисипацію визначають, як проактивну дію з розпізнання, передбачення, прогнозування та превентивного попередження настання певних процесів, подій, явищ. Відповідно антисипативне управління ризиками має передбачати і попереджувати настання кризових процесів, подій та ризикових явищ за ідентифікацією слабких сигналів. Р.А. Руденський [142] характеризує антисипативне управління як „управління, що базується на таких станах елементів складної системи і зовнішнього середовища, які ще не відбулися, але очікуються, що дозволяє підвищити рівень підготовки системи управління складним економічним об’єктом до появи і розвитку неочікуваних подій, як кризового характеру, так і зв’язаних з новими можливостями” [142].

В унісон такій характеристиці В.В. Прохорова стверджує [137], що „антисипативне управління передбачає раннє розпізнавання загроз середовища функціонування та розроблення випереджувальних управлінських дій щодо їхньої локалізації з метою забезпечення стійкого розвитку підприємства [137]. Опираючись на здійснений розгляд існуючих трактувань понять „антисипація” й „антисипативне управління”, визначимо антисипативне управління ризиками телекомунікаційних підприємств, як проактивний процес передбачення, прогнозування, сканування, розпізнання, обробки, ітерації та ідентифікації різноманітних сигналів щодо настання кризових процесів, подій та ризикових явищ що забезпечує гнучкість превентивного попередження їх впливу на основі збалансованості управлінських рішень та заходів щодо своєчасного нівелювання та мінімізації ризиків. Таке тлумачення дає змогу адекватно сформулювати дієвий методичний інструментарій антисипативного управління ризиками телекомунікаційних підприємств, конкретизувати джерела й площини витоків загроз та ризиків, ідентифікувати й оцінити потужність їх впливу, що забезпечить обґрунтованість, об’єктивність, адекватність і своєчасність ухвалення необхідних управлінських рішень і стратегій, сприятиме пошуку альтернативних сценаріїв ризикозахищеності та імплементації

результативних заходів стосовно нівелювання чи мінімізації ризиків. Тарасова Г.О. [155] засвідчує, що „застосування методу сканування в якості основного для проведення діагностики слабких сигналів, дозволяє завчасно виявити кризу, що насувається – початкове економічне явище, яке свідчить про те, що з’явилися ознаки зміни стану організації або зовнішнього середовища підприємства” [155]. І далі умотивовується „проведення діагностики за кількісною оцінкою інтенсивності сигналів, що дає можливість визначити цю інтенсивність (потужність, діапазон) на основі доступної інформації, виділення з „фонових шумів” істинного сигналу” [155]. М.М. Рубанов [141] обґрунтовує доцільність „використання системи раннього попередження загроз за слабкими сигналами, що має ґрунтуватись на тривірневій системі контролю, що включає попередній, поточний і заключний контроль. Кожен з даних видів контролю є своєрідним бар’єром, що дозволяє попередити виникнення відхилень, здатних істотно вплинути на підприємство, що, в свою чергу, дозволяє зробити висновок про доцільність застосування даної системи на практиці [141].

Варто виділити наступні характерні конститутивні атрибути антисипативного управління ризиками телекомунікаційних підприємств: превентивність: спрямована на випередження дії будь-яких потенційних ризикових явищ через своєчасне ухвалення та реалізацію відповідних управлінських рішень; систематичність: здійснюється постійно задля забезпечення високого рівня готовності підприємства до потенційних деформацій внутрішнього та коливань зовнішнього середовища у будь-який часовий період; стратегічна зорієнтованість: цілеспрямованість на досягнення визначеної мети підприємства та стратегічних завдань, пов’язана із подоланням, мінімізацією, нівелюванням потенційних ризиків на основі максимального використання ресурсних та інших можливостей підприємства; функціональність: здійснює розпізнавальну, попереджувальну, захисну, прогнозну, експертну, реагуючу, спостережну, інформаційну, превентивну функції задля підвищення результативності управління ризиками; комплексність: передбачає розробку портфеля альтернативних сценаріїв розвитку ризикових процесів задля забезпечення максимальної готовності підприємства до кожного із сценаріїв; відкритість: постійно сканує усі слабкі та латентні сигнали зовнішнього та внутрішнім середовища підприємства через сформовані інформаційні та комунікаційні прямі та зворотні ланцюги задля виявлення загроз і ризиків; адаптивність: швидко, безболісно та своєчасно пристосовується до деформацій внутрішнього та коливань зовнішнього середовища у будь-який часовий період; всеосяжність: спрямоване на сканування та розпізнання усіх можливих слабких та латентних сигналів зовнішнього та внутрішнім середовища щодо потенційних деформацій внутрішнього та коливань зовнішнього середовища та охоплює усі бізнес-процеси та бізнес-комбінації підприємства для виявлення загроз, ризиків та ресурсних можливостей у будь-який часовий період; адекватність: ухвалення управлінських рішень відбувається відповідно до виявлених загроз, ризиків та ресурсних можливостей на основі моделювання та прогнозування;

пріоритетність: здійснюється ранжування виявлених загроз, ризиків та ресурсних можливостей за ступенем їх вагомості, терміновості, інтенсивності й потужності впливу на функціонування підприємства та відповідно до розроблених стратегій.

Метою формування і впровадження антисипативного управління ризиками телекомунікаційних підприємств реаліях цифрових трансформацій варто визначити: удосконалення та активізація розвитку управління ризиками на основі високого рівня готовності підприємства до потенційних деформацій внутрішнього та коливань зовнішнього середовища у будь-який часовий період для забезпечення стабільності стратегічного розвитку підприємства за допомогою розробки і ухвалення збалансованих управлінських заходів зорієнтованих на превентивне подолання, нівелювання чи мінімізацію ризиків через максимальне використання ресурсних можливостей підприємства.

Відповідно до мети антисипативного управління ризиками телекомунікаційних підприємств реаліях цифрових трансформацій доцільно окреслити його ключові завдання: своєчасна безболісна адаптація підприємства до нових викликів та реалій сьогодення; ухвалення та реалізація превентивних рішень щодо реагування на трансформації, що передбачаються в перспективі; максимально результативне опрацювання від зайвого шуму усіх можливих слабких та латентних сигналів щодо потенційних деформацій внутрішнього та коливань зовнішнього середовища тощо.

Розглянемо загальний алгоритм антисипативного управління ризиками в телекомунікаційних підприємствах за допомогою m -слабкого сигналу з довільним впливом коливань $\alpha_1, \alpha_2, \dots, \alpha_m$ і сукупністю ризиків $\varphi_1, \varphi_2, \dots, \varphi_m$. За таких умов i -й варіант за слабкого сигналу матиме вигляд:

$$S_i(t) = \alpha_i \sin(\omega t + \varphi_i), \quad i = 1, 2, \dots, m. \quad (3.1)$$

В управлінському комунікаційному ланцюгу із гаусовським некореляційним шумом алгоритм прийому слабких сигналів (3.14) сформулюємо у наступний спосіб: фіксується i -й варіант слабкого сигналу, за умови, що $j \neq i$ справедливою буде нерівність:

$$\int_0^T [x(t) - S_i(t)]^2 dt < \int_0^T [x(t) - S_j(t)]^2 dt,$$

або: $i = \arg \min_j \int_0^T [x(t) - S_j(t)]^2 dt; \quad j = 1, 2, \dots, m. \quad (3.2)$

При антисипативному управлінні ризиками в телекомунікаційних підприємствах реаліях цифрових трансформацій зручно переходити від слабкого сигналу ризиків (3.1) до спектру багатоканальних сигналів ризиків. Так, на інтервалі проєкції слабкого сигналу ризиків $x(t)$ і сигналів (3.1) на передбачене коливання з амплітудою α_0 і сукупністю ризиків φ_0

$$\left. \begin{aligned} X_0 &= \int_0^T x(t) \alpha_0 \sin(\omega t + \varphi_0) dt; \\ Y_0 &= \int_0^T x(t) \alpha_0 \cos(\omega t + \varphi_0) dt; \end{aligned} \right\} \quad (3.3)$$

$$\left. \begin{aligned} X_j &= \int_0^T S_j(t) \alpha_0 \sin(\omega t + \varphi_0) dt; \\ Y_j &= \int_0^T S_j(t) \alpha_0 \cos(\omega t + \varphi_0) dt; \quad j=1, 2, \dots, m \end{aligned} \right\} \quad (3.4)$$

Тоді алгоритм антисипаційного управління ризиками в телекомунікаційних підприємствах реаліях цифрових трансформацій (3.2) можна представити

$$i = \arg \min_j [(X_0 - X_j)^2 + (Y_0 - Y_j)^2]; \quad j=1, 2, \dots, m. \quad (3.5)$$

Якщо слабкий сигнал ризику реаліях цифрових трансформацій відбувається на інтервалі N , тоді він $S_1(t)$ із гаусівським шумом матиме правдоподібне сприйняття X_1 і Y_1 :

$$\tilde{X}_1 = \frac{1}{N} \sum_{n=1}^N X_{0n}; \quad \tilde{Y}_1 = \frac{1}{N} \sum_{n=1}^N Y_{0n}, \quad (3.6)$$

де X_{0n} і Y_{0n} – проекції коливань (3.3) на інтервалі n -й. Сприйняття за виміром (3.5) вважаємо не перекрученим та об'єктивним. З них сформуємо об'єктивні оцінки проекцій коливань ризиків реаліях цифрових трансформацій і для інших альтернатив (3.4). Для цього, позначимо $\varphi_j = \varphi_1 + \Delta\varphi_j$ і трансформуємо проекцію коливань X_j в:

$$\begin{aligned} X_j &= \int_0^T \alpha_j \sin(\omega t + \varphi_0) \alpha_0 \sin(\omega t + \varphi_0) dt = \\ &= (\alpha_j / \alpha_1) \int_0^T \alpha_1 \sin(\omega t + \varphi_1 + \Delta\varphi_j) \alpha_0 \sin(\omega t + \varphi_0) dt = \\ &= (\alpha_j / \alpha_1) \left[\cos \Delta\varphi_j \int_0^T \alpha_1 \sin(\omega t + \varphi_1) \alpha_0 \sin(\omega t + \varphi_0) dt \right. \\ &\quad \left. + \sin \Delta\varphi_j \int_0^T \alpha_1 \cos(\omega t + \varphi_1) \alpha_0 \sin(\omega t + \varphi_0) dt \right] = \\ &= (\alpha_j / \alpha_1) \left[\cos \Delta\varphi_j \int_0^T \alpha_1 \sin(\omega t + \varphi_1) \alpha_0 \sin(\omega t + \varphi_0) dt - \right. \\ &\quad \left. - \sin \Delta\varphi_j \int_0^T \alpha_1 \sin(\omega t + \varphi_1) \alpha_0 \cos(\omega t + \varphi_0) dt \right] = \\ &= (\alpha_j / \alpha_1) (X_1 \cos \Delta\varphi_j - Y_1 \sin \Delta\varphi_j). \end{aligned} \quad (3.7)$$

Аналогічно, розрахуємо проекцію коливань ризиків Y_j . Замінивши X_1 і Y_1 їхніми параметрами, і буде:

$$\left. \begin{aligned} \tilde{X}_j &= (\alpha_j / \alpha_1) (\tilde{X}_1 \cos \Delta\varphi_j - \tilde{Y}_1 \sin \Delta\varphi_j); \\ \tilde{Y}_j &= (\alpha_j / \alpha_1) (\tilde{X}_1 \sin \Delta\varphi_j + \tilde{Y}_1 \cos \Delta\varphi_j); \end{aligned} \right\} \quad (3.8)$$

де $\Delta\varphi_j$ – різниця між слабкими сигналами ризиків $S_j(t)$ і $S_1(t)$.

Ключовими перевагами формування та впровадження антисипативного управління ризиками телекомунікаційних підприємств реаліях цифрових трансформацій можна визначити: підприємство має можливість заздалегідь розробити адекватні рішення до того, як загрози та ризики наберуть обертів та потужного впливу і своєчасно сформувати резерви та запаси для вирішення гострих проблем та реалізації нових можливостей; технології антисипативного управління ризиками за слабких та латентних сигналів сприяють моніторингу, експертизі, ідентифікації, діагностиці і розробці адекватних реакцій підприємства на деформації внутрішнього та коливання зовнішнього середовища, нові реалії та виклики сьогодення; можливість трансляції підприємством, деяких сильних, слабких чи латентних сигналів в оточення для інформування усіх контактних аудиторій; формування адекватного гнучкого гармонійного організаційного дизайну підприємства; розвиток компетентностей працівників підприємства та підвищення їх креативності.

Таким чином, у результаті проведеного дослідження систематизовано специфічні ризики підприємств телекомунікацій в залежності від бізнес-процесів, проаналізовані підходи до визначень поняття активізації в управлінні та запропоновано авторське визначення поняття «активізація управління ризиками підприємств телекомунікацій» як *«цілеспрямований вплив на систему управління ризиками підприємства телекомунікацій з виключення або зниження негативних наслідків настання ризикових подій для прискорення досягнення підприємством стратегічних цілей та цілей організаційних бізнес-процесів, процесів розвитку та підтримки»* з урахуванням специфіки ризиків в сфері телекомунікацій. Побудовано *трикутник напрямів активізації управління ризиками телекомунікаційних підприємств*, які взаємопов'язані між собою та охоплюють стадії процесу управління ризиками, співвідносяться до функцій менеджменту та є базою механізму управління ризиками телекомунікаційного підприємства. Проаналізовано принципи управління ризиками на підприємствах згідно з міжнародних стандартів, відомих моделей світових компаній та науковців й розроблено систему принципів з урахуванням специфіки телекомунікаційних підприємств, яка включає *загальноуправлінські, загальні принципи ризик-менеджменту та специфічні для підприємств телекомунікацій принципи*, використання яких сприятиме активізації управління ризиками на підприємстві.

Розроблені наукові підходи до формування антисипативного управління ризиками в телекомунікаційних підприємствах, що ґрунтуються на слабких чи

латентних сигналах щодо потенційних деформацій внутрішнього та коливань зовнішнього середовища і охоплює усі бізнес-процеси та бізнес-комбінації підприємства для виявлення загроз, ризиків та ресурсних можливостей у будь-який часовий період та враховують альтернативні сценарії розвитку ризикових процесів задля забезпечення максимальної готовності підприємства до кожного із сценаріїв дозволяють досягати мети щодо мінімізації чи нівелювання ризиків за визначеними часовими періодами на усіх ієрархічних управлінських рівнях та є підґрунтям для ухвалення результативних своєчасних тактичних й стратегічних інструментів і заходів для управління ризиками телекомунікаційних підприємств реаліях цифрових трансформацій, що сприятиме динамізму пошуку й формуванню резервів і запасів для стабільного розвитку підприємства та дозволить йому адекватно реагувати на турбулентні ризикові явища й виклики сьогодення, що на практиці сприятиме мати своєчасну об'єктивну ідентифікацію про стан ризикозахищеності телекомунікаційних підприємств та моделювати альтернативні траєкторії розвитку для досягнення позитивних результатів.

3.2. Модернізація механізму розвитку управління ризиками в телекомунікаційних підприємствах

На багатьох телекомунікаційних підприємствах, управління ризиками носить фрагментарний, досить поверховий характер. Одна із основних причин, що заважають розвитку управління ризиками в них, полягає в тому, що у керівництва телекомунікаційних підприємств немає ясного уявлення про механізм такого розвитку, не кажучи вже про переваги від модернізації цього механізму із запровадженням контрольно-дозвільної комплаєнс-функції та проактивних методів управління, що притаманні управлінню ризиками на підґрунті антиципації та інтеграції цього механізму в загальну систему управління.

Варто зазначити, що більшість ризиків та загроз є уніфікованими та повторюваними, вони виникають через об'єктивні чи суб'єктивні чинники впливу, саме тому менеджмент підприємства має розробляти конкретні чіткі правила реагування на будь-яку відому чи не відому ризикову ситуацію.

Акцентуємо, що комплаєнс-ризиками становлять велику небезпеку, оскільки можуть генерувати для підприємства події, пов'язані з великими збитками. Комплаєнс (англ. compliance – відповідність) – це здатність підприємства відповідати нормам та правилам, як зовнішнім, так і внутрішнім. Бути відповідальним за ведення бізнесу [173]. Комплаєнс-ризиками можуть вести до репутаційних втрат, що зумовлює втрату частини ринку, ділової репутації тощо. І тому, запровадження контрольно-дозвільної комплаєнс-функції набуває ключового значення у контурі інтеграції системи управління ризиками телекомунікаційних підприємств в загальну систему управління має бути присутнім на всіх ієрархічних рівнях.

Нині, загальноприйнятою точкою зору є, те що комплаєнс-ризиками генеруються, внаслідок виникнення різних форм конфлікту інтересів різних контактних аудиторій підприємства (від топ-менеджменту до рядових

виконавців), що призводить до невідповідності їх дій різним регламентам і нормативним документам, а також правовим зобов'язанням.

Практична реалізація контрольно-дозвільної комплаєнс-функції в сучасних телекомунікаційних підприємствах полягає у включенні контрольних елементів (контрольних точок) в основні бізнес-процеси. Тому комплаєнс-функцію у процесі інтеграції управління ризиками можливо поєднати з будь-якими бізнес-процесами підприємства. Фактично, комплаєнс може розглядати як сучасну концепцію здійснення контрольно-дозвільної функції управління ризиками на основі документально зафіксованих регламентів бізнес-процесів (у тому числі, технологічних процесів і операцій) і проектів. І, у цьому відношенні, він має високий потенціал застосування як елемент механізму розвитку управління ризиками. Особливо, в частині ризиків, пов'язаних з поведінкою персоналу, та його конфлікту інтересів.

Враховуючи те, що здійснення контрольно-дозвільної комплаєнс-функції будеться навколо ризиків конфлікту інтересів персоналу підприємства, спробуємо ідентифікувати види подібних конфліктів залежно від рівня регулюючих документів (регламентно-нормативної системи) з порушенням, яким пов'язані відповідні комплаєнс-ризиків.

Базовим різновидом конфлікту інтересів стейк-холдерів різного рівня, що веде до виникнення комплаєнс-ризиків, і, відповідно, ризиків технологічного характеру, є, загалом, конфлікт (суперечність) інтересів безпеки та інтересів отримання матеріальної вигоди різних стейк-холдерів у середньостроковій та короткостроковій перспективі. При довгостроковому плануванні суперечності між безпекою та вигодою не виникає через те, що збігаються інтереси стейк-холдерів: акціонерів, власників, інвесторів, а також суспільства в цілому. Тобто, матеріальна вигода збігається з альтернативною забезпечення безпеки, збереження майна, цінностей, а також відсутності шкоди для зовнішніх сторін, яка пов'язана із суттєвими втратами на відшкодування завданої шкоди, репутаційними втратами.

Реалізація даних протиріч, як правило, може виражатися в наступних формах:

1) Конфлікту інтересів безпосередніх виконавців, що призводить до суперечності бізнес-практик (бізнес-процесів та поведінки окремих виконавців) стандартам і регламентним нормам управління підприємства, що веде до зниження технічної безпеки (ризиків поведінкового та виконавчого комплаєнсу персоналу). При цьому, можна відзначити наявність конфлікту інтересів, що веде до виникнення комплаєнс – ризиків: коли порушення регламентуючих документів здійснюються на користь отримання матеріальної вигоди безпосереднім виконавцем (це може статися при порушенні техніки безпеки при виконанні робіт з метою підвищення продуктивності, скорочення часу виконання операції, порушення технічних умов і стандартів операцій тощо).

2) Конфлікту інтересів операційного менеджменту, коли керівники, з метою отримання власної вигоди (як правило, досягнення власних високих оцінок ефективності – KPI та інших, з отриманням відповідного матеріального чи нематеріального, наприклад, підвищення за посадою заохочення)

примушує нижчестоящих працівників до порушення регламентів здійснення операцій, бізнес-процесів та регулюючого законодавства (зазначимо, що конфлікти інтересів цього роду вступають у протиріччя з інтересом решти стейк-холдерів підприємства: топ-менеджменту, власників, інвесторів, акціонерів, держави й суспільства).

3) Конфлікту інтересів вищого менеджменту, внаслідок чого, як правило, може виникати протиріччя стандартів і регламентів (регламенти технологічних та бізнес-процесів, регламенти роботи, технічні умови тощо) управління підприємством із системою технічного регулювання та законодавства. Метою подібних порушень є підвищення показників ефективності підприємства (прибуток, виручка, обсяг виробництва) за рахунок ігнорування вимог технічної безпеки, природоохоронного законодавства, нормативів щодо захисту здоров'я та природних ресурсів. В даному випадку, інтереси власної вигоди вищого менеджменту (в результаті отримання особистої матеріальної та нематеріальної винагороди за високі операційні та фінансово-економічні результати підприємства) протиставляються інтересам власне підприємства, його акціонерам чи власникам, інвесторам, а часто й інтересам безпосередніх виконавців.

4) Конфлікту інтересів підприємства законним інтересам її контрагентів, протиріччя діяльності підприємства її правовим зобов'язанням (у тому числі цивільно-правовим), а також законним інтересам третіх осіб та організацій (цивільно-правові комплаєнс-ризиків).

Результатом реалізації комплаєнс-ризиків пов'язаних з конфліктом інтересів всіх названих типів, якщо вони своєчасно не ідентифікуються механізмом управління ризиками телекомунікаційного підприємства і не усуваються, можуть бути небажані наслідки. Наприклад, правового характеру (не пов'язані безпосередньо з настанням подій технологічного ризику, викликаних з комплаєнс-ризиками): пред'явлення позовів, вимоги регулюючих органів про усунення порушень або про припинення діяльності, відкликання ліцензій, кримінальне переслідування керівників та виконавців, штрафні санкції. Всі ці наслідки впливають на фінансово-економічне становище телекомунікаційного підприємства, як у результаті виникнення безпосередніх витрат, і опосередковано у вигляді:

репутаційних витрат, втрати ділової репутації, зниження вартості бізнесу, втрати лояльності клієнтів і ринків збуту тощо;

реалізації подій технологічного ризику всіх типів: як аварійного, процесного, проектного та операційного.

Практично, безпосередня реалізація подій комплаєнс-ризиків, як правило, не обмежується для підприємства тільки безпосередньо пов'язаними з ними втратами, а й переважно супроводжується, виникненням наслідків правового і репутаційного характеру.

У процесі модернізації механізму розвитку управління ризиками та його інтеграції у загальне управління телекомунікаційного підприємства пропонується забезпечити реалізацію контрольно-дозвільної комплаєнс-функції наступним:

1) консультаційною підтримкою, що передбачає підтримку підрозділів підприємства у формі консультацій щодо нормативно-правового регулювання, у тому числі відстеження поточних змін регулювання та інформування про зміни;

2) постійним навчанням та підвищенням кваліфікації, що передбачає навчання персоналу щодо проблем комплаєнсу, інформуванні персоналу про поточний стан нормативно-правових документів, що регулюють їхню діяльність, роз'ясненні різних аспектів використання різноманітних регламентів, стандартів та нормативів та здійсненні діяльності в рамках існуючих бізнес-процесів;

3) формуванням комплаєнс-культури у персоналу телекомунікаційного підприємства, у тому числі, технологічного комплаєнсу – культури безпеки;

4) аналітичною підтримкою – виявлення, оцінка та аналіз поточних та потенційних комплаєнс-ризиків, зумовлених як конфліктами інтересів різного роду, так і змінами нормативно-правової та регламентної бази;

5) контролінгом – оцінка регламентів та практики бізнес-процесів (включаючи технологічні процеси) підприємства, з погляду, відповідності (комплаєнса) існуючій нормативно-правовій базі, іншим регламентам, правилам і стандартам, а також цивільно-правовим зобов'язанням підприємства [158].

Контрольно-дозвільна комплаєнс-функція телекомунікаційного підприємства може здійснюватися трьома способами:

дозвільним порядком, коли рішення виконавчих органів (накази та розпорядження, регламенти, інструкції, зміни до нормативних актів підприємства та підрозділів) щодо здійснення діяльності телекомунікаційного підприємства підлягають обов'язковому схваленню органу, відповідального за комплаєнс, як правило, вищого керівництва;

повідомчим порядком (методом моніторингу), коли інформація про прийняті рішення, здійснені дії та результати передається до підрозділу телекомунікаційного підприємства відповідального за комплаєнс. З метою проведення аналізу, видачі оцінок законності та обґрунтованості рішень і дій, вироблення рекомендацій щодо вдосконалення діяльності (при цьому визначається порядок, періодичність і склад ситуацій) вони спочатку повідомляються у відповідні органи комплаєнсу. Наприклад, рішення про зміну технологічних та експлуатаційних параметрів (у рамках допустимих діапазонів, інформації щодо збоїв та помилок в процессах, аварійних ситуаціях тощо);

методом вибіркового спостереження – аудиту діяльності. Дана форма важлива для виявлення латентних комплаєнс-ризиків виробництва.

В механізмі розвитку управління ризиками телекомунікаційного підприємства можна виділити такі типи управлінських рішень:

стратегічні (довгострокові) рішення, коли процес розробки рішення (вираженого, як правило, у формі регламентного, нормативного документа або цивільно-правового акту (договору) займає досить тривалий час, що допускає включення етапу узгодження з відповідним підрозділом комплаєнсу, причому,

прийнятті рішення мають тривалий період дії (місяці, роки), до цього типу рішень слід віднести рішення щодо комплаєнс-ризиків, що відповідають конфлікту інтересів другого та третього типу: вищого менеджменту та самого підприємства щодо своїх зобов'язань.

тактичні (короткострокові) рішення, коли процес ухвалення рішення займає стислий час, рішення має виконуватися (застосовуватися) негайно, і, як правило, має обмежений час дії (конкретний цикл виробничої операції, виробнича зміна, доба), що не дозволяє, як правило, включити етап узгодження з відповідним підрозділом комплаєнсу, такі рішення відповідають за виконання оперативних виробничих завдань і відносяться до компетенції лінійного менеджменту підприємства та безпосередніх виконавців (від оператора обладнання до керівника робіт, виробничої ділянки, цеху) і співвідносяться з комплексними ризиками, зумовленими конфліктом інтересів першого типу, який характерний для рівня операційного персоналу.

Відповідно, три різні вектора дії контрольно-дозвільної комплаєнс-функція необхідні для модернізації механізму розвитку управління ризиками на різних його ієрархічних управлінських рівнях. Для стратегічних рішень управління ризиками, основним способом реалізації контрольно-дозвільної комплаєнс-функції може бути використання дозвольного порядку з використанням аудиту/вибіркового контролю (як допоміжний спосіб). При цьому використання дозвольного контролю має здійснюватися в тісному зв'язку із здійсненням консультативної підтримки.

Для тактичних рішень управління ризиками основним способом реалізації контрольно-дозвільної комплаєнс-функції є поєднання сповіщувального порядку, спільно з регулярним аудитом/вибірковим контролем. Використання дозвольного контролю, при даному типі управлінських рішень, як допоміжний тип можливе, а, в деяких випадках, функціонування технологічної системи підприємства необхідно (робота в перехідних, нестійких режимах, проведення випробувань і пусконаладжувальних робіт, освоєння нової продукції/послуг/технологій тощо). Однак, у цьому випадку, контрольно-дозвільна комплаєнс-функція повинна делегуватися вищому рівню менеджменту, що володіє достатніми не тільки компетенціями комплаєнс-контролю, а й технічними.

Для підсилення контрольно-дозвільної комплаєнс-функції в механізмі розвитку управління ризиками в телекомунікаційних підприємствах, доцільно використання проактивних методів управління ризиками. Поняття „проактивності” введено в науковий вжиток теорії ризиків в кінці минулого століття, фактично як протиставлення реактивності, тобто реагування на ризикові події за певних обставин. На противагу реактивним методам управління ризиками, характерними рисами проактивних слід вважати:

завчасна розробка спектру превентивних і випереджуючих заходів щодо відвернення чи мінімізації настання ризикових процесів із чітким окресленням результатів і відповідальності за ухвалення відповідних рішень;

прогнозування ризикових явищ та завчасна ідентифікація потенційних загроз і їх наслідків у стратегічному горизонті;

генерування ініціатив персоналом підприємства щодо конфігурації вибору та використання методів управління ризиками, а не реактивне пристосування до нових умов;

розробка інноваційних і креативних підходів до вибору та використання методів управління ризиками для результативного розв'язання існуючих чи нових проблем і завдань підприємства;

комплекс методів управління ризиками зорієнтований на стратегічну перспективу;

широке застосування сценарного підходу до прогнозування настання і наслідків ризикових процесів;

впровадження різноманітних цифрових комунікаційних ланцюгів та сучасних інформаційно-комунікаційних технологій.

Тобто, формування системи проактивних методів управління ризиками телекомунікаційних підприємств передбачає: ініціативність, випереджувальність, зорієнтованість, стратегічність, превентивність щодо уникнення прояву ризикових явищ і їх наслідків та максимізацію позитивних ефектів із впровадженням новаторських і креативних підходів. Фактично, проактивність передбачає вибір методів управління ризиками перед тим, як ризикові явища настануть, тобто вплив ризикових процесів прогнозується, і відповідно будується стратегія управління ризиками та розробляється спектр сценаріїв їх нівелювання чи мінімізації.

Узагальнюючи, відмітимо, що проактивні методи управління ризиками телекомунікаційних підприємств – це сукупність певних дій і заходів підприємства, які передбачають превентивне формування і використання динамічних здатностей і нових компетенцій, зорієнтований потужний вплив на конфігурацію ризиків і загроз на підґрунті прогнозування й моделювання розвитку ризикових процесів та примноження ініціативності й креативності персоналу підприємства.

Для впровадження проактивних методів управління ризиками в телекомунікаційних підприємствах доцільно виділити спектр необхідних заходів: своєчасне виявлення різноманітних ризиків (ідентифікація, діагностика, регулювання, моніторинг і контроль за окремими блоками ризиків і загроз); розробка та реалізація програми щодо мінімізації витрат і забезпечення результативності усіх бізнес- процесів, коригування заходів у разі настання форс-мажорних ситуацій; своєчасне здійснення аудитів бізнес-процесів та комунікаційних ланцюгів, аналіз їх результативності та контрольованості; формування стратегії ризикозахищеності підприємства із конкретними планами і заходами щодо мінімізації чи нівелювання ризиків; жорсткий контроль за фінансовими потоками підприємства; розробка альтернативних сценаріїв розвитку ризикових процесів та виміру їх наслідків у стратегічному горизонті з урахуванням усіх потенційних ризиків та загроз; формування „фінансової безпекової подушки”, що дасть змогу забезпечити ризикозахищеність підприємства та у разі настання ризикових явищ швидко відновити необхідні бізнес-комбінації (актуальність та необхідність її формування підтвердилось процесами поширення пандемії COVID-19 та

неочікуваним впровадженням воєнного часу в країні на тривалий період, оскільки жодне телекомунікаційне підприємство не було готово до них, проте підприємства, у яких вони були сформовані, змогли витримати жорсткий локдаун, а під час дії воєнного стану відновлюють своє функціонування, і навіть диверсифікують напрями своєї діяльності).

Для фільтрації й формування проактивних методів управління ризиків в телекомунікаційних підприємствах доцільно врахувати низку чинників: складність системи управління і організаційного дизайну підприємства, технології і якість та ефективність надання послуг чи продуктів, збалансованість розподілу управлінських функцій, складність алгоритмів бізнес-процесів, процедури взаємодії з усіма контактними аудиторіями, вимоги до компетентностей персоналу, обсяг інформаційних потоків, часові параметри для вирішення проблеми, запити партнерів та клієнтів, кількість вузлів і користувачів, стратегічні пріоритети і орієнтири підприємства, рівень цифрової зрілості підприємства, гнучкість розкладів і графіків, стабільність напрямів діяльності та команди підприємства, технологічна інфраструктура підприємства. Акцентуємо, що результативність проактивних методів управління ризиками помітно залежить від належного організаційного та інформаційного забезпечення, оскільки необхідна оперативна інформація для ухвалення відповідних заходів, а сучасний розвиток діджиталізації усіх бізнес-процесів вносить помітні зміни в обробку інформаційних потоків, водночас, важливо враховувати рівень компетентностей управлінського персоналу щодо забезпечення бажаної результативності рішень з управління ризиками.

Доцільно використовувати оптимізацію динамічного, лінійного програмування й економіко-математичне моделювання для оцінки масштабів ризикових процесів підприємства та їх наслідків, що дасть змогу використати її при здійсненні діагностики ризикозахищеності підприємства, виявленні тенденцій розвитку ризикових подій, оцінюванні результативності методів управління ризиками та ухвалення відповідних управлінських заходів.

Так, зокрема, коливання проекції ризиків X_{1n} і Y_{1n} за слабким сигналом на n -й інтервалі розрахуємо через бажані проекції коливань ризиків X_{0n} і Y_{0n} за рівнянням:

$$\left. \begin{aligned} X_{1n} &= (\alpha_1 / \tilde{\alpha}_n) (X_{0n} \cos \Delta \tilde{\varphi}_n + Y_{0n} \sin \Delta \tilde{\varphi}_n); \\ Y_{1n} &= (\alpha_1 / \tilde{\alpha}_n) (Y_{0n} \cos \Delta \tilde{\varphi}_n - X_{0n} \sin \Delta \tilde{\varphi}_n). \end{aligned} \right\} \quad (3.9)$$

Показники $\tilde{\alpha}_n$ і $\Delta \tilde{\varphi}_n$ визначаються управлінськими рішеннями щодо використання проактивних методів у на n -й альтернативі слабого сигналу ризиків, прийнятого за результатами опрацювань X_{0n} і Y_{0n} .

Показники (3.9) усереднюються:

$$\left. \begin{aligned} \tilde{X}_1 &= \frac{1}{N} \sum_{n=1}^N \frac{\alpha_1}{\tilde{\alpha}_n} (X_{0n} \cos \Delta \tilde{\varphi}_n + Y_{0n} \sin \Delta \tilde{\varphi}_n); \\ \tilde{Y}_1 &= \frac{1}{N} \sum_{n=1}^N \frac{\alpha_1}{\tilde{\alpha}_n} (Y_{0n} \cos \Delta \tilde{\varphi}_n - X_{0n} \sin \Delta \tilde{\varphi}_n). \end{aligned} \right\} \quad (3.10)$$

Таким чином, алгоритм гармонізації використання проактивних методів управління ризиками в телекомунікаційних підприємствах за багатопозиційними слабкими сигналами набуває вигляд:

$$i = \arg \min_j [(X_{0n} - \tilde{X}_j)^2 + (Y_{0n} - \tilde{Y}_j)^2], \quad j = 1, 2, \dots, m, \quad (3.11)$$

де \tilde{X}_j і \tilde{Y}_j визначаються за (3.10).

Альтернативи використання проактивних методів управління ризиками в телекомунікаційних підприємствах враховуючи векторність, амплітуду коливань та потужність сигналів, можуть окреслюватися наступними рівняннями:

$$\begin{aligned} \alpha_3/\alpha_1 &= \alpha_7/\alpha_1 = \alpha_{11}/\alpha_1 = \alpha_{15}/\alpha_1 = 3; \\ \alpha_2/\alpha_1 &= \alpha_4/\alpha_1 = \alpha_6/\alpha_1 = \alpha_8/\alpha_1 = \alpha_{10}/\alpha_1 = \alpha_{12}/\alpha_1 = \\ &= \alpha_{14}/\alpha_1 = \alpha_{16}/\alpha_1 = \sqrt{5}; \quad \alpha_5/\alpha_1 = \alpha_9/\alpha_1 = \alpha_{13}/\alpha_1 = 1. \end{aligned} \quad (3.12)$$

Зауважимо, що для деяких альтернатив зручно визначити безпосередньо $\cos \Delta \varphi_j$ і $\sin \Delta \varphi_j$, і матимемо:

$$\left. \begin{aligned} \sin \Delta \varphi_4 &= \sin(\varphi_4 - \pi/4) = \frac{1}{\sqrt{2}} (\sin \varphi_4 - \cos \varphi_4) = \\ &= \frac{1}{\sqrt{2}} \left(\frac{y_4}{\sqrt{x_4^2 + y_4^2}} - \frac{x_4}{\sqrt{x_4^2 + y_4^2}} \right) = \frac{1}{5}; \\ \cos \Delta \varphi_4 &= \cos(\varphi_4 - \pi/4) = (1/\sqrt{2})(\sin \varphi_4 + \cos \varphi_4) = 2/\sqrt{5}. \end{aligned} \right\} \quad (3.13)$$

Таким чином, при дії сукупності ризиків за даної альтернативи слабого сигналу гармонійна система проактивних методів згідно (3.11), (3.12) і (3.13) буде мати вигляд:

$$X_{1n} = \frac{1}{5}(2X_{0n} + Y_{0n}); \quad Y_{1n} = \frac{1}{5}(2Y_{0n} - X_{0n}). \quad (3.14)$$

Аналогічно, для іншої альтернативи одержимо $\sin \Delta \varphi_2 = -1/\sqrt{5}$, $\cos \Delta \varphi_2 = 2/\sqrt{5}$, а сукупність проактивних методів розрахуємо:

$$\left. \begin{aligned} X_{1n} &= \frac{1}{5}(2X_{0n} - Y_{0n}); \\ Y_{1n} &= \frac{1}{5}(2Y_{0n} + X_{0n}). \end{aligned} \right\} \quad (3.15)$$

Наочно гармонізацію використання проактивних методів управління ризиками в телекомунікаційних підприємствах наведено на рисунку 3.3, а алгоритм відбору та використання проактивних методів управління ризиками в телекомунікаційних підприємствах наведено на рисунку 3.4.

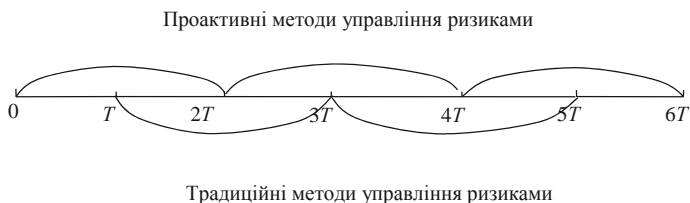


Рис. 3.3. Гармонізація використання проактивних методів управління ризиками в телекомунікаційних підприємствах

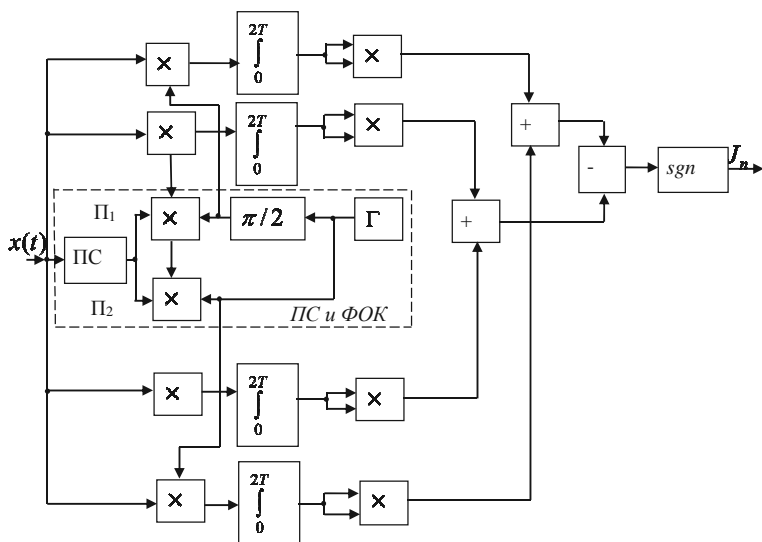


Рис. 3.4. Алгоритм відбору та використання проактивних методів управління ризиками в телекомунікаційних підприємствах

Крім того, система проактивних методів управління ризиками має включати:

мозковий штурм (для ідентифікації джерел загроз, ризиків та кількісної оцінки наслідків їх настання);

метод Делфі (для генерування і акумуляції експертних знань і думок щодо джерел загроз, ризиків та ефектів наслідків їх настання);

SWOT аналіз (для визначення слабких та сильних сторін кожного використання кожного методу управління ризиками);

сценарне комп'ютерне моделювання (для визначення ймовірності та масштабів настання ризикових подій, розробки різних сценаріїв розвитку ризикових процесів та виміру їх наслідків на основі методу теорії ігор, зокрема Монте-Карло);

карту ризиків (для систематизації наявних та прогнозованих загроз і ризиків та їх оцінки у розрізі бізнес-процесів та управлінських підрозділів).

Проактивність методів управління ризиками телекомунікаційного підприємства необхідна при динамізмі настання ризикових подій, складності й турбулентності економічного простору.

При чому, акцентуємо, що чим більш динамічними, турбулентними, складними і невизначеними є прояви економічного простору, тим потужнішими і проактивнішими мають бути методи управління ризиками телекомунікаційного підприємства.

Саме тому рекомендується модернізований механізм розвитку управління ризиками із запровадженням контрольно-дозвільної комплаєнс-функції та проактивних методів управління, що притаманні управлінню ризиками на підґрунті антиципації інтегрувати до процесу управління телекомунікаційним підприємством з метою поліпшення ефективності прийняття управлінських рішень, отримання ефекту постійності економічного поступу, врегулювання і збереження на високому рівні стану ризикозахисності підприємства.

„Через те, що фундаментом механізму розвитку управління ризиками виступає стійкий, ефективно функціонуючий комплекс захисту, який базується на концепції побудови та реалізації плану ефективного застосування ресурсів підприємства, можливостей та потенціалу, протидії руйнуючій дії зовнішнього та внутрішнього середовищ, вирішальним компонентом у створенні сучасної системи управління підприємством виступає її інтеграція з системою ризик-менеджменту” [93].

Можна виділити наступні напрями інтеграції модернізованого механізму розвитку управління ризиками в загальне управління телекомунікаційного підприємства:

швидке виявлення операційних ризиків, а саме запуск процесу ідентифікації, оцінки, регулювання та моніторингу ризиків при створенні річного плану та звітності за окремими групами ризиків;

створення та реалізація програми, яка б забезпечила мінімальні операційні витрати (передусім, елементи матеріальних витрат), забезпечення результативності усіх бізнес- процесів, коригування планів в разі ліквідації форс-мажорних ситуацій;

у конкретно визначені терміни проведення аудитів бізнес-процесів підприємницької діяльності, аналіз їх ефективності та контрольованості (менеджмент має впроваджувати моніторинг на основі проведених перевірок, результати цих перевірок мають бути оголошені усім відділам та структурним підрозділам телекомунікаційного підприємства);

для мінімізації результатів ризиків потрібно активно впроваджувати страхування (на підприємстві має бути створений Департамент внутрішнього контролю, аудиту та ризик-менеджменту, який забезпечував би популяризацію ідеї страхового захисту та злагоджений зв'язок між усіма відділами та службами);

з метою мінімізації ризиків та гарантування економічної безпеки підприємства формується і впроваджується стратегія сталого розвитку підприємства з врахуванням розроблених планів захисту від ризиків;

формування механізму управління фінансовими потоками (дасть можливість швидкого реагування у внутрішньому та зовнішньому середовищах, забезпечить високу ліквідність та платоспроможність підприємству);

побудова альтернативних сценаріїв зміни зовнішнього середовища, досягнення стратегічних цілей з урахуванням усіх можливих ризиків, регулювання різнобічних ситуацій з призначенням відповідальних осіб у кожному відділі чи підрозділі;

створення спеціального фонду так званої „фінансової подушки безпеки”, що дозволить у разі настання критичної ситуації мати кошти на відновлення усіх бізнес-процесів.

Особливо така форма стала актуальною при поширенні пандемії COVID-19 та воєнної ситуації в країні, оскільки жодні прогнози чи системи ризик-менеджменту не були готові до таких подій. Лише ті підприємства, які мали спеціальні фонди, змогли протриматись в умовах жорсткого локдауну, а зараз під час війни мають можливість відновлювати свою роботу або переорієнтовуватись у інші сфери діяльності [165]. Доцільно інтеграцію механізму розвитку управління ризиками у загальну систему управління телекомунікаційних підприємств, здійснювати за наступними принципами:

1. *Принцип контрольованості*: всі види діяльності повинні бути контрольованими, механізм розвитку управління ризиками має охоплювати всі функціональні підрозділи підприємства;

2. *Принцип збалансованості*: проведення економічної діагностики при прийнятті рішень щодо втрат та можливостей;

3. *Принцип комплексності*: механізм розвитку управління ризиками функціонує з єдиною базою відповідних принципів та методів з врахуванням характеру та взаємодії їх впливу, визначенням можливих наслідків подій;

4. *Принцип безперервності*: постійний моніторинг змін у внутрішньому та зовнішньому середовищі з внесенням нової інформації для механізму розвитку управління ризиками.

5. *Принцип комплаєнс-захисту*: запобігання потенційних втрат і юридичних санкцій через недотримання законів або правил ведення бізнесу.

Методичний підхід щодо інтеграції модернізованого механізму управління ризиками в механізм управління телекомунікаційного підприємства наведено на рисунку 3.5.

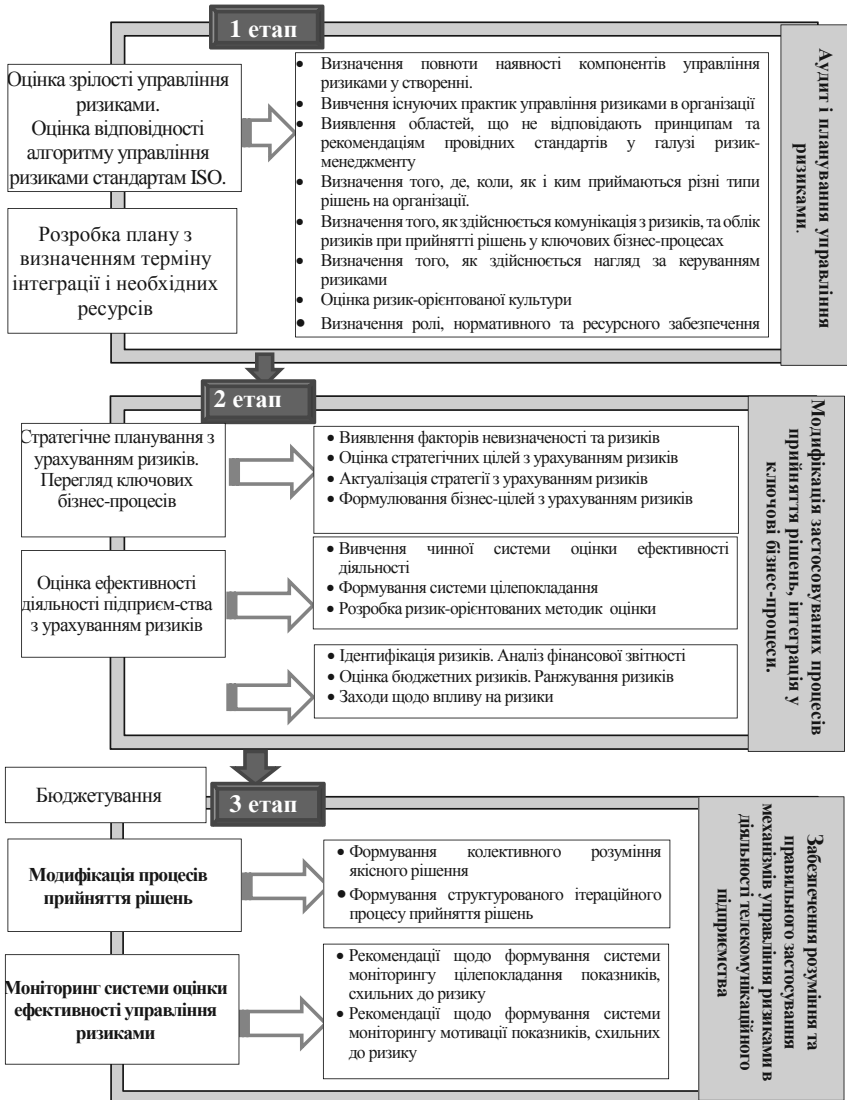


Рис. 3.5. Методичний підхід щодо інтеграції модернізованого механізму управління ризиками в механізм управління телекомунікаційного підприємства (запропоновано автором)

Він складається із трьох основних етапів:

Етап 1 – аудит управління ризиками, розробка відповідного плану з визначенням термінів інтеграції та необхідних для цього ресурсів.

Етап 2 – модифікації застосовуваних процесів прийняття рішень, інтеграція у ключові бізнес-процеси.

Етап 3 – забезпечення розуміння та правильного застосування механізму розвитку управління ризиками в діяльності телекомунікаційного підприємства.

Таким чином, запропоновано науковий підхід до модернізації механізму розвитку управління ризиками в телекомунікаційних підприємствах на основі поєднання та ієрархічного структурування контрольної-дозвільної функції та запровадження проактивних методів управління на підґрунті антиципації та його інтеграції в загальне управління телекомунікаційного підприємства з врахуванням організаційної структури, поведінки, культури й бізнес-контексту, що є динамічним та ітеративним процесом, що сприятиме розробці комплексу стратегічних рішень та альтернативних сценаріїв, зорієнтованих на забезпечення спектральної гнучкості ризикозахисності телекомунікаційних підприємств за допомогою передбачення та нівелювання різноманітних ризикових явищ та побудови надійних інформаційних й комунікаційних ланцюгів. Перевагою запропонованого проактивних методів управління ризиками слід вважати, що вони враховують специфіку діяльності телекомунікаційних підприємств та передбачають градацію відповідних заходів щодо зниження ризиків за пріоритетністю, сприяють розробці комплексу стратегічних рішень та альтернативних сценаріїв, зорієнтованих на забезпечення спектральної гнучкості ризикозахисності телекомунікаційних підприємств за допомогою передбачення та нівелювання різноманітних ризикових явищ та побудови надійних інформаційних та комунікаційних ланцюгів що дозволить розв'язати проблему виживання та використати потенційні можливості телекомунікаційного підприємства щодо його стабільного успішного розвитку в стратегічному горизонті.

3.3. Нові інструменти страхування та методи управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації

Незважаючи на безумовні переваги цифровізації економіки (розвиток ІКТ, Dig Data, штучного інтелекту, технології блокчейну, хмарних обчислень, створення сучасних матеріалів, впровадження нових дифузних моделей управління), з'являються і новітні ризики, генеровані використанням новітніх цифрових технологій, що можуть негативно впливати на результати функціонування телекомунікаційних підприємств. Це зумовлює впровадження та використання нових інструментів та методів страхування для управління ризиками в реаліях цифрових трансформацій. Саме тому питання, пов'язані з активізацією та розширенням можливостей нових інструментів та

методів страхування їх адаптації до цифрових перетворень в економічному просторі, набувають сьогодні особливої актуальності.

Окремі теоретичні положення щодо проблем впровадження та використання нових інструментів та методів страхування для управління ризиками в реаліях цифрових трансформацій розкрито у наукових розвідках таких відомих вчених, як Л. Алексеевко, В. Базилевич, В.П. Братюк, О. Вірбулевської, С. Волосович, О.О. Гаманкової, В. Гесць, В. Діби, Ю. Кожедуб, Р. Пікус, О. Пономарьової, Н. Приказюк та інших учених. Проте, зважаючи на важливість та актуальність окресленої проблематики, існує необхідність більш глибокого її розкриття та розробки пропозицій щодо передумов активізації та розширення переліку нових інструментів та методів страхування для управління ризиками в реаліях цифрових трансформацій.

Визначальною ознакою цифрових трансформацій вважається зміна структури та вагомості факторів виробництва, ключовим із яких стає інформація. „Опрацювання значних обсягів даних та використання результатів їх аналізу дозволяють значно підвищити ефективність різноманітних виробництв, технологій та обладнання, зберігання, продажу і постачання товарів й послуг” [220].

Відбувається digital - трансформація бізнесу, що зумовлює генерування нових ризиків. „Розумні” пристрої та інноваційні послуги можуть спровокувати непередбачені негативні наслідки та появу специфічних надскладних загроз (крадіжка інформації, збої комунікацій та цілих виробничих комплексів і логістичних ланцюгів). Так, за звітними даними Міжнародного економічного форуму (World Economic Forum) по глобальним ризикам, віртуальні (кібер) ризики означені, найголовнішими комерційними ризиками. Підтверджують таке ствердження і аналітичні дані компанії Global Corporate & Specialty, які аналізували ризики щодо ведення бізнесу.

Їх дані демонструють, що кібер-ризик є найнебезпечнішими для провадження бізнесу. Так, сумарні втрати світової економіки від їх реалізації становили у 2015 році близько 445 мільярдів доларів [221 с. 10], а вже у 2017 році – 600 мільярдів доларів [224]. За аналізом Страхового брокера „ІНСАРТ” – 25 млн. дол. США – понесений збиток українським бізнесом в результаті кібер-атак, близько 50% вітчизняних компаній мали справу з кібер- атаками; більш ніж 125000 комп’ютерів було заражене внаслідок кібер-атаки вірусу Retya.A, а розмір збитків склав 466,3 млн. доларів США [224]

Більшість вчених, вважають, що кібер-ризик – це ризик, що генерується використанням: телекомунікаційного обладнання, програмного забезпечення, локальних і Інтернет-мереж, розрахунково-платіжних систем, систем інтернет-торгівлі, промислових систем менеджменту, а також це ризик, що пов’язаний з накопиченням, зберіганням, передачею і використанням персональних даних.

Змістове наповнення кібер-ризиків розкривається через їх особливості [212]:

об’єктом зазіхань (потенційної втрати) є дані (інформація) (нематеріальні активи), що несанкціоновано видаляються, спотворюються,

порушується їх конфіденційність або унеможливується доступ до них (неавторизоване розкриття, зміна або руйнування цифрових активів);

підмножина сукупних ризиків, які відносяться одночасно до ризиків ІТ та інформаційної безпеки;

це ризики реалізації навмисних злочинних дій за допомогою використання ІТ;

результати настання кібер-ризиків можуть розглядатися з позиції видів завданих збитків (фінансовий і майновий) та суб'єктів наслідків їх реалізації (1-ша особа, 3-тя особа).

Кібер-ризики проявляються внаслідок настання таких подій:

нецільові атаки (фішинг, кардинг, sms-шахрайство);

цільові атаки (фінансове шахрайство, розкрадання баз даних, промислове шпигунство, DDoS атаки, вимагання);

атаки зсередини (розкрадання, знищення інформації, сприяння цільовій атаці).

Отже, у контексті збільшення чисельності кібер-злочинів, телекомунікаційним підприємствам необхідно розробляти шляхи їх мінімізації. Для цього використовують: технологічні рішення, просвітницьку діяльність щодо протидії кібер-злочинів, профілактичні заходи та кібер-страхування.

Кібер-страхування за ствердженням Р. Беме і Г. Шварца: це передача фінансового ризику, пов'язаного з мережевими та комп'ютерними інцидентами, третій стороні [222]. Фактично, кібер-страхування – це страховий продукт, який захищає економічні суб'єкти від ризиків, що відносяться до інформаційно-комунікаційних технологій, використання Інтернет - мережі, ІКТ-інфраструктури та діяльності у кібер-просторі.

Страховий ринок змушений адекватно реагувати на окреслені digital – трансформації і широке генерування кібер-ризиків, „зادля максимального задоволення потреб і побажань своїх клієнтів з метою їх страхового захисту в частині удосконалення підходів до ведення бізнесу, розробки інноваційних каналів реалізації продуктів і надання послуг та технологій обслуговування” [216 с. 49].

Нині, рівень розвитку вітчизняного страхового ринку окреслюється: соціально-економічними реаліями в країні, готовністю економічних суб'єктів до споживання якісно нових страхових послуг, а також державною підтримкою. „Порівняно з європейськими країнами, де страхування охоплено понад 94% страхового поля, в Україні страхові послуги користуються значно меншим попитом (10–15% страхового поля), особливо у галузі майнового та окремих видів особистого страхування, що зумовлено як низькою довірою економічних суб'єктів до страховиків, так і низьким рівнем їхньої обізнаності у сфері страхування” [219]. Так, за ствердженням аналітиків, „частка страхових платежів за особистим страхуванням в Україні становить усього 4-5%, тоді як у Західній Європі та США цей вид послуг займає близько 60%, у Японії – 80%, у Великобританії – 70%, а у світі в середньому – 58,3%. Загальний обсяг страхових послуг на фінансовому ринку

України в останньому десятиріччі за зібраними преміями дорівнював 0,06% світового обсягу і був меншим у 400 разів порівняно із США, у 60 разів – із Німеччиною, у 50 разів – із Францією” [214 с. 413].

Останні роки спостерігається тенденція щодо зменшення кількості страхових компаній: на початок 2018 року їх кількість склала 294, з них 33 займаються страхуванням життя (СК „Life”) та 261 ризиковими видами страхування (СК „non-Life”) [218].

Коефіцієнт концентрації страхового ринку (CR-3) по СК „Life” сягає 54,3%, а по ризиковому страхуванню – 21,3%. У Франції цей коефіцієнт по „non-life” страхуванню становить 43,37%, по страхуванню життя – 38,54%; у Великобританії – 29,83% та 18,24%; у Нідерландах – 47,36% та 48,23% відповідно [217 с. 78]. Така висока концентрація страхового ринку України вказує на те, що вітчизняна економіка переобтяжена великою кількістю страхових компаній, частка з яких навіть не здатна надавати якісні страхові послуги, розраховуватися за власними зобов’язаннями та взагалі конкурувати за хоча б невеликий сегмент ринку [210 с. 5]. Для розвитку нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки страховий ринок варто очистити від недобросовісних страховиків та запровадити жорсткіші вимоги до показників їх ліквідності, платоспроможності, розміру мінімального капіталу, що сприятиме виконанню зобов’язань у періоди кризових деформацій.

Індекс Герфіндаля-Гіршмана (ННІ) характеризує рівень конкуренції на ринку через призму його концентрації і показує розподіл „ринкової влади” між суб’єктами ринку [209 с. 302]. Для оцінки ринкової концентрації використовуються наступні діапазони даного показника: $\text{ННІ} < 1000$ – ринок оцінюється як неконцентрований; $1000 < \text{ННІ} < 1800$ – ринок оцінюється як помірно концентрований; $\text{ННІ} > 1800$ – ринок оцінюється як висококонцентрований [213 с. 83-84]. В Україні по Life-страхуванню у 2017 році цей індекс склав 1417,52 (у 2016 р. – 1079,59), а по non-Life-страхуванню, відповідно – 305,27 та 280,74. Загалом по страховому ринку індекс Герфіндаля-Гіршмана у 2017 р. становив 272,07, а у 2016 р. – 245,09.

Іншим ключовим показником вважається індекс щільності страхування. Страховий захист в країні вважається належним, якщо цей показник перебільшує 140 дол. США. Акцентовано, що „для України характерним є низький рівень поширеності страхових послуг, адже витрати однієї особи на страхування в середньому становлять 65,4 дол. США, в той час, як в Польщі показник щільності страхування має значення 140 дол. США, в Німеччині – 1482 дол. США, в Японії – 5-6 тис. дол. США” [225].

За таких умов, подією, що сприятиме зростанню кіберстрахування вважаємо набуття чинності регламентного документа Європейського Союзу щодо захисту даних (General Data Protection Regulation, GDPR) внаслідок підвищення обізнаності компаній про ризики, викликаних порушеннями конфіденційності при обробці даних. Регламентні нововведення надають економічним суб’єктам ЄС більше прав на свою онлайн-інформацію і передбачають штрафи обсягом до 4% річного доходу підприємств при

виявленні грубих порушень. За ствердженням страхових аналітиків, цей регламент, а також широго відомі наслідки кібератак WannaCry і NotPetya сприятимуть попиту на послуги кібер-страхування. Так, кількість синдикатів Lloyd's, що пропонують кібер-страхування за 2016 рік зросла на 20%. За переконанням виконавчого директора Lloyd Інги Біль, щорічні прирости бруто-премії європейського кіберстрахування до 2024 року можуть скласти понад \$ 2 млрд, що сумарно становитиме близько \$ 9 млрд. Аналітики зазначають, що великі підприємства при ухваленні рішень щодо співробітництва, вимагають наявності поліса кібер-страхування у своїх контрагентів, оскільки інформаційні ресурси дорожчають, диджиталізація набирає оберти, відповідно і ймовірність фінансових і репутаційних втрат стрімко підвищується. Перспективність розвитку кібер-страхування, підтверджується і тим, що світові потужні страхові компанії вже пропонують його продукти.

Задля зростання привабливості кібер-страхування, страхові компанії розширюють страхове покриття та надають додакові послуги:

- відшкодування витрат на розслідування кібер-злочинів;
- антикризовий піар з метою відновлення репутації;
- витрати на захист у суді і відновлення роботи ІТ-системи.

Тобто використання нових інструментів та методів страхування для управління ризиками в реаліях цифрових трансформацій є вигідним при великомасштабному інциденті збою чи компрометації ІКТ-системи, та сприяє телекомунікаційним підприємствам підтримувати економічну стабільність і мінімізувати втрати.

В. Братюк акцентує, що страхування кібер-ризиків спрямоване на подолання наслідків втручання кібер-злочинців (відновлення функцій, інформації, комунікацій) та пов'язане з покриттям всіх необхідних для цього витрат, а також на відшкодування збитків, які є результатом простою комп'ютерних систем [211].

Н. Приказок вважає, що розвитку кібер-страхування заважає: невизначеність регулювання відносин у кіберстрахуванні; нестача інформації для проведення актуарних розрахунків; концентрація ризиків у разі настання страхового випадку [220]. Окрім того, відсутня необхідна статистика, нормативна база, судова практика, недостатньо і кваліфікованих фахівців, що мають уявлення про даний вид ризику та його структуру [215].

Проведені дослідження дозволяють стверджувати, що в Україні розвиток кібер-страхування гальмується:

- відсутністю фінансово потужно страхових компаній здатних прийняти кібер-ризик;
- браком належної нормативної підтримки;
- відсутність адекватних методик щодо ідентифікації, оцінки та систематизації кібер-ризиків;

браком достатньої статистичної та інформаційної бази для проведення актуарних розрахунків, що унеможливає встановлення тарифів на продукти кібер-страхування;

відсутність платоспроможних страхувальників, які мають можливість придбати продукти кібер-страхування;

нормативна невизначенність статусу цифрових активів.

Нині, вітчизняні страхові компанії оцінюють кібер-ризик економічних суб'єктів за допомогою непрямих ознак, показників і характеристик, серед них: наявність ризик-менеджменту, наявність служб економічної та інформаційної безпеки, способи і технології зберігання конфіденційних даних, частота проведення тестування та аудиту безпеки інформаційних потоків та комунікаційних ланцюгів, кількість IT-спеціалістів тощо.

Водночас, у цій площині, як позитив, слід відмітити диджиталізацію страхових компаній, що дозволяє їм надавати персоналізовані послуги через зручні канали для страхувальників та ширше використання програм лояльності.

За даними Gartner „Hype cycle for property & casualty (P&C) insurance” хмарні обчислення (cloud computing) входять до п'ятірки найбільш пріоритетних IT-рішень серед страхових компаній. А, за даними Gartner, 41% страхових компаній вже використовують хмарні обчислення в своїй діяльності, ще 41% впроваджує чи планує впровадити хмарні технології в наступні 6-12 місяців. За прогнозами Gartner хмарні технології будуть широко використовуватися в страховій галузі в наступні 5-10 років [225 с.7].

25% страхувальників бажає купити страхове покриття онлайн. Нині, характерна пряма залежність між рівнем розвитку страхового ринку та часткою каналу онлайн-продажів страхових послуг серед інших каналів збуту. На розвинутих ринках частка агентського каналу складає 50-60%, на середньорозвинутих – 60-70%, на нерозвинутих – 80-90% [218].

Варто виділити наступні ключові тенденції щодо розширення каналів продажу страхових продуктів: зростання ролі Інтернет-мережі; широке використання різних соціальних мереж, як альтернативних каналів дистрибуції; використання хмарних технологій, SaaS рішень тощо; автоматизація бізнес-процесів (андерайтинг, врегулювання збитків тощо) та збільшення частки прямих продажів.

Серед ключових чинників, що сприяють нарощенню частки онлайн страхування є: можливість обрання персоналізованих страхових продуктів; низька вартість страхового продукту з високою якістю; можливість порівняння страхових продуктів страхувальниками; зручність для споживачів.

У Великобританії понад 20% акумульованих страхових премій приходить на онлайн-канал [216]. Водночас, слід зауважити, що вітчизняним страховим компаніям варто переймати світовий досвід для розробки пропозицій із кібер-страхування. Так, цікавим у цій площині є поліс CyberEdge від American International Group (AIG), який нині вважається вершиною розвитку кібер-страхування. Визиває інтерес, те що за даними TechCrunch, компанії Apple і Cisco уклали угоду про партнерство із страховою компанією Allianz. І тепер економічні суб'єкти, які використовують технології Apple і Cisco, мають можливість укласти більш вигідні договори з кібер-страхування з Allianz.

І сьогодні, завдяки діджиталізації страхового сегменту економічного простору генерується якісно нова сфера – InsurTech, як синтез сучасних цифрових технологій і традиційного страхування. InsurTech – це технології, які зосереджені на розробці страхових IT- рішень. До них відносять сервіси для споживачів та нові інструменти для роботи страховиків.

За інформацією IBM – 81% потужних успішних страхових компаній вже співпрацюють з InsurTech-проектами, і 45% інших страховиків. Це підтверджує тезу, що для розвитку і успішного функціонування, страховим компаніям необхідні сучасні цифрові технології.

За ствердженням McKinsey, найбільш популярними технологічними рішеннями в InsurTech-проектах є: мікрострахування (3%), блокчейн (4%), P2P (4%), робо-едвайзер (10%), гейміфікація (10%), страхування для IoT-сфери (12%), страхування на основі використання (13%), великі дані і машинне навчання (20%).

У звіті 2018 року, Edelman Trust Barometer експерти 2017 рік означають роком кризи довіри, а 2018 рік – роком битви за правду. Вірогідно, InsurTech – допоможе у цій битві.

Штучний інтелект, машинне навчання та аналіз великих даних – мають великий потенціал щодо поліпшення страхового захисту економічних суб'єктів. Big Data допоможе страховикам краще ідентифікувати й оцінити ризики. Робо-едвайзер на основі AI і machine learning допоможуть з рутинними завданнями: консультування, підбір пропозицій і рішень, оформлення необхідних документів. Нині, об'єктом страхування стає не лише майно, а й інформація. Саме це є прикметною ознакою трансформації страхового сегменту. За дослідженнями PwC, від кіберзлочинів світова економіка втрачає 400 млрд дол на рік, і цей показник буде зростати. Для порівняння (за інформацією Time з посиланням на SpaceX): запуск ракети Falcon 9 коштує 62 млн дол, а Falcon Heavy – 90 млн дол. Вочевидь, що захищати свої бізнесові та приватні інтереси телекомунікаційні підприємства без нових інструментів та методів страхування для управління ризиками в реаліях цифрових трансформацій та без InsurTech-рішень не зможуть.

Адаптація страхового ринку до змін, пов'язаних із діджиталізацією підприємств, зміною дизайну страхових інструментів, впровадженням цифрових технологій в організацію страхової індустрії і кібер-страхування, сприятиме підвищенню якості страхового захисту й стабільному прибутковому функціонуванню телекомунікаційних підприємств, стимулюванню впровадження нових інструментів, методів, технологій і InsurTech-рішень, урізноманітненню спектру страхових продуктів, удосконаленню форм і методів страхового нагляду тощо.

Надані пропозиції дозволять сформувати передумови для активізації та розширення обсягів використання нових інструментів та методів страхування для управління ризиками в реаліях цифрових трансформацій, що сприятиме підвищенню якості страхового захисту й конкурентоспроможності та нарощенню конкурентних переваг на вітчизняних та світових ринках усіх телекомунікаційних підприємств.

3.4. Стратегічні орієнтири розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації

З початку війни українські телекомунікаційні підприємства щодня стикаються з новими викликами та загрозами. Ризики руйнування телекомунікаційної інфраструктури, відновлювальні роботи, розмінування, міграція персоналу, зниження платоспроможності населення, інвестиційні ризики тощо – все це потребує адекватного реагування задля збереження позицій або мінімізації руйнації. Водночас, нині, як підтверджують спеціальні обстеження та наявні публікації, у більшості телекомунікаційних підприємств не сформовано стратегічних орієнтирів розвитку управління ризиками та відсутні регламенти реагування на загрози й ризикові процеси. Водночас, як свідчать результати експертного опитування керівників та спеціалістів 17 телекомунікаційних підприємств, переважно, керівництво та топ-менеджери телекомунікаційних підприємств добре усвідомлюють необхідність і важливість формування стратегічних орієнтирів розвитку управління ризиками. Більше того, під час поглибленого обговорення означених питань, встановлено, що деякі керівники і спеціалісти продемонстрували обізнаність із специфікою та ключовими стратегіями розвитку управління ризиками в телекомунікаційних підприємствах. Водночас, не зважаючи на це, реальних заходів щодо системного формування і впровадження стратегічних орієнтирів розвитку управління ризиками в практичну діяльність телекомунікаційних підприємств на підґрунті обґрунтованих теоретико-методичних засад сучасної ризикології не спостерігається.

Вагомими науковими розробками щодо осмислення стратегічних аспектів й орієнтирів розвитку управління ризиками в телекомунікаційних підприємствах є праці таких видатних науковців як: Виноградова О., Головач Т., Гранатуров В., Гудзь О., Гусева О., Євтушенко Н., Лазоренко, Лук'янова В., Л., Князева О., Попович А., Приймак І., Старинець О., Сазонова С. та інших. Високо оцінюючи їх науковий внесок у розробку означеної тематики, відмітимо, що залишаються дискусійними проблеми щодо з'ясування важливості, окреслення особливостей та етапів формування стратегічних орієнтирів управління ризиками в телекомунікаційних підприємствах, також потребує уточнення регламентація реагування на загрози й ризикові процеси, що сприятиме ухваленню більш ефективних управлінських рішень за кризових умов невизначеності, деформацій та загроз.

Вагомою причиною, яка стримує процес практичного формування і впровадження стратегічних орієнтирів управління ризиками на багатьох телекомунікаційних підприємствах, за нашими спостереженнями, вважаємо складність їх розробки та аналізу згенерованих ефектів, оскільки кількісний та якісний вимір результативності, переважно, можливий у випадку, реалізації ризикової події, а не її превенції, тому часто й нівелюються зусилля керівників й спеціалістів. Означене у сукупності обґрунтовує доцільність представленого наукового дослідження. Сучасна ризикологія, окреслює ризик як вірогідне явище, наслідком якого можуть бути позитивні, нейтральні або негативні ефекти.

Формування стратегічних орієнтирів вважаємо мистецтвом управління ризиками в телекомунікаційних підприємствах за умов економічних деформацій й невизначеності бізнес-процесів, що ґрунтується на прогнозуванні загроз і ризиків і використанні методів їх нівелювання чи зниження. Такі стратегічні орієнтири включають в себе регламенти, правила, стандарти, що виступають базисом для ухвалення відповідних управлінських рішень і заходів.

Метою формування стратегічних орієнтирів управління ризиками в телекомунікаційних підприємствах є підвищення конкурентоспроможності і примноження конкурентних переваг за допомогою надійного захисту від реалізації загроз та ризикових подій.

Фактично, правилами формування стратегічних орієнтирів управління ризиками в телекомунікаційних підприємствах слід вважати:

- оптимальність поєднання прибутку і величини ризику;

- максимум позитивних ефектів;

- оптимальна волатильність позитивного результату;

- оптимальна ймовірність позитивного результату.

Успіх формування стратегічних орієнтирів управління ризиками в телекомунікаційних підприємствах, здебільшого, залежить від наступних чинників:

- всебічна підтримка керівниками і спеціалістами;

- оптимальний розподіл відповідальності і повноважень;

- усвідомленість вагомості стратегічних проблем управління ризиками серед усього персоналу.

Різні управлінські ієрархічні рівні в телекомунікаційних підприємствах вимагають і різної інформаційної деталізації щодо загроз і ризиків. Так, для керівників і топ-менеджерів і головних спеціалістів ключовими завданнями мають бути:

- ідентифікація та формування реєстрів ключових ризиків підприємства;

- розробка ієрархічної мультимодульної карти ризиків;

- розробка ризик-профіля й конкретних результативних програм в нових реаліях сьогодення;

- контроль за виконанням заходів програми управління ризиками;

- модернізація механізму розвитку управління ризиками;

- формування гнучких організаційних структур та інформаційно-комунікаційних ланцюгів підприємства;

- розробку стратегічного портфеля, корпоративної політики щодо управління ризиками;

- розробку корпоративної ризик-культури персоналу;

- затвердження положень, посадових інструкцій, регламентів, стандартів, форм звітності щодо управління ризиками.

Для структурних підрозділів телекомунікаційних підприємств (їх керівників і спеціалістів середньої ланки) ключовими завданнями мають бути:

- ідентифікація та формування реєстрів ключових ризиків підприємства у діяльності свого структурного підрозділу;

здійснювати постійний моніторинг ефективності за виконанням заходів програми управління ризиками;
систематично надавати звіти керівництву щодо виконання заходів програми управління ризиками;
стежити за дотриманням процедур корпоративної ризик-культури персоналу.

Для кожного працівника телекомунікаційного підприємства ключовими завданнями мають бути:

у межах своїх компетенцій надавати пропозиції щодо заходів програми управління ризиками;

дотримуватись процедур корпоративної ризик-культури персоналу;

усвідомлювати важливість системи управління ризиками;

своєчасно доповідати про зміни чи відхилення щодо ідентифікації ключових ризиків підприємства.

Формування стратегічних орієнтирів управління ризиками в телекомунікаційних підприємствах слід здійснювати за наступними етапами:

виявлення та ідентифікація ризику і діагностика ймовірності його настання та прогноз масштабу наслідків за песимістичним, оптимістичним та реалістичним сценаріями;

фільтрація та відбір методів, інструментів, технологій управління ризиками;

формування стратегічних орієнтирів, стратегічного набору та розробка відповідних ризик-стратегій задля мінімізації можливих негативних ефектів;

впровадження ризик-стратегії;

оцінка досягнутих ефектів та коригування стратегічних орієнтирів.

Ми підтримуємо наукові позиції дослідників [7], які до ключових ризик-стратегій відносять: „запобігання (уникнення), відхилення, зниження, збереження (прийняття), передача, поділ відповідальності, використання, ігнорування” [152].

Ризик-стратегії щодо уникнення ризиків здебільшого [36, 37, 48, 89, 130] передбачають:

відмову від ненадійних постачальників, партнерів, клієнтів, тобто прагнення вести бізнес лише з надійними, перевіреними постачальниками, партнерами, клієнтами;

відмову від участі у бізнесових проектах що пов'язані із розширенням кола постачальників, партнерів, клієнтів;

відмова від інвестиційних чи інноваційних бізнес проектів ефективність яких викликає сумнів;

швидке звільнення некомпетентних спеціалістів і працівників.

Ризик-стратегії щодо збереження / прийняття ризику здебільшого [36, 37, 48, 89, 130] передбачають:

чітке систематичне стратегічне планування бізнес діяльності, що дає змогу передбачити вузькі місця, заздалегідь ідентифікувати чинники і джерела ризиків, передбачити компенсуючі заходи чи резерви;

систематична розробка різних (песимістичного, оптимістичного та реалістичного) сценаріїв стратегічного розвитку і діагностика майбутніх викликів та запитів зовнішнього середовища;

прогнозування поведінки постачальників, партнерів, клієнтів і дій конкурентів;

моніторинг макроекономічного середовища;

формування системи резервів і запасів підприємства;

створення структурних підрозділів для імплементації ризикованих бізнес-проектів;

систематичне навчання і підвищення кваліфікації спеціалістів і працівників, розробка спеціальних інструкцій на випадок настання ризикових подій.

Ризик-стратегії щодо зниження ризику здебільшого [36, 37, 48, 89, 130] передбачають:

зниження ймовірності настання ризикових чи несприятливих подій;

зниження обсягів можливого збитку та недоотримання бажаних обсягів прибутків,

профілактика ризиків;

диверсифікація діяльності та інвестицій;

лімітування усіх проектів та бізнес-процесів;

стратегування та хеджування ризиків;

формування матеріальних та фінансових резервів і запасів.

Ризик-стратегії щодо перерозподілу чи передачі ризику здебільшого [36, 37, 48, 89, 130] передбачають:

пошук та залучення гарантів;

укладання договорів щодо спільної реалізації ризикованих бізнес-проектів;

розподіл відповідальності між усіма учасниками бізнес-проекту;

розподіл ризику в часі (за етапами впровадження бізнес-проекту);

використання технологій аутсорсингу;

страхування ризиків.

Проте тільки зформулювати стратегічні орієнтири управління ризиками в телекомунікаційних підприємствах недостатньо, доцільно модернізувати механізм їх впровадження, що має передбачити:

„створення ефективної системи оцінки і контролю прийнятих рішень;

виділення у структурі підприємства спеціального підрозділу (працівника), якому буде доручена організація управління ризиками;

виділення коштів і формування спеціальних резервів для реалізації механізмів управління ризиками, покриття збитків і втрат” [18, 49].

Розглянувши різноманітні підходи до формування стратегічних орієнтирів управління ризиками в телекомунікаційних підприємствах, доцільно дотримуватись наступних положень:

„не варто ризикувати більше, ніж може дозволити власний капітал; варто прогнозувати наслідки ризику;

не слід ризикувати багато чим заради малого;

позитивне рішення щодо обраної стратегії управління ризиками приймається лише у разі відсутності сумнівів;

у разі наявності сумнівів краще прийняти негативне рішення;

не слід вважати, що завжди існує тільки одне рішення, варто завжди порівнювати альтернативи” [42].

Цікаво, що у наукових публікаціях та світовій практиці зустрічається декілька підходів до побудови формування стратегічних орієнтирів управління ризиками в телекомунікаційних підприємствах:

„для розвинутих країн світу характерний профілактичний підхід до стратегічних завдань управління ризиками – робота з ризиками, які ще не перетворились у проблеми;

у вітчизняних підприємствах переважно практикується реагуючий підхід – робота з ризиками, які вже стали проблемами” [139].

Як переконують матеріали нашого дослідження, для вітчизняних телекомунікаційних підприємств притаманна орієнтація на реагуючу композицію управління ризиками, водночас, потужні європейські та американські ІТ-компанії більше орієнтуються на превентивну композицію управління ризиками, тобто на новий рівень осмислення цих процесів [89, 90, 185].

Зарубіжні ІТ-компанії здійснюють безперервне формування стратегічних орієнтирів управління ризиками, а вітчизняні телекомунікаційні підприємства характеризуються епізодичним ризик-менеджментом, тобто використовують його лише за безпосередньою вказівкою керівництва. В зарубіжних ІТ-компаніях стратегії ризик-менеджменту координуються і коригуються керівництвом, але кожен працівник компанії розглядає стратегічні орієнтири управління ризиками як частину своїх функціональних обов’язків.

На противагу цьому, кожен структурний підрозділ українських телекомунікаційних підприємств, переважно вибірково, на розсуд керівників середньої ланки намагаються управляти ризиками.

В зарубіжних ІТ-компаніях уважно аналізують увесь спектр ризиків та прогнозують можливість їх реалізації, керівники вітчизняних телекомунікаційних підприємств, переважно аналізують лише ризикові події, що підлягають страхуванню чи фінансуванню.

Формуючі сучасні пули стратегічних орієнтирів розвитку управління ризиками доцільно використовувати різноманітні їх ансамблі, що підвищують ризикозахищеність телекомунікаційних підприємств.

Так, ансамбль, який містить M стратегічних орієнтирів:

$S_1(t), S_2(t), \dots, S_M(t)$.

Відповідно до певного часового інтервалу T та ризикостійкості конкретного підприємства доцільно використовувати наступні характеристики, при відборі стратегічних орієнтирів:

Асортимент ризиків і їх інтенсивність:

$$E_i = \int_0^T S_i^2(t) dt. \quad (3.16)$$

Взаємну потужність впливу ризиків $S_i(t)$ та $S_j(t)$:

$$E_{ij} = \int_0^T S_i(t) S_j(t) dt. \quad (3.17)$$

Ефективність методів управління за різницею зниження впливу ризиків $S_i(t)$ та $S_j(t)$:

$$E_{i-j} = \int_0^T [S_i(t) - S_j(t)]^2 dt = E_i + E_j - 2E_{ij}, \quad (3.18)$$

Коефіцієнт взаємної кореляції:

$$\rho_{ij} = \frac{E_{ij}}{\sqrt{E_i E_j}}. \quad (3.19)$$

Формуючи пул стратегічних орієнтирів розвитку управління ризиками, варто враховувати й ймовірність похибки P_0 яку можна розрахувати для очікуваних ризиків та амплітуд їх впливу. При цьому алгоритм формування набуде вигляд:

$$\int_0^T [X(t) - S_i(t)]^2 dt \langle \int_0^T [X(t) - S_j(t)]^2 dt, i, j = 1, \dots, M; i \neq j.$$

При виконанні такої нерівності доцільно ухвалити рішення щодо прийняття стратегічних орієнтирів що спрямовані на передачу ризиків $S_i(t)$. Пул має містити M стратегічних орієнтирів, в кожному визначається ефективність його реалізації $\|X - S_i\|^2 = \int_0^T [X - S_i(t)]^2 dt, i = 1, \dots, M$, та витрати на його впровадження. Для стратегічних орієнтирів з однаковою ефективністю алгоритм можна окреслити:

$$\int X(t) S_i(t) dt \langle \int_0^T X(t) S_j(t) dt. \quad (3.20)$$

У загальному окресленні алгоритм набуває наступного вигляду:

$$Y_i \rangle Y_j, i = 1, \dots, M, j = 1, \dots, M; i \neq j. \quad (3.21)$$

Наведені Y_i, Y_j – це результати витрат та вигод використання стратегічних орієнтирів. Рішення щодо включення в пул стратегічних орієнтирів ухвалюється за напрямом, в якому Y має максимальну величину.

Якщо декілька таких стратегічних орієнтирів S_i , то ймовірністю правильного ухвалення рішень вважається ймовірність виконання $M-1$ одночасно, або:

$$P_{\text{пр}}(S_i) = P\{Y_i \rangle Y_1, \dots, Y_i \rangle Y_{i-1}, Y_i \rangle Y_{i+1}, \dots, Y_i \rangle Y_M\}$$

Ймовірність похибки ухвалення рішення щодо стратегічного орієнтиру S_i :
 $P_0(S_i) = 1 - P_{\text{пр}}(S_i). \quad (3.22)$

При великому інформаційному шумі щодо загроз та ризиків розрахунок ймовірності похибки в багатопозиційній управлінській системі варто оцінити сумарною ймовірністю: $P_0(S_i) = \sum_{\substack{j=1 \\ j \neq i}}^N P_{0ij}$.

$$(3.23)$$

При $M > 8$, P_0 розраховуємо:

$$P_0 = \frac{1}{2M} \sum_{i=1}^N \sum_{j=1}^N \left[1 - \Phi\left(a_{ij} \sqrt{\frac{2E_{\bar{\sigma}}}{N_0}}\right) \right]. \quad (3.24)$$

Зауважимо, що різні ансамблі стратегічних орієнтирів сформують різну ризикостійкість. При великій кількості стратегічних орієнтирів у пулі M ймовірність похибки залежить від потужності впливу ризиків d та їх дотичності. Тому порівняння ансамблів стратегічних орієнтирів доцільно здійснювати за коефіцієнтом ризикостійкості.

$$a = \frac{d}{2\sqrt{E_{\bar{\sigma}}}}. \quad (3.25)$$

Тоді потужність впливу ризиків d вимірюється водночас із затратами та вигодами від реалізації стратегічного орієнтиру:

$$E_{\bar{\sigma}} = \frac{E_c}{\log_2 M}. \quad (3.26)$$

При мінімальній потужності взаємовпливу між ризиками d та рівноймовірності їх настання середня ефективність стратегічного орієнтиру

$$\text{буде: } E_c = \frac{d}{2M} \sum_{i=1}^N (2i-1)^2, \text{ де } M - \text{парне.} \quad (3.27)$$

За таких умов індекс ризикостійкості дорівнює:

$$a_c = \frac{d}{2\sqrt{E_{\bar{\sigma}c}}} = \frac{\sqrt{M \log_2 M}}{\sqrt{2 \sum_{i=1}^{N/2} (2i-1)^2}}. \quad (3.28)$$

Максимальна ефективність стратегічного орієнтиру визначається:

$$E_M = \frac{[(M-1)d]^2}{4}. \quad (3.29)$$

Тоді індекс ризикостійкості за максимальної ефективності дорівнює:

$$a_M = \frac{d}{2\sqrt{E_{\bar{\sigma} \max}}} = \frac{\sqrt{\log_2 M}}{\sqrt{(M-1)^2}}. \quad (3.30)$$

Криві ймовірності похибки при оптимальному формуванні пула стратегічних орієнтирів розвитку управління ризиками на прикладі досліджуваних телекомунікаційних підприємств наведено на рисунку 3.6.

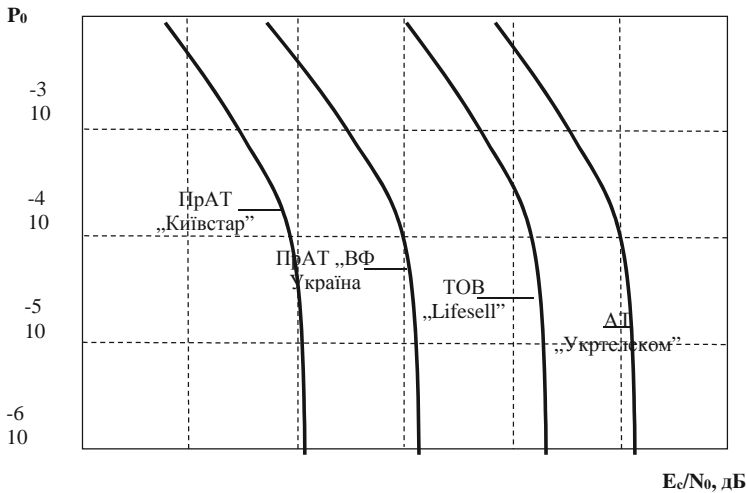


Рис. 3.6. Криві ймовірності похибки при оптимальному формуванні пула стратегічних орієнтирів розвитку управління ризиками в досліджуваних телекомунікаційних підприємствах в реаліях цифрової трансформації

Прогнозовані індекси ризикостійкості за різними ансамблями стратегічних орієнтирів для досліджуваних телекомунікаційних підприємств наведено на рисунку 3.7.

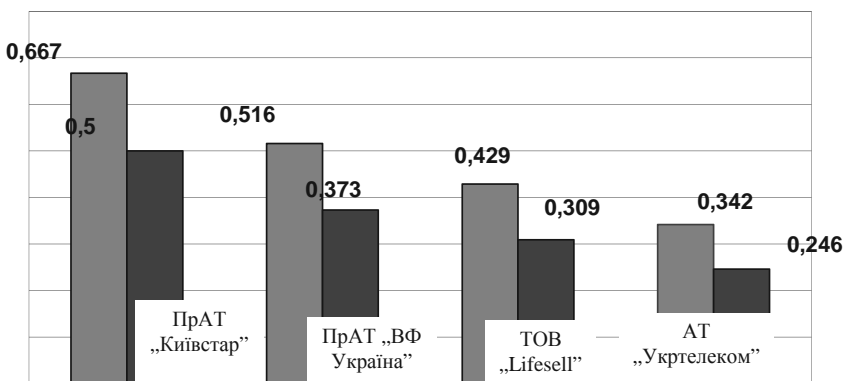


Рис. 3.7. Прогнозовані індекси ризикостійкості за різними ансамблями стратегічних орієнтирів для досліджуваних телекомунікаційних підприємств

Опираючись на основні постулати теорії стратегічного управління [36, 37, 48, 89, 130] та результати наших наукових розвідок, стратегічними орієнтирами розвитку управління ризиками в телекомунікаційних підприємствах слід вважати наступні:

- побудова ефективної системи стратегічного ризик-менеджменту на основі системного, комплексного та ситуаційного підходів;

- розробка ризик-стратегій (песимістична, оптимістична та реалістична) має спиратися на науково обґрунтоване прогнозування можливих наслідків і виявлення потенційно найбільш небезпечних чинників та джерел ризиків;

 - розробка стратегічних та операційних планів, бюджетування;

- стратегія і тактика ризик-менеджменту має затверджуватись керівництвом телекомунікаційного підприємства відповідно до мети його діяльності та його унікальних особливостей;

- управління ризиками має бути неперервним комплексним процесом, координованим вищим керівництвом та впроваджуватись спільними зусиллями всього персоналу;

 - діагностика ринкових тенденцій і запитів потенційних клієнтів;

- комплексний розгляд усього спектру ризиків з урахуванням усіх взаємозв'язків і можливих ефектів;

- підвищення рівня клієнтоорієнтованості, управління взаємодій з постачальниками і партнерами;

 - розробка заходів програми управління ризиками;

- трансформація організації бізнес-процесів, пов'язаних з технологіями та управлінням;

 - удосконалення організаційної структури підприємства;

 - покращення процедур ухвалення управлінських рішень;

 - забезпечення інформаційної безпеки;

 - підвищення кваліфікації спеціалістів та працівників;

 - формування корпоративної культури управління ризиками.

- Регламентація реагування на загрози й ризикові процеси, відповідно до сформованих стратегічних орієнтирів в телекомунікаційних підприємствах має передбачати:

 - ідентифікацію та формування реєстрів ключових ризиків підприємства;

 - розробку ієрархічної мультимодульної карти ризиків;

- модернізацію механізму розвитку управління ризиками в телекомунікаційних підприємствах;

- формування гнучких організаційних структур та інформаційно-комунікаційних ланцюгів;

- затвердження положень, посадових інструкцій, регламентів, стандартів, форм звітності щодо управління ризиками;

- розробку ризик-профіля й конкретних результативних програм в нових реаліях сьогодення;

- розробку стратегічного портфеля, корпоративної політики щодо управління ризиками;

 - розробку корпоративної ризик-культури персоналу.

Формування гнучких організаційних структур та інформаційно-комунікаційних ланцюгів має передбачати надання підрозділам та посадовим особам додаткових функцій, відповідальності й повноважень щодо управління ризиками з обов'язковим передбаченням організаційної горизонтальної (між структурними підрозділами) та вертикальної (керівник – топ-менеджери – начальники підрозділів і відділів – функціональні менеджери) взаємодії щодо управління ризиками в телекомунікаційних підприємствах та має забезпечувати збір, обробку, збереження та аналіз інформаційних потоків щодо превенції, реагування й прогнозування на загрози й ризикові процеси, підтримку ухвалення управлінських рішень, дієвість системи диспетчерського, тактичного, оперативного управління, стабільність функціонування комунікаційних ланцюгів та відповідного обладнання, систем управління активами ЕАМ та RCM-системи тощо.

Важливим вважаємо, відповідно до сформованих стратегічних орієнтирів в телекомунікаційних підприємствах розробку конкретних результативних програм щодо управління ризиками, модернізацію механізмів забезпечення цього процесу, впровадження постійного моніторингу й контролю за загрозами, ризиками та їх чинниками, розробку стратегічного портфеля, корпоративної політики щодо управління ризиками та корпоративної ризик-культури персоналу, формування й аналіз відповідних інформаційних баз даних тощо. Систематизація основних проблем діяльності телекомунікаційних підприємств України, викликані війною і перспективні напрями їхнього вирішення за стратегічними орієнтирами розвитку управління ризиками представлено на рисунку 3.8.

Доцільним вважаємо й визначення ефектів від сформованих стратегічних орієнтирів в телекомунікаційних підприємствах, так економічний ефект буде свідчити про підвищення прибутків, зниження собівартості продукції та послуг, організаційний ефект відобразатиме якість організації процесів і процедур управління ризиками в телекомунікаційних підприємствах розширення клієнтської бази, соціальний ефект – зростання продуктивності праці, примноження компетентностей, зниження непродуктивних втрат, конфліктів, порушень трудової дисципліни, плинність кадрів тощо. Тобто використання запропонованих сформованих стратегічних орієнтирів в телекомунікаційних підприємствах сприятиме ухваленню більш ефективних управлінських рішень за кризових умов невизначеності, деформації та загроз, а наявність різноманітних ефектів підтверджуватиме доцільність її практичного впровадження.

У той же час інтеграційні процеси приєднання до телекомунікаційного середовища ЄС передбачають врахування необхідності адаптації до умов конкурентного зовнішнього середовища, що зумовлює потребу врахування макро- і мезо ризиків телекомунікаційних підприємств, в основі яких має лежати розв'язання проблем довгострокового їхнього розвитку: трансформація корпоративних і конкурентних стратегій, створення цінності для всіх зацікавлених сторін, формування стратегічної поведінки, максимально відповідної умовам глобалізації та тенденціям змін цифрового світу.

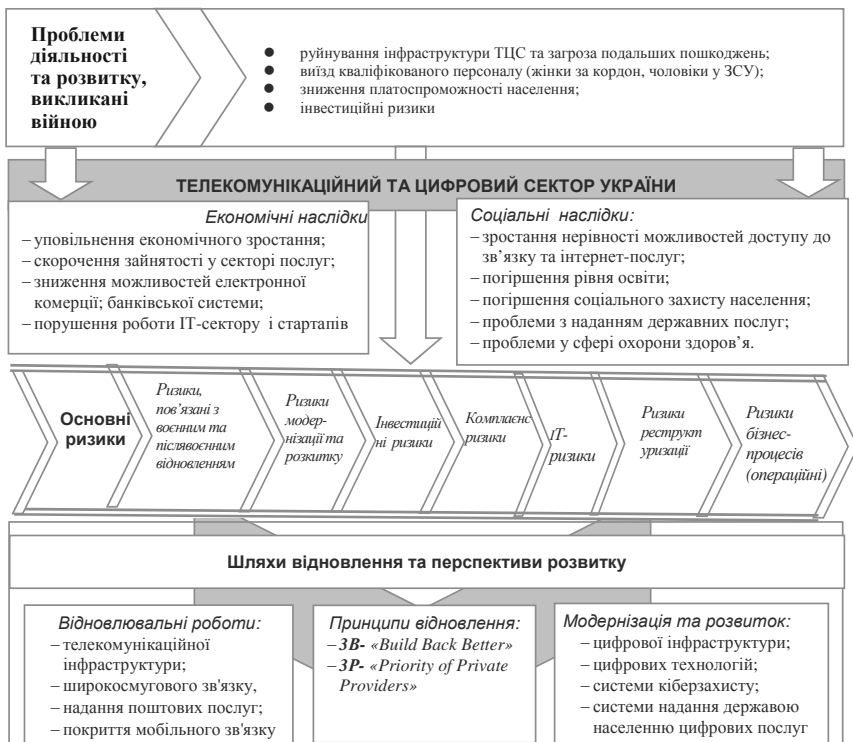


Рис. 3.8. Основні проблеми діяльності телекомунікаційних підприємств України, викликані війною і перспективні напрями їхнього вирішення за стратегічними орієнтирами розвитку управління ризиками
Примітка: побудовано за [14, 57, 86, 151].

Виходячи з проведеного дослідження тенденцій розвитку сфери телекомунікацій в Україні і на глобальному рівні сучасного становлення соціально-економічних відносин були виявлені і сформовані основні проблеми та перспективні напрями діяльності підприємств у майбутньому. Ефективність діяльності телекомунікаційних підприємств в сучасних кризових умовах повинна будуватись на основі модернізованого механізму розвитку управління ризиками. Особливо актуальне урахування ризиків і управління ними стало при необхідності переформатування всієї системи економічних відносин і життєдіяльності суспільства в наслідок пандемії COVID-19 і воєнно-політичних конфліктів. Ці зовнішні фактори внесли додаткові умови та індикативні вектори у всі бізнес-процеси і систему управління ризиками на телекомунікаційних підприємствах. Проведені вище дослідження і пропозиції

полягли в основу розробленої кватровекторної моделі розвитку управління макро- і мезо ризиками (рис. 3.9).

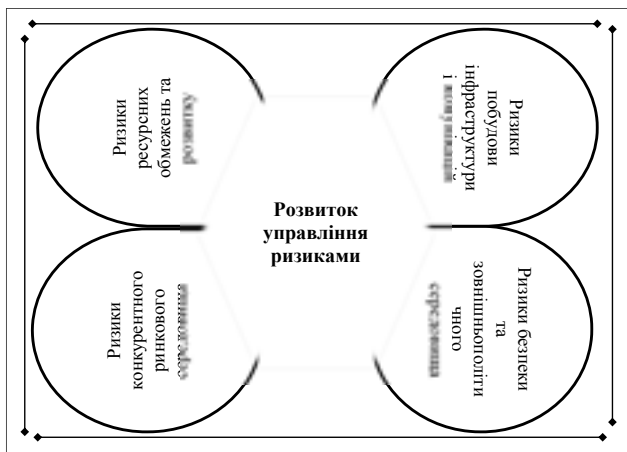


Рис. 3.9. Кватровекторна модель розвитку управління макро- і мезо ризиків на телекомунікаційних підприємствах

Примітка: сформовано з використанням [56, 124, 125, 170].

Кватровекторна модель розвитку управління ризиками на телекомунікаційних підприємствах базується на чотирьох основних векторах – управління ризиками пов’язаними з ресурсними обмеженнями для забезпечення сталого розвитку; управління ризиками конкурентного ринкового середовища; управління ризиками побудови інфраструктури та комунікацій; управління ризиками з забезпечення безпеки та зовнішньополітичного оточення.

При цьому, стратегія має бути основним документом щодо розвитку управління ризиками в телекомунікаційних підприємствах, з метою виявлення нових можливостей для отримання прибутку, забезпечення стабільного та прогнозованого перебігу подій, а значить окреслення засобів для подолання ризиків, які можуть призвести до отримання непередбачуваних збитків, або негативно вплинути на його діяльність та здатність виконувати свої зобов’язання.

Стратегія розвитку управління ризиками в телекомунікаційних підприємствах мають бути спрямованими на виявлення, визначення, оцінку та врегулювання ризиків, де оцінкою ризику є визначення його кількісних характеристик, які ґрунтуються на показниках ймовірності настання та розміру можливого збитку, а також контроль за дотриманням допустимих меж ризиків. При розробці стратегії розвитку управління ризиками, ризики в телекомунікаційних підприємствах варто розділити на три групи: як імовірність зазнання збитків і втрати від обраного рішення та стратегії

діяльності; як імовірність відхилення від поставлених цілей; як виникнення небажаної події. Стратегія розвитку управління ризиками є поглядом у майбутнє, плануванням, прогнозуванням і прийняттям рішень з певних дій у майбутньому. Також слід зауважити, що навіть ретельно розроблений стратегічний план матиме силу доти, поки припущення, що лежать у його основі, мають місце [170]. Д. Кент зважав на необхідність стратегічного управління ризиками та виділив стадії даного процесу [180], а А. Сливоцький виокремив сім типів стратегічних ризиків [194]. У момент формування місії та стратегічних намірів розвитку управління ризиками в телекомунікаційних підприємствах мають бути окреслені ризики, що мають часові межі. Модель взаємозв'язку „стратегічні наміри-ризики”, що у [170] демонструє, що прийняття рішень у площині стратегічних намірів призводить до виникнення ризиків і, навпаки, управління ризиками впливає на процес досягнення стратегічних намірів. Нами цю модель було розвинено з уточненням особливостей розвитку управління ризиками телекомунікаційних підприємств на даний момент, а саме: ризики, пов'язані з воєнним та післявоєнним відновленням, ризики реструктуризації, модернізації та розвитку, інвестиційні ризики, комплаєнс ризики, ІТ – ризики (рис. 3.10).

Розвиток управління ризиками є складовою не лише процесу формування стратегічних намірів, а й подолання негативних наслідків від будь-яких змін. Також слід зауважити, що у ході досягнення стратегічних планів відбуваються зворотний зв'язок і постійне вдосконалення сформованих стратегічних наборів. Тобто, основою для вдосконалення процесу формування стратегічних планів, на нашу думку, повинен бути розвиток управління ризиками, адже він має забезпечити передбачення несподіваних подій, формування та досягнення цілей і реалізацію стратегій у реальних умовах сьогодення, мотивування персоналу за допомогою впевненості в майбутньому телекомунікаційних підприємств, а також підвищення рівня ризикозахисності підприємства загалом.

Аналіз виникнення можливих стратегічних ризиків в телекомунікаційних підприємствах передбачає дослідження таких основних чинників:

- динаміки основних техніко-економічних показників поступу телекомунікаційних підприємств, а також підприємств суміжних галузей;
- рівня конкуренції телекомунікаційних підприємств;
- специфічних чинників, що характеризують функціонування та розвиток телекомунікаційних підприємств;
- ринку телекомунікаційної продукції та перспектив його розвитку;
- сформованої системи державного регулювання економіки та наявності державних замовлень;
- показників стійкості телекомунікаційних підприємств порівняно з підприємствами суміжних галузей;
- показників науково-технічного прогресу.

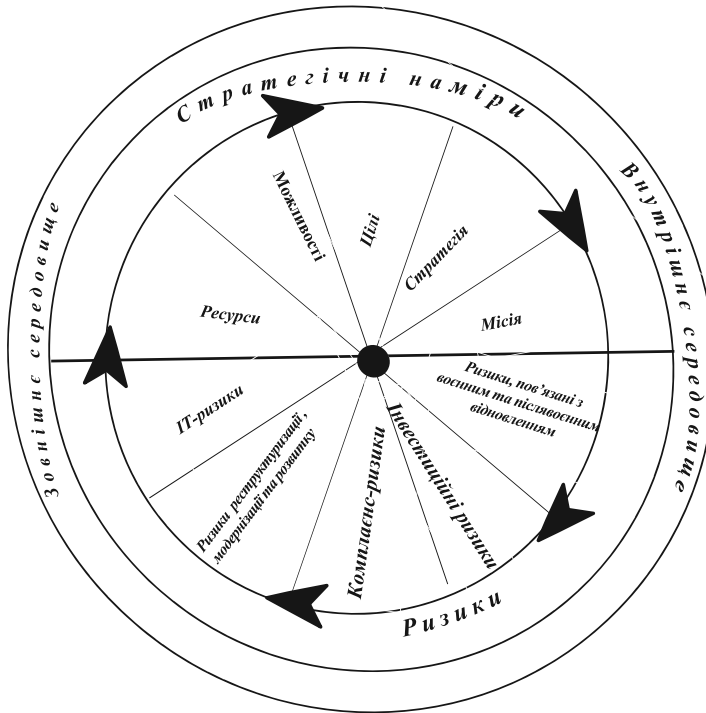


Рис. 3.10 Модель взаємозв'язку „стратегічні наміри-ризики” з уточненням ризиків стратегічного розвитку телекомунікаційних підприємств
Примітка: побудовано за [170, 173, 178].

За результатами проведених досліджень, виокремлено блок із трьох груп завдань, вирішення яких необхідне в процесі аналізу ризиків у ході формування стратегічних планів розвитку управління ризиками телекомунікаційних підприємств:

1) група аналітико-управлінських завдань (ідентифікація та класифікація ризиків, виявлення джерел ризиків, дослідження динаміки їх взаємозв'язків і змін, визначення методів аналізу та оцінювання ризиків);

2) група виконавчих завдань (балансування послідовності дій усіх учасників процесу розробки та реалізації стратегічних намірів, контролінг дій щодо досягнення мінімального рівня ризиків сформованих стратегічних намірів, прогнозування непередбачуваних подій);

3) група координаційних завдань (застосування термінових заходів щодо коригування прийнятих стратегічних наборів і попередження наслідків наявних ризиків та виявлення методів управління ними).

Акцентуємо, що, специфікою аналізу ризиків стратегічних намірів є той факт, що за час їх розробки та реалізації можуть з'явитися нові види ризиків і змінюватися ступінь впливу вже ідентифікованих ризиків. Отже, діагностика ризиків стратегічних планів передбачає дослідження процесу розробки та реалізації цілей і стратегій спільно з аналізом усіх факторів, що визначають і впливають на запланований результат. Тому стратегічний аналіз не є дискретною дією, а розглядається як безперервний процес, що дозволяє оптимізувати ступінь впливу ризиків. З урахуванням процесу реалізації визначеної стратегії телекомунікаційного підприємства доцільно проводити оцінювання рівня ризиків, які відповідають п'яти силам конкуренції за М. Портером. Так, у процесі стратегічного аналізу ризиків потрібно досліджувати учасників розробки й реалізації стратегії та ступінь їх впливу на хід реалізації плану; фактори, що впливають на процес реалізації плану, та безліч даних, що характеризують об'єкт [192 с. 218-221]. Розв'язання проблеми вимірювання ризиків підприємства вимагає формування відповідної інформаційної бази для діагностики можливих ризиків, яка містить передусім інформацію про динаміку показників, що характеризують результати, прогнозовані в рамках стратегічних намірів, і ступінь їх чутливості до ідентифікованих ризиків. Інформація, що характеризує фактори ризику, може бути умовно розділена на такі групи: статистична інформація; облікові дані; нормативні дані; інтуїтивна інформація, заснована на досвіді та знаннях фахівців; предметний опис [192]. Проведені дослідження дають змогу стверджувати, що для оцінювання рівня ризику можна використовувати теорію вимірювань, яка включає системний аналіз, побудову спеціальної моделі, вибір шкали вимірювання ризику і методу встановлення значень показника ризику.

Отже, концепція стратегічних орієнтирів розвитку управління ризиками сприяє результативному поступу телекомунікаційних підприємств, їх зростанню та лідерству з-поміж конкурентів у довгостроковій перспективі. Формування стратегічних орієнтирів розвитку управління ризиками зумовлює низку переваг для телекомунікаційного підприємства, а саме: можливість поглибленого ціле встановлення для досягнення кінцевої мети існування підприємства, розроблення найменш ризикованого стратегічного набору та дієвої системи показників результативності його діяльності, підвищення ефективності управління ризиками, адаптацію до змін зовнішнього та внутрішнього середовища, підвищення гнучкості бізнес-моделі, ідентифікацію кожним працівником своєї ролі в досягненні стратегічної мети. Виділено відповідні ризики й перспективні напрями їхнього вирішення за означеними стратегічними орієнтирами на принципах відновлення: ЗВ „Build Back Better” і ЗР „Priority of Private Providers”. Розвинено існуючу модель взаємозв'язку „стратегічні наміри-ризики” з уточненням стратегічних та поточних ризиків телекомунікаційних підприємств, а саме: ризики, пов'язані з воєнним та післявоєнним відновленням, ризики реструктуризації, модернізації та розвитку, інвестиційні ризики, комплаєнс-ризики, ІТ-ризики. Прикладне значення дослідження полягає у можливості його використання при формуванні стратегії розвитку управління ризиками у практичній діяльності

телекомунікаційного підприємства, що дасть змогу чітко будувати управлінський процес на довгострокову перспективу та забезпечити бажаний рівень ризикозахищеності телекомунікаційного підприємства.

Таким чином, удосконалений науково-організаційний підхід до формування пулу стратегічних орієнтирів управління ризиками в телекомунікаційних підприємствах базисом якого є: гармонізація поєднання прибутку і величини ризику; максимум позитивних ефектів; оптимальна волатильність та ймовірність позитивного результату, що дозволило розробити кватровекторну модель розвитку управління ризиками на телекомунікаційних підприємствах та модель взаємозв'язку „стратегічні наміри-ризики” на принципах відновлення: ЗВ „Build Back Better” і ЗР „Priority of Private Providers”, з уточненням особливостей розвитку управління ризиками телекомунікаційних підприємств на даний момент, а саме: ризики, пов'язані з воєнним та післявоєнним відновленням, ризики реструктуризації, модернізації та розвитку, інвестиційні ризики, комплаєнс-ризики, ІТ – ризики, сприяють результативному поступу телекомунікаційних підприємств, їх зростанню та лідерству з-поміж конкурентів у довгостроковій перспективі, що зумовлює низку переваг, а саме: можливість поглибленого ціле встановлення для досягнення кінцевої мети існування підприємства, розроблення найменш ризикованого стратегічного набору та дієвої системи показників результативності його діяльності, підвищення ефективності управління ризиками, адаптацію до змін зовнішнього та внутрішнього середовища, підвищення гнучкості бізнес-моделі, ідентифікацію кожним працівником своєї ролі в досягненні стратегічної мети.

ПІСЛЯМОВА

У монографії поглиблено теоретико-методологічні засади та обґрунтовано науково-організаційні рекомендації щодо розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрової трансформації, що сприятиме підвищенню їх ризикозахищеності та конкурентоспроможності у стратегічному горизонті. Результати проведеного монографічного дослідження дозволяють сформулювати висновки концептуального, теоретичного, методологічного та прикладного характеру.

1. З'ясовано, що традиційні класичні наукові постулати щодо сутнісних аспектів категорії „ризик” стали перепорою і вказують на глибокі протиріччя між існуючими науковими теоріями та практикою, що пояснює необхідність впровадження управління ризиками телекомунікаційних підприємств та його розвиток. Запропоновані наукові положення до формування унікальної траєкторії розвитку управління ризиками для кожного телекомунікаційного підприємства сприятимуть пошуку стратегічних альтернатив та імплементації превентивних управлінських рішень щодо мінімізації чи уникнення ризиків та дозволять точніше обрати специфічний методичний інструментарій управління ризиками для кожного телекомунікаційного підприємства.

2. Доведено, що механізм розвитку управління ризиками необхідно розуміти як динамічну сукупність взаємопов'язаних субсистем, інструментів, методів та важелів. Змістове наповнення і структура кожної із субсистем механізму розвитком управління ризиками залежить від типу телекомунікаційного підприємства, сфери, масштабів і результатів його діяльності, ступеня впливу чинників зовнішнього і внутрішнього середовища. Умотивовано, що для визначення конкретних методів управління ризиком, слід зважати на: складність алгоритмів операційних бізнес-процесів; адаптивність організаційного дизайну; обсяг інформаційних потоків; технологічні вимоги та компоненти й рівень діджиталізації; кількість мереж, вузлів, партнерів і клієнтів; ефективність комунікаційних ланцюгів взаємодії; обмеження й виклики та пріоритети й можливості; хиткість і гнучкість зовнішнього середовища; рівень компетенцій кадрів; параметри часових, ресурсних та організаційних контурів. Обґрунтовано, що реалізація розвинутого концепту побудови механізму розвитку управління ризиками в телекомунікаційних підприємствах, вагомо впливатиме на ефективність функціонування телекомунікаційного підприємства відповідно до його мети та обраної стратегії поступу, що зорієнтує менеджерів та працівників на активну й цілеспрямовану діяльність щодо підвищення конкурентних можливостей, зростання прибутків у довгостроковій перспективі, сприятиме ухваленню необхідних рішень.

3. З'ясовано, що для превентивного гальмування розгортання ризикових процесів та явищ в телекомунікаційних підприємствах необхідно виявляти, ідентифікувати та оцінювати ризики за допомогою здійснення діагностики та побудови сигнальної ієрархічної мультимодульної карти ризиків. Розроблено організаційний контур й доведено релевантність

здійснення діагностики з використанням ключових макро-, мезо- і мікро чинників, що дає змогу своєчасно передбачити ризикові явища та обирати оптимальні механізми і методи їх нейтралізації чи мінімізації. Аргументовано, що побудова й конкретизація сигнальної ієрархічної мультимодульної карти ризиків дозволить мати своєчасну об'єктивну ідентифікацію про стан ризикозахищеності телекомунікаційних підприємств та моделювати альтернативні траєкторії розвитку для досягнення бажаних результатів, організувати відповідну команду, генерувати стратегічні конкурентні переваги за агресивних впливів зовнішнього оточення.

4. Виявлено тенденції розвитку управління ризиками телекомунікаційних підприємств в реаліях цифрових трансформацій та окреслено особливості, основні проблеми й загрози їх діяльності, викликані війною. Так, у 2015 році рівень збитковості склав 8,2%, у 2021 році цей показник набув прибутковості і рентабельності телекомунікаційних підприємств значно зросла до 17,8%. У 2021 р. зрівняно з 2017 роком індекс автономії знизився з 0,414 до 0,263, а індекс покриття відповідно впав з 0,705 до 0,356, тобто майже вдвічі, що вказує на генерування додаткових ризиків. Використовуючи кваліджметрію ризиків досліджуваних телекомунікаційних підприємств, здійсненої на основі ієрархічної мультимодульної карти ризиків за допомогою коефіцієнту конкордації визначено, що найвпливовішими ризиками є технологічні (93%), діджиталізації (64%), виробничі (51%) та підприємницький ризик (45%). Водночас, досить гостро виникла проблема загрози кібер-ризиків (38%) та інвестиційних ризиків (25%).

5. Оцінено ключові чинники впливу на розвиток управління ризиками на прикладі: ПрАТ „Київстар”, ПрАТ „ВФ Україна”, АТ „Укртелеком”, ТОВ „Lifesel” через значення інтегрованих оцінок внутрішніх можливостей щодо підвищення розвитку управління ризиками за концептами: „фінансово-економічні чинники”, „чинники цифровізації”, „еколого-енергетичні чинники” й „чинники інтелектуалізації діяльності”. Встановлено, що нині, застосування методів управління ризиками в телекомунікаційних підприємствах зводиться до диверсифікації, страхування та формування резервів і запасів. Розрахунки засвідчили, що найвищий рівень ефективності розвитку управління ризиками і найменш „радикальний” фокус змін у стратегію ризик-менеджменту серед досліджуваних підприємств має ПрАТ „Київстар”. Вище середнього рівень розвитку управління ризиками мають ПрАТ „ВФ Україна” (2 місце) та ТОВ „Lifesel” (3 місце). Середній рівень розвитку управління ризиками демонструє АТ „Укртелеком” (4 місце). Цифровий розвиток відбувається нерівномірно, демонструє висхідні та низхідні періоди, коливання кількісних та якісних економічних характеристик, конструктивні та руйнівні тренди і має розглядатися в певному часовому відтинку. Запропонований підхід до формування можливостей ризикозахищеності телекомунікаційних підприємств в реаліях цифрових трансформацій сприятиме їх цифровому розвитку, підвищенню їх конкурентоспроможності та нарощуванню ефективності.

6. Уточнено систему принципів активізації розвитку управління ризиками з урахуванням специфіки телекомунікаційних підприємств і на цій основі побудувати трикутник напрямів активізації розвитку управління ризиками телекомунікаційних підприємств, які взаємопов'язані між собою та охоплюють стадії процесу управління ризиками, використання яких сприятиме пошуку драйверів та своєчасному коректуванню напрямів активізації розвитку управління ризиками, що буде підґрунтям для ухвалення результативних своєчасних тактичних й стратегічних інструментів і заходів для розвитку управління ризиками й дозволить мінімізувати ризики за визначеними часовими періодами на усіх ієрархічних управлінських рівнях. Розроблені наукові підходи до формування антисипаційного управління ризиками в телекомунікаційних підприємствах на практиці сприятимуть динамізму пошуку й формуванню резервів і запасів для стабільного розвитку підприємства та дозволять йому адекватно реагувати на турбулентні ризикові явища й виклики сьогодення

7. Запропоновано науковий підхід до модернізації механізму розвитку управління ризиками в телекомунікаційних підприємствах що сприятиме розробці комплексу стратегічних рішень та альтернативних сценаріїв, зорієнтованих на забезпечення спектральної гнучкості ризикозахищеності телекомунікаційних підприємств за допомогою передбачення та нівелювання різноманітних ризикових явищ та побудови надійних інформаційних й комунікаційних ланцюгів. При цьому, перевагою проактивних методів управління ризиками слід вважати, що вони враховують специфіку діяльності телекомунікаційних підприємств та передбачають градацію відповідних заходів щодо зниження ризиків за пріоритетністю, що дозволить розв'язати проблему виживання та використати потенційні можливості телекомунікаційного підприємства щодо його стабільного успішного розвитку в стратегічному горизонті.

8. Встановлено нові виклики та загрози, з якими стикаються телекомунікаційні підприємства з початку війни: ризики руйнування телекомунікаційної інфраструктури, відновлювальні роботи, розмінування, міграція персоналу, зниження платоспроможності населення, інвестиційні ризики тощо. Виявлено, що у більшості телекомунікаційних підприємств не сформовано стратегічних орієнтирів розвитку управління ризиками та відсутні регламенти реагування на загрози й ризикові процеси. Удосконалені наукові підходи до формування пулу стратегічних орієнтирів управління ризиками в телекомунікаційних підприємствах зумовлюють низку переваг, а саме: можливість поглибленого ціле встановлення для досягнення кінцевої мети існування підприємства, розроблення найменш ризикованого стратегічного набору та дієвої системи показників результативності його діяльності, підвищення ефективності управління ризиками, адаптацію до змін зовнішнього та внутрішнього середовища, підвищення гнучкості бізнес-моделі, ідентифікацію кожним працівником своєї ролі в досягненні стратегічної мети.

БІБЛОГРАФІЯ

1. Адамів М. Сутність та роль антисипативного управління на підприємствах. *Галицький економічний вісник*. 2010. №3 (28). С. 112-121.
2. *Активізація діяльності в менеджменті*. URL: https://studref.com/635476/menedzhment/aktivizatsiya_deyatelnosti_menedzhmente
3. Ансофф І. Стратегічне управління. Київ. Знання. 1989. 650 с.
4. Артишук І.В. Підходи до побудови карти ризиків на основі врахування впливу базових факторів на діяльність торговельного підприємства. *Торгівля, комерція, підприємництво: збірник наукових праць*. Львів. Видавництво Львівської комерційної академії, 2011. Вип. 13, С.101-107.
5. Афанасьєв М.В., Білоконенко Г.В. *Економічна діагностика: Навчально- методичний посібник*. Харків.: ВД „Інжек”, 2007. 296 с.
6. Афанасьєв Н. В., Рогожин В. Д., Рудика В.І. *Управління розвитком підприємства*: монографія. Харків. ВД „Інжек”, 2003. 184 с.
7. Бакуліч О. О., Кіс І. Р., Занора В. О. Тенденції управління екологічними ризиками транспортних проєктів. *Збірник наукових праць Черкаського державного технологічного університету. Серія „Економічні науки”*. 2020. Вип. 56. С. 62–69.
8. Балла М. І. Новий англо-український словник. Понад 160 000 слів та словосполучень. 4-е вид., випр. та доп. Київ. Чумацький Шлях. 2007.668 с.
9. Баранцева С. М., Хлевицька Т. Б. *Ризикологія: навчальний посібник*. Донецьк. ДОНУЕТ, 2011. 224 с.
10. Беляєв О.О. *Механізм господарювання: сутність та форми прояву*. Київ. Вища школа, 1990. 147 с.
11. Бланк І.А. *Інвестиційний менеджмент: навчальний посібник*. Київ. Ельга: Ника-Центр, 2001. 448 с.
12. Богоніколюс Н.Д. Моделі антисипативного управління у фінансовій діяльності підприємства: автореф. дис. Харків. Харк. нац. екон. ун-т. 2005. 18 с.
13. Борисова Т. Теоретичні аспекти управління ризиком на підприємстві. *Актуальні проблеми економіки*. 2005. № 7. С. 116–121.
14. Боровик М.В. *Ризик-менеджмент: конспект лекцій*. Харків: ХНУМГ ім. О.М. Бекетова, 2018. 65 с.
15. Бояринова К. О. Властивості економічної функціональності підприємства в інноваційному розвитку. *Економіка розвитку. Науковий журнал*. 2015. № 4 (76). С. 66–72.
16. Бусел В.Т. Еволюція: Великий тлумачний словник сучасної української мови Ірпінь: ВТФ Перун, 2002. 1440 с.
17. *Великий тлумачний словник сучасної української мови*. Уклад. і голов. ред. В. Т. Бусел. Ірпінь: Перун, 2007. 1736 с.
18. Вербіцька І.І. Ризик-менеджмент як сучасна система управління ризиками підприємницьких структур. *Сталий розвиток економіки*. № 5. 2013. С. 282–291.
19. Верескун М.В. Методи оцінки ефективності впровадження інформаційних систем на промислових підприємствах. *Теоретичні і практичні аспекти економіки та інтелектуальної власності*. Маріуполь, 2015. Вип. 1 (11), Т. 1. С. 21-27.
20. Виноградова О. В., Гончаренко С. В. Передумови впровадження технологій 4g і 5g як складових інноваційного розвитку телекомунікаційних підприємств України. *Економіка. Менеджмент. Бізнес*. 2016. № 4. С. 50–55.
21. Вишневська О. А. Підприємницький ризик в управлінні конкурентоспроможністю підприємств. *Економіка і суспільство*. 2016. № 7. С. 232-237.
22. Вітлінський В. В., Великоіваненко Г. І. Кількісне оцінювання ризику у фінансово-економічній сфері. *Фінанси України*. 2003. № 11. С. 16–24.
23. Вітлінський В. В., Великоіваненко Г. І. *Ризикологія в економіці та підприємстві*: монографія. Київ. КНЕУ, 2004. 480 с.
24. *Внутрішньовиробниче планування на промислових підприємствах* : навч. посіб. Свіщов М. В., Гречан А. П., Попович Л. М. та ін. Київ. Арістей, 2005. 528 с.

25. Гаркуша О.Ю. Концептуальний підхід до формування механізму управління розвитком виноробного підприємства. *Вісник Херсонського державного університету*. 2014. Вип. 6. Ч. 2. С. 128–133.
26. Гегель Г. В. Наука логіки. Київ. Наукова думка, 1997. 800 с.
27. Герасименко О.М. *Ризик-орієнтоване управління в системі економічної безпеки підприємства*: дис. ... д-ра екон. наук: 21.04.02. Київ, 2021. 667с.
28. Герасимчук Н. А., Мірзоева Т. В., Томашевська О. А. *Економічні і фінансові ризики*: навч. посібник. Київ. Компрінт, 2015. 288 с.
29. Голобородько А. Ю. Плевако Н.О. Статистичне прогнозування тенденцій розвитку телекомунікаційної сфери економіки в умовах цифровізації. *Бізнес Інформ*. 2020. №12. С. 265-270.
30. Головач Т.В., Грушевицька А.Б., Швид В.В. Ризик менеджмент: зміст і організація на підприємстві. *Вісник Хмельницького національного університету*. 2009. № 3, Т. 1. С. 157–163.
31. Горго І. О. Ризики як ключовий об'єкт управлінської діяльності сільськогосподарських підприємств. *Науковий вісник НУБіП України, Серія Економіка, аграрний менеджмент, бізнес*. 2018. № 284. С. 288-298.
32. *Господарський кодекс України*: Закон України від 16.01.2003 р. № 436-IV. Відомості Верховної Ради України. 2003. № 18–22. Ст. 144.
33. Гранатуров В. М. *Ризики підприємницької діяльності: проблеми аналізу*. Київ. Державне вид.-інф. агентство „Зв'язок”, 2000. 150 с.
34. Гранатуров В. М., Литовченко І. В., Харічков С. К. *Аналіз підприємницьких ризиків: проблеми визначення, класифікації та кількісні оцінки*: монографія. Одеса. Ін-т проблем ринку та екон.-екол. досліджень НАН України, 2003. 164 с.
35. Грещак М. Г., Гребешкова О. М., Коцюба О. С. *Внутрішній економічний механізм підприємства* : навч. посіб. Київ. КНЕУ, 2001. 228 с.
36. Гришова І.Ю., Гнатєва Т.М. Управління ризиками у контексті стратегії антикризового управління. *Український журнал прикладної економіки*. 2016. Том 1. № 3. С. 32–40.
37. Гудзь О. Є. Стратегічне управління ризикозахищеністю інноваційної діяльності підприємств. *Вісник Харківського національного аграрного університету ім. В. В. Докучаєва*. 2015. № 1. С. 3-8.
38. Гудзь О.Є. Гармонізація механізму стратегічного управління інноваційним розвитком підприємства. *Миколаївський національний університет імені В.О. Сухомлинського*. 2015. Випуск 3. С. 272-277.
39. Гудзь О.Є. Лазоренко Л.В. Ресурсне забезпечення соціально-економічного розвитку діяльності підприємств зв'язку. *Економіка. Менеджмент. Бізнес*. №1 (18), 2017. С. 5–10.
40. Гудзь О.Є. Розвиток страхування: нові інструменти та методи управління ризиками в цифровій економіці. *Економіка. Менеджмент. Бізнес*. №3 (29), 2019. С. 12–19.
41. Гудзь О.Є. Старинець О.Г. Парадигма побудови системи антикризового управління підприємством. *Економіка. Менеджмент. Бізнес*. №1 (18), 2017. С. 11–18.
42. Гудзь О.Є., Рубцов В.С. *Управління ризиками при реалізації власних бізнесових проєктів (Ризик менеджмент у малому та середньому бізнесі)*: Навч. Посібник. Київ. Планета людей, 2003. 88 с. с.5–78.
43. Гудзь О.Є., Стецюк П.А. Концептуальні засади управління ризикозахищеністю підприємства. *Економіка АПК*. 2014. № 11. с. 61–68.
44. Гусева О. Ю. *Управління стратегічними змінами: теорія і прикладні аспекти*: монографія. Донецьк. Вид-во „Ноулідж”, 2014. 395 с.
45. Данчук В. Д., Козак Л. С., Данчук М. В. *Дослідження природи підприємницьких ризиків в умовах нелінійної динаміки розвитку економіки*. *Вісник НТУ*. 2011. Вип. 24. С. 251–265.
46. Дергачова В.В., Колешня Я.О. Економічна безпека підприємства на засадах антикризового управління. *Економіка. Менеджмент. Бізнес*. №3 (25), 2018. С. 27–35.

47. Дергачова В.В., Манасенко І. М. Ризикологія: управління, проекти, тренди та перспективи. *Підприємництво та інновації*. 2020. (11-1), с. 24-31.
48. Дергачова В.В., Мельник В.О. Теоретичні основи формування конкурентних стратегій підприємства. *Актуальні проблеми економіки та управління*. К.: КПІ ім. Ігоря Сікорського, 2017. №11 С. 13– 18.
49. Дергачова В.В., Рудницька Ю.В. Управління ризиками зовнішньоекономічної діяльності в умовах пандемії COVID-19. *Економіка та держава*. №12, 2020. С. 15-21.
50. Державний класифікатор видів економічної діяльності, 2010. URL: <https://zakon.rada.gov.ua/rada/show/vb457609-10#Text>
51. Донець Л. І. *Економічні ризики та методи їх вимірювання*. Київ. Центр навч. літератури, 2006. 312 с.
52. Донець О.М., Савельєва Т.В., Урецька Ю.І. Використання міжнародних стандартів в управлінні ризиками. *Збірник наукових праць: Управління розвитком складних систем*. Київ: КНУБА, 2011. Випуск 6. С. 36-42.
53. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018 Risk Management – Principles and guidelines on implementation, IDT). URL: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v:1:en>
54. ДСТУ ISO Guide 73:2013. Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT). Вид. офіц. Київ: Мінекономрозвитку України, 2014. 17 с. URL: https://bambangkesit.files.wordpress.com/2015/12/iso-73_2009_risk-management-vocabulary.pdf
55. ДСТУ ISO/TR 31004:2013 Управління ризиками – Керівництво з впровадження ISO 31000 (Risk management – Guidance for the implementation of ISO 31000, IDT). [Чинний від 2019-01-01]. URL: <http://irpmo.com/wp-content/uploads/2018/04/ISO-31004-2013.pdf>
56. Дунда С. П. Розвиток підприємств та оцінка факторів, що на нього впливають. *Ефективна економіка* № 12, 2016.
57. Дядюк М.А. Управління ризиками: кон. лекцій. Харків: Форт, 2017. 81 с.
58. *Економіко-математичне моделювання*: навчальний посібник. За ред. О.Т. Івашука. – Тернопіль: THEU „Економічна думка”, 2008. 704 с.
59. Економічна енциклопедія: у трьох томах. Т. 1. С. В. Мочерний (відп. ред.) та ін. Київ. Видавничий центр „Академія”, 2000. 864 с.
60. Євтушенко Н.О. Механізм управління конвергентно-орієнтованим розвитком телекомунікаційних підприємств. *Економіка та суспільство*. Електронне фахове видання. Мукачєво: МДУ, 2017.-№11. С.220–228.
61. Єріна А.М. *Статистичне моделювання та прогнозування*. Київ : КНЕУ, 2001. 170 с.
62. Закон України „Про стимулювання розвитку цифрової економіки в Україні” від 15.07.2021 року URL: <https://zakon.rada.gov.ua/laws/show/1667-20#Text>
63. Захаржевська А. А. Гусєва О.Ю. Діагностика розвитку управління ризиками телекомунікаційних підприємств. *Бізнес-інформ*. № 12, 2022. С. 133-140.
64. Захаржевська А. А. Управління ризиками телекомунікаційних підприємств: сутнісні аспекти. *Економіка. Менеджмент. Бізнес*. № 1-2 (39), 2022. С. 69–74.
65. Захаржевська А. А., Зеліско І. М. Глобалізаційні імперативи діагностики розвитку управління ризиками телекомунікаційних підприємств. *Управління змінами та інновації* № (4), 2022. С.9-13.
66. Захаржевська А. А., Голобородько А. Ю. Тенденції розвитку управління ризиками телекомунікаційних підприємств. *Ефективна економіка*. № (11), 2022 р. С. 1–17.
67. Захаржевська А. А., Гудзь О.Є. Проактивні методи управління ризиками в телекомунікаційних підприємствах та їх результативність. *Підприємництво і торгівля*. №(34), 2022. С.
68. Захаржевська А. А., Хаврова К.С. Система індикаторів оцінки ключових факторів впливу на розвиток управління ризиками телекомунікаційних підприємств. *Бізнес-навігатор*. Вип.3 (70). 2022. С. 82-86.
69. Захаржевська А. А., Євтушенко Н.О. Особливості формування механізму розвитку управління ризиками в підприємствах. *Економічний простір*. № (182), 2022 С. 61–66.

70. Захаржевська А. А. Аналіз розвитку управління ризиками телекомунікаційних підприємств України за основними міжнародними індексами рівня розвитку. *The 16th International scientific and practical conference "Modern science: innovations and prospects"* (December 11-13, 2022) SSPG Publish, Stockholm, Sweden. 2022. 547 p. P. 453–458.
71. Захаржевська А. А. Напрями розвитку управління ризиками телекомунікаційних підприємств в нових економічних реаліях. *Актуальні проблеми управління та економічного розвитку в умовах інформатизації суспільства*: матер. наук.-практ. конф. (м. Київ, 20 грудня 2016 р.). Київ. ДУТ, ННІМП, 2016. 170 с. С. 22–23.
72. Захаржевська А. А. Принципи побудови механізму розвитку управління ризиками телекомунікаційних підприємств. *Телекомунікаційний простір XXI сторіччя: ринок, держава, бізнес*: матер. І міжнар. науково-практ. конф. (м. Київ, 18-19 грудня 2019 р.). Київ. ННІМП, ДУТ, 2019. 372 с. С. 288–290.
73. Захаржевська А. А., Гудзь О. Є. Завдання антисипаційного управління ризиками в телекомунікаційних підприємствах. *VI Міжнародна наукова конференція на тему «Від Балтики до Причорномор'я: формування сучасного економічного простору»*. Балтійський науково-дослідний інститут проблем трансформації економічного простору. Рига. Латвія. 9-10 грудня 2022 р.
74. Захаржевська А. А., Гудзь О. Є. Методи управління ризиками в телекомунікаційних підприємствах на проактивній основі. *Актуальні проблеми економіки, фінансів, менеджменту і права: збірник тез доповідей міжнародної науково-практичної конференції* (Житомир, 2 грудня 2022 р.): у 2 ч. Житомир: ЦФЕНД, 2022. Ч. 2. 59 с. С. 45-46.
75. Захаржевська А. А. Результативність управління ризиками телекомунікаційних підприємств. *Сучасні тенденції та перспективи розвитку системи управління в Україні та світі*: матер. міжнар. науково-практ. конф. (м. Київ, 16-17.03. 2017). Київ. ДУТ, 2017. 257 с. С. 29–30.
76. Захаржевська А. А. Сутнісні характеристики управління ризиками телекомунікаційних підприємств. *The 8th International scientific and practical conference „Modern research in world science”* (October 29-31, 2022) SPC “Sci-conf.com.ua”, Lviv, Ukraine. 2022. 1828 p. P.1300-1304.
77. Захаржевська А. А. Концепція удосконалення управління ризиками телекомунікаційних підприємств на антиципаційній основі. *Підприємництво, торгівельна, біржова діяльність: тенденції, проблеми та перспективи розвитку*. Матер. міжнар. науково-практ. конф. (м. Київ, 11.02.2020). Київ. ННІМП, ДУТ. 2020. 250 с. С. 94–97.
78. Захаржевська А. А. Управління ризиками в умовах цифрової трансформації телекомунікаційних підприємств в поствоєнний період. Міжнародна конференція для країн Європи *„Цифрова трансформація як стратегічний напрям розвитку цифрової економіки в світі та в Україні”* (м. Київ, Україна) 28 грудня 2022 р. С. 17-19.
79. *Звіт „Про роботу Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації” за 2021 рік*. URL: <https://nkrzi.gov.ua>
80. *Звіт „Швидка оцінка завданої шкоди та потреб на відновлення України”*. Серпень 2022. Світовий Банк, Уряд України, Європейська Комісія. URL: <https://www.kmu.gov.ua/news/uriad-ukrainy-ievropeiska-komisiia-ta-svitovyi-bank-prezentuvaly-zvit-shvydka-otsinka-zavdanoi-shkody-ta-potreb-na-vidnovlennia>
81. Зеліско І. М., Сосновська О. О. Аналіз впливу глобальних ризиків сучасності на функціонування вітчизняних підприємств зв'язку. *Бізнес Інформ*: науковий журнал. Харків: Інжек, 2018. № 12. С. 232–238.
82. Зінченко О. А., Зінченко Д. С. Теоретико-методичні аспекти удосконалення функціонального управління інноваційним розвитком промислових підприємств. *Підприємництво та інновації*. 2018. № 5. С. 26–33.
83. Івахненко С.В. *Інформаційні технології в організації бухгалтерського обліку та аудиту*: навч. посіб. Київ. Знання, 2006. 350 с.

84. Івченко І.Ю. *Економічні ризики*: навчальний посібник. Київ: „Центр навчальної літератури”. 2004. 304 с.
85. Камінська Б. Аналіз потенціалу розвитку промислового підприємства в антисипативному управлінні. *Економічний вісник ЗДА*. 2018. № 4(16), с. 82-87.
86. Караєва Н.В., Войтко С.В., Сорокіна Л.В. *Ризик-менеджмент сталого розвитку енергетики: інформаційна підтримка прийняття рішень*: навчальний посібник. Київ: Альфа Реклама, 2013. 308с.
87. Кіберполіція: рівень уразливості майже половини інформаційних систем приватного та державного секторів критичний. *Дебет-Кредит*. 2017. URL: <https://news.dtk.ua/state/other/44693>
88. Князева О.А., Шамін М.В. Формування кадрового резерву для забезпечення розвитку інтелектуального потенціалу персоналу підприємства. *Соціально-економічні проблеми сучасного періоду України*. Львів, 2019. № 5 (139). С. 49-55.
89. Князева О.А. Стратегічні вектори економічного розвитку країни у післявоєнний час. *Науковий вісник ОНЕУ*. № 3-4 (292-293), 2022. С. 94-100.
90. Князева О.А. Стратегія забезпечення конкурентних переваг малих та середніх телекомунікаційних підприємств. *Економіка. Менеджмент. Бізнес*. № 1(27). Київ, ДУТ. 2019. С. 4-11.
91. Ковальова Т.В., Євтушенко Н. О. *Економічний ризик: оцінка, прогнозування та шляхи мінімізації на промислових підприємствах*: монографія. Харків: ХНАДУ, 2013. 180 с.
92. *Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки*. URL: <http://zakon.rada.gov.ua/laws/show/67–2018-%D1%80> .
93. Кутєргина Г.В. Аналіз ефективності систем управління фінансовими ризиками комерційного підприємства. *Аудит і фінансовий аналіз*. 2010. № 3. С. 149-162.
94. Кутковецький В.Я. *Ймовірнісні процеси і математична статистика в автоматизованих системах*. Миколаїв: МДГУ ім. Петра Могили. 2003. 168 с.
95. Легомінова С. В. *Теоретичні та методологічні аспекти управління конкурентними перевагами телекомунікаційних підприємств*: монографія. Київ. Міленіум, 2018. 380 с.
96. Ліпич Л., Глубіцька Т. Парадигма антисипативного управління еколого-економічних систем підприємства. *Економічний часопис Східноєвропейського національного університету імені Лесі Українки*. 2015. № 4. С. 46-53.
97. Літовченко І. В. *Обґрунтування складу ризиків та їх рівня при оцінці загроз діяльності підприємства*: дис. ... канд. екон. наук: 08.01.06 – „Економіка, організація і управління підприємствами” ОНАЗ ім. О. С. Попова. Одеса, 2003. 170 с.
98. Лозовський О. М. Основні методи оцінки рівня ризиків у процесі управління підприємством. *Молодий вчений*. 2014. № 5(1). С. 138-141.
99. Лоскоріх Г.Л. Облікове відображення зниження ризику діяльності ІТ-підприємств. *Інфраструктура ринку*. 2021. № 58. С. 105-108.
100. Лук'янова В. В. *Економічний ризик*: навч. посіб. Київ. Академвидав, 2007. 262 с.
101. Лук'янова В.В. *Діагностика функціонування економічних систем з урахуванням фактору ризику*. *Вісник соціально-економічних досліджень*. 2012. № 121 (44). С. 239–245.
102. Луців О. *Стратегічний аналіз оптимальної поведінки підприємства в умовах невизначеності*. URL: <http://www.irbis-nbuv.gov.ua>
103. Ляшенко В. І. *Регулювання розвитку економічних систем: теорія, режими, інститути*: монографія. Донецьк: ДонНТУ, 2006. 668 с.
104. Мала Н. Т. Економічний розвиток підприємства: планування та моделювання. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку*. *Вісник Національного університету Львівська політехніка*. 2012. Випуск №739. С. 22–28.
105. Матвієнко-Біляєва Г. Л. Ризик-менеджмент як сучасна система ефективного управління ризиками підприємницьких структур. *Молодий вчений*. 2018. №4. URL: <http://www.donnuet.edu.ua/index.php/en/nauka/holoshennia/1413-zbirka-tez-za-robotoiu-e>

106. Мельник О. Г., Адамів М. Є. Антисипативне управління підприємствами на засадах слабких сигналів. *Актуальні проблеми економіки*. 2013. № 1. С. 32-41.
107. Месюра В. І., Ваховська Л. М., Колодний В. В. *Системи прийняття рішень з нечіткою логікою*. Частина 1. Математичні основи нечіткої логіки. Вінниця : ВНТУ, 2014. 124 с.
108. *Методи стимулювання і мотивації навчальної діяльності. Менеджмент*. URL: <https://intellect.icu/aktivizatsiya-i-stimulirovanie-6641>
109. Миколайчук І.П. Формування організаційно-економічного механізму управління ризикозахисністю підприємства. *Академічний огляд*. 2018. № 2 (49). С. 45-51.
110. Мирошниченко Г. О. Управління ризиками підприємницьких структур: аспекти ризик-менеджменту. *Економіка та суспільство*. 2022. № 44. С. 87-93.
111. Мізюк Б.М. Фінансовий механізм управління ризиками підприємств. *Фінанси України*. 2003. № 11. С. 66-67.
112. Мороз В.М. Мороз С.А. *Ризик-менеджмент*. Харків: НТУ «ХПИ», 2018. 140 с.
113. Надтока Т. Б. Соціальний розвиток промислового підприємства та механізми його управління. *Управлінські технології у рішенні сучасних проблем розвитку соціально-економічних систем*: монографія. За заг. ред. О. В. Мартякової. Донецьк: Вид-во ДонНТУ, 2011. 744 с. С. 564-569
114. Нікіфоров М.М. Особливості управління ризиками телекомунікаційних підприємств. *Держава та регіони. Серія: Економіка та підприємництво*, 2020, № 6 (117). С. 67-69. URL: http://www.econom.stateandregions.zp.ua/journal/2020/6_2020/12.pdf
115. Новак Н. Г., Гаценко С. В. Організаційно-економічний механізм розвитку виробничого підприємства у змінному середовищі. *Економіка. Менеджмент. Бізнес*. 2014. № 3. С.117–123.
116. Новосад В. П., Селіверстов Р. Г. *Методологія експертного оцінювання*: конспект лекцій. Київ. НАДУ, 2008. 48 с.
117. *Огляд цифрової трансформації економіки України в умовах війни (жовтень 2022)*. URL: <https://niss.gov.ua/news/komentari-ekspertiv/ohlyad-tsyfrovyoi-transformatsiyi-ekonomiky-ukrayiny-v-umovakh-viyny>
118. *Офіційний сайт Державної служби статистики України*. URL: www.ukrstat.gov.ua
119. Офіційна інтернет сторінка *The Committee of Sponsoring Organizations of the Treadway Commission (COSO)*. URL: <https://www.coso.org/Pages/guidance.aspx>.
120. *Офіційний сайт Міжнародної організації зі стандартизації (International Organization for Standardization, ISO)*. URL: <https://www.iso.org/committee/629121/x/catalogue/>
121. *Офіційний сайт Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації*. URL: <https://nkrzi.gov.ua>
122. *Офіційний сайт ПАТ „Укртелеком”*. URL: <http://www.ukrtelecom.ua>.
123. *Офіційний сайт ПрАТ „Київстар”*. URL: <http://www.kyivstar.ua>.
124. Підкамінний І. М. Системні фактори впливу на інноваційний розвиток підприємства. *Ефективна економіка*. 2011 рік. Випуск № 3. URL: http://nbuv.gov.ua/UJRN/efek_2011_3_4
125. Плугіна Ю. А. Інтелектуальний розвиток: сутність поняття. *Вісник економіки транспорту і промисловості*. Харків. 2011 рік. Випуск № 36. С. 193-195.
126. Побережний Р. О. Сутність стратегій розвитку підприємства: класифікаційний аспект. *Економічний вісник ЗДА*. 2016. Вип. 5(1). С. 129-135.
127. Погорелов Ю. С. *Оцінювання та моделювання розвитку підприємства*: монографія. Луганськ. Глобус, 2010. 512 с
128. Погорелов Ю. С. Категорія розвитку та її експлейнарний базис. *Теоретичні та прикладні питання економіки*. 2012. Вип. 27(1). С. 30–34.
129. Полінкевич О. М. Адаптивний механізм управління змінами у бізнес-структурах в умовах covid-19. *European scientific journal of Economic and Financial innovation*. 2020. №2(6). С. 173-182.
130. Пономаренко В. С., Тридід О. М., Кизим М. О. *Стратегія розвитку підприємства в умовах кризи*: монографія. Харків. ВД „ІНЖЕК”, 2003. 328 с.

131. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або запобігання тероризму: Закон України від 28.11.2002, № 249-IV. *Верховна Рада України: Офіційний сайт.* URL: <http://zakon4.rada.gov.ua/laws/show/249-15>.
132. Про затвердження Методики виявлення ризиків, пов'язаних з державно-приватним партнерством, їх оцінки та визначення форми управління ними: Закон України від 16.02.2011 р. №232. *Верховна Рада України: Офіційний сайт.* URL: <http://zakon3.rada.gov.ua/laws/show/232-2011-%D0%BF>
133. Про затвердження Методичних рекомендацій щодо організації проведення перевірок підприємств, які входять до складу фінансово-промислових груп, інших об'єднань та великих платників податків: Закон України від 16.07.2007р. №432. *Державна фіскальна служба України: Офіційний портал.* URL: <http://sfs.gov.ua/yuridichnim-osobam/podatkoviy-kontrol/nakazi/print-66306.html>
134. Про затвердження термінологічної бази системи внутрішнього контролю та аудиту Державного казначейства України”: Закон України від 07.10.2008 р. №417. *Законодавство України: Платформа ligazakon.* URL: http://search.ligazakon.ua/l_doc2.nsf/link1/DKU0702.html
135. Про об'єкти підвищеної небезпеки: Закон України від 18.01.2001, № 2245-III. *Верховна Рада України: Офіційний сайт.* URL: <http://zakon0.rada.gov.ua/laws/show/2245-14>
136. Проект Положення про організацію системи управління ризиками в надавачах фінансових послуг та небанківських фінансових групах. URL: https://bank.gov.ua/admin_uploads/article/proekt_Regulation_SUR_2022-06-27.pdf.
137. Прохорова В. В. Антикризисне управління підприємством як система заходів його ефективного розвитку. *Вісник Національного технічного університету «Харківський політехнічний інститут».* Збірник наукових праць. Тематичний випуск: *Технічний прогрес і ефективність виробництва.* Харків: НТУ «ХПІ». 2009. № 35. С. 12-21.
138. Раєвська О. В. *Управління розвитком підприємства: методологія, механізми, моделі* : монографія. Харків: ВД «НЖЕК», 2006. 496 с.
139. *Ризикогенність та страхування в аграрній сфері (теорія, практика):* колект. монографія/ за заг. ред. д.е.н., проф. Є. І. Ходаківського. Житомир: Полісся, 2013. 323 с.
140. Рішук Л.І. Формування програми ризик-менеджменту для нафтопереробного підприємства. *Економіка і суспільство.* 2016. № 2. С. 351 – 357.
141. Рубанов М. М. Система раннього попередження загроз за слабкими сигналами. *Вісник ХНУ. Економічні науки.* 2013. № 3(2). С. 257-261.
142. Руденський Р.А. Моделювання процесів антисипативного управління економічною безпекою: автореф. дис. на здобуття наук. ступеня канд. екон.наук: спец. 08.03.02 Економіко-математичне моделювання. Донецький нац. ун-т. Донецьк. 2002. 16 с.
143. Савченко Ю. В., Солоненко М. В. Управління ризиками на підприємствах сімейного бізнесу. *Економіка і організація управління.* 2019. № 2 (34). С. 28-36.
144. Свідерська А. В. *Управління ризиками зовнішньоекономічної діяльності підприємства:* Дис. ... канд. екон. наук: 08.00.04. Хмельницький: ХНУ, 2016. 290 с.
145. Секерін В., Мазур І. Методичні аспекти оцінки масштабів тіньової економіки. *Економіка України.* 2004. № 8. С. 36-44.
146. Семенова К., Тарасова К. *Ризики діяльності промислових підприємств: інтегральне оцінювання: монографія.* Одеса: Гуляєва В.М., 2017. 234 с.
147. *Система ризик-менеджменту в банках: теоретичні та методологічні аспекти:* монографія. За ред. В. В. Коваленко. Одеса: ОНЕУ, 2017. 304 с.
148. *Словник української мови:* в 11 т. Київ. Наукова думка. 1973. Т 4. С. 275.
149. Сосновська О. О., Деденко Л. В. Ризик-менеджмент як інструмент забезпечення стійкого функціонування підприємства в умовах невизначеності. *Європейський науковий журнал Економічних та Фінансових інновацій.* 2019. № 1(3). С. 70–79.

150. Сосновська О.О. Система економічної безпеки підприємств зв'язку: монографія. Київ. „Центр учбової літератури”, 2019. 440 с.
151. Старостіна А. О. Кравченко В. А. *Ризик-менеджмент: теорія та практика*: навчальний посібник. Київ. ІВЦ „Політехніка”, 2014. 200 с.
152. *Стратегічні напрями соціально-економічного розвитку аграрного сектору економіки України*: колективна монографія. За заг. редакцією А. В. Руснак. Херсон. ТОВ „БКФ СТАР ЛТД”, 2017. 432 с.
153. Стрельбіцька Н. Уніфікований міжнародний стандарт ризик-менеджменту як відповідь на виклики глобалізації. *Соціально-економічні проблеми і держава*. 2011. Вип. 2 (5). URL: <http://sepd.tntu.edu.ua/images/stories/pdf/2011/11snyvnh.pdf>
154. Супрун А.А. Ризики в діяльності підприємств гірничо-металургійного комплексу: види, методи, оцінки та фінансування. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління*. Том 31 (70). № 3, 2020. С. 95 – 102.
155. Тарасова Г.О. Забезпечення планування роботи з сигналами в антисипативному управлінні розвитку промислового підприємства. *Економіка та суспільство*. 2018. № 18, с. 72-77.
156. Тарашевський М. М. Стан управління ризиками на транспортних підприємствах України. *Бізнес-інформ. Економіка транспорту та зв'язку*. 2020. № 8. С. 125-133.
157. Тітова С. П. Особливості прояву ризику в діяльності сільськогосподарських підприємств. *Економіка АПК*. 2009. № 14. С. 33–36.
158. Українські компанії почали впроваджувати комплаєнс-контроль. Що це і навіщо? URL: <https://youcontrol.com.ua/articles/komplaiens-kontrol-shcho-tse-i-navishcho/>
159. *Управління підприємницьким ризиком*. За заг. ред. Д.А. Штефаніча. Тернопіль. Економічна думка, 1999. 224 с.
160. Устенко О. Л. *Підприємницькі ризики: основи теорії, методологія оцінки та управління*. Київ. Всесвіт, 1996. 146 с.
161. Устенко О. *Теорія економічного ризику*: монографія. Київ. МАУП, 1997. 164 с.
162. Фролова Л.В. *Механізми логістичного управління торговельним підприємством* : монографія. Донецьк: ДонДУЕТ ім. М. Туган-Барановського, 2005. 322.
163. Халімон Т. М. Механізм управління конкурентоспроможністю телекомунікаційних підприємств. *Інтелект XXI*. 2016. № 5. С. 127–131.
164. Цвігун Т.В. Механізм управління ризиками в системі управління підприємством. *Науковий вісник Міжнародного гуманітарного університету*. 2014. С. 9–13.
165. Чайкіна А.О., Золотар К.В. Основи формування системи ризик-менеджменту на підприємстві. *Економічний розвиток держави та її соціальна стабільність*: матеріали Міжнародної науково-практичної Інтернет- конференції, 14 червня 2021 р. Полтава : Національний університет імені Юрія Кондратюка, 2021. С. 47-48.
166. Черненко Ю. О. Вибір методів управління ризиками на промислому підприємстві. *Вісник ОНУ. Серія : Економіка*. 2014. Т. 19, Вип. 1(2). С. 36-39.
167. Чечетова Н. Ф. Ризики, їх природа, класифікація і способи виміру на ринку цінних паперів. *36. наук, праць ЧДТУ. Серія: Економічні науки*. 2018. Вип. 22. С. 123-126.
168. Шандова Н. В. Рушійні сили стійкого розвитку промислового підприємства. *Економічні інновації*. 2013 рік. Випуск №54. С. 354–362.
169. Швець Ю. О. Ризики в діяльності промислових підприємств: види, методи оцінки та заходи подолання ризику. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні ек. відносини та світове господарство*. 2018. Вип. 17(2). С. 131–135.
170. Швиданенко Г. О., Бойченко К. С. *Розвиток підприємства: стратегічні наміри, ризики та ефективність*: монографія. Київ. КНЕУ, 2015. 231 с.
171. Шегда, А.В. *Ризики в підприємстві: оцінювання та управління*: навч. посіб. Київ. Знання, 2008. 271 с.
172. Шпакова Г. В. *Детермінація системи оцінки еколого-економічних ефектів на основі індикаторів біосферосумісного виробництва*. URL: http://www.economy.nayka.com.ua/pdf/3_2020/79.pdf

173. *Що таке комплаєнс-ризик та як ними управляти.* URL: <https://bakertilly.ua/news/id44586>
174. *2021 Global ICT Development Index – ITU.* URL: <https://www.itu.int/net4/ITU-D/idi/2017/index.html>
175. *A Risk Management Standard. The Institute of Risk Management: 2002.* URL: https://www.theirm.org/media/6827/arms_2002_irm.pdf
176. Activation. *BCMPedia. A Wiki Glossary for Business Continuity Management (BCM) and Disaster Recovery (DR).* URL: <https://www.bcmpedia.org/wiki/Activation>
177. Aric Wood. *What is “Strategy Activation”?* February 23, 2022. URL: <https://xplane.com/what-is-strategy-activation/>
178. *BDO’s 2021 Telecommunications Risk Factor Survey. Risks in the new reality facing telecom companies*
179. *Brand Activation Management and your business: how to take control of your brand.* 26 May 2022. URL: <https://www.papirfly.com/blog/brand-activation-management/brand-activation-management-and-your-business-how-to-take-control-of-your-brand/>
180. Davis J. Sherman Kent’s final thoughts on analysis Bpolicymaker relations . *The Sherman Kent Center for Intelligence Analysis.* Occasional Papers, 2003. Vol. 2. No 3. Pp. 43–44.
181. Dergachova V., M. Kravchenko, O. Vynogradova, K. Kuznietsova, V. Holiuk. Determinant management of competitive devaluation: theoretical and practical aspects. *Financial and credit activities: problems of theory and practice.* No 1 (36). 2021. №1. pp. 281–292.
182. *Enterprise Risk Management – Integrating with Strategy and Performance.* URL: <https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf>
183. *Global Open Data Index.* URL: https://index.okfn.org/place/?fbclid=IwA R1jXf7Wo_XqfwW8TT6f2XT9QP5-o0umpV2HSm CsJ3nuZgeYQjkOz_a2Cbo
184. Gudz O., Prokopenko N., Korsakov D., Solovei N. Insurance And Innovative Technologies Of Risks Management Of Ukrainian Companies In The Digital Economy. *Estudios de Economia Aplicada* 2020. Vol. 38, No 3 (1). URL: <http:ojs.ual.esojsindex.php/eea>.
185. Jankelova N., Masar D., Moricova S. Risk factors in the agriculture sector. *Agric. Econ. Czech.* 2017. 63:247–258.
186. Kaplan R. S., Norton D. P. *Using the Balanced Scorecard as a Strategic Management System.* Harvard Business Review, 1996, 325 p.
187. Kathie Fuce-Hobohm. *What is Activation?* URL: <https://spaceinc.net/what-is-activation/>
188. Keynes J. M. *The General Theory of Employment, Interest and Money,* London, 1936. 139 p.
189. Kniazieva O., Obodovskyi Y. The influence of the informal component on the transformation processes of the enterprise management structures. *Tree Seas Economic Journal,* Volume 1 Number 1. Riga: Publishing House “Baltija Publishing”, 2020, P. 1–6.
190. Marshall Alfred *Principles of Economics.* Prometheus; Revised edition, 1997. 320 p.
191. Merriam-Webster’s Collegiate Dictionary. 2003. Merriam-Webster, 1664 p. URL: <http://www.merriam-webster.com/netdict/anticipation>
192. Ross S. A. *Compensation, Incentives, and the Duality of Risk Aversion and Riskiness.* Journal of Finance. Vol. 59. 2004. Pp. 207–225.
193. Shvydanenko G. Intellectualization of business planning process in the modern economic conditions. *Social processes regulation in the context of economics, law and management: Materials digest of the LIII International Research and Practice Conference and II stage of the Championship in economics, management and juridical sciences,* (London, June 06–June 11, 2013). International Academy of Science and Higher Education. London: IASHE, 2013. Pp. 69–73.
194. Slywotzky A. *Turning Strategic Risk into Growth Opportunities.* Harvard Business Review. 2008. Sep 15. Pp. 78–88.
195. *Technology and Communications Industry Report.* URL: <http://www.aon.com>.
196. *The Global Innovation Index (GII) 2020. Who Will Finance Innovation?* URL: <https://www.globalinnovationindex.org/gii-2018-report>

197. *UN E-Government Survey 2018*. URL: <https://public-administration.un.org/egovkb/en-us/Reports/UN-EGovernment-Survey-2018?fbclid=IwAR0ROie7FQWAo7F3USIMIS5ePu2YMA40NLQ2rA52uUAUX6QCZJdXtT2k8https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine>
198. Zakharchezvska A., Al-Ababneh Hassan Ali, Borisova V., Tkachenko P., Andrusiak N. Performance of Artificial Intelligence Technologies in Banking. WSEAS TRANSACTIONS on BUSINESS and ECONOMICS. Vol. 20, 2023, pp.307-317.
199. Zakharchezvska A., Vynogradova O., Drokina N. Directions of activation of risk management of telecommunications enterprises in Ukraine in martial law and post-war conditions. *Acta Scientiarum Polonorum. Oeconomia*, 28(4), 2022.
200. Zakharchezvska A., Zghurska O., Malik M., Baidala V., Somkina T., Kubiv S., Huzhavina I., Sukhostavets A., Kulik A. Modelling the influence of the environmental factor on ensuring the sustainability of Ukraine's food security. *Journal of Hygienic Engineering and Design. Vol.40, 2022, pp. 191-200*.
201. Zakharchezvska A. A. Formation of strategic guidelines for risk management in telecommunications enterprises. *Економіка. Менеджмент. Бізнес*. № 3-4 (40), 2022. С. 54–61.
202. Zakharchezvska A., Vynogradova O., Pysar N. The formation of strategic portfolio of the development of risk management in telecommunications enterprises during martial law and post-war conditions. *Technology Audit and Production Reserves, Economics of enterprises. Macroeconomics Vol.№6(4)(68),2022 P.12- 16/*
203. Zakharchezvska A.A. Key factors that influence the development of risk management of telecommunications enterprises in the conditions of digitalisation of the economy. V Міжнародна науково-практична конференція „SCIENCE and INNOVATION of MODERN WORLD” 25-27.01.2023 р. (м. Лондон, Великобританія).
204. Zakharchezvska A. A. Strategic guidelines for risk management in telecommunications enterprises. *The 2nd International scientific and practical conference “Scientific progress: innovations, achievements and prospects”* (November 6-8, 2022) MDPC Publishing, Munich, Germany. 2022. 596 p. P.478-482.
205. Гудзь О.Є., Рубцов В.С. *Управління ризиками при реалізації власних бізнесових проєктів (Ризик менеджмент у малому та середньому бізнесі)*: Навч. Посібник. Київ. Планета людей, 2003. 88 с. с.5 – 78.
206. Гудзь О.Є. Рубцов В.С. *Мистецтво бізнесу або управління бізнесовими проєктами: Навч. посібник*. Київ. Планета людей, 2006. 159 с. С.12 –159.
207. Гудзь О.Є., Глушенкова А.А. *Менеджмент ідей та управління проєктами*: навч. посібник. Київ. Планета людей, 2016. 156 с.
208. Гудзь О.Є. *Інноваційне підприємництво*. Київ. Планета людей, 2018. 187 с.
209. Абакуменко О.В. Моделювання рівня конкуренції на фінансовому ринку України. *Бізнесінформ*. 2013. № 5. С. 302–310
210. Базилевич В.Д. Новітні тенденції та протиріччя на страховому ринку України. *Вісник КНУ імені Тараса Шевченка. Економіка*. 2012. Вип. 133. С. 5- 8.
211. Братюк В.П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. *Актуальні проблеми економіки*. 2015/ № 9. С. 421-427
212. Вороненко Т. Безпечний Інтернет URL: <http://calameo.com/books/002793881c6046eb0d2fb>
213. Гаманкова О.О. Інформаційні вади дослідження ступеня монополізації ринку страхових послуг України. *Актуальні проблеми економіки*. 2009. № 10. С. 80–87.
214. Золотарьова О.В. Ключові тенденції та пріоритети розвитку ринку страхових послуг в Україні *Економіка і суспільство*. 2017. №11. С. 413-420.
215. Івашенко А.М. Світовий ринок страхування кібер-ризиків: перспективи та перешкоди. *Матеріали ІХ Міжнародної науково-практичної конференції „Національна економіка: проблеми та перспективи розвитку*. Київ КНУ, 2016. С. 196–202.

216. Кулина Г. Світовий ринок страхових послуг в умовах зміни парадигми глобального економічного розвитку. *Світ фінансів*. 2017. № 3(52). С. 48-59.
217. Малікова І.П. Оцінка концентрації страхового ринку України, її зв'язок з процесами монополізації та конкуренції. *Науковий вісник Херсонського державного університету. Серія «Економічні науки»*. 2017. Вип. 23. С. 76-79.
218. Підсумки діяльності страхових компаній за 2017 рік. URL: https://www.nfp.gov.ua/files/OgIadRinkiv/SK/2017_rik/sk_%202017.pdf
219. Пономарьова О.Б. Визначення проблем страхового ринку та їх вирішення. *Глобальні та національні проблеми економіки*. 2015. №5.
220. Приказюк Н.В. Прогресивний досвід зарубіжних країн у вирішенні проблем розвитку кіберстрахування. *Вісник ОНУ. Серія: «Економіка»*. 2016. Вип. 2. С. 164-168.
221. Allianz Risk Barometer Top Business Risks 2016. Available at: <http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf>
222. Böhme R., Schwartz G. (2010) Modeling cyber-insurance: towards a unifying framework. WEIS. Available at: <http://econinfosec.org/archive/weis2010/papers/session5/weis>.
223. Marotta A. A Survey on Cyber-Insurance. Marotta A., Martinelli F., Nanni S., Yautsiukhin A. Bologna, Italy: Unipol Gruppo Finanziario S.p.A. (in English)
224. The digital insurer. A new era in insurance: Cloud computing changes the game.
225. World insurance in 2015: steady growth amid regional disparities. Available at: http://media.swissre.com/documents/sigma_3_2016_en.pdf.
226. ANSI PMI PMBOK® Guide 3rd Edition. URL: <http://webstore.ansi.org/>.
227. Glossary of Project Management Terms. URL: <http://www.uc.edu/sashtml/orpm/chapa/index.htm>.
228. SimonBuehring. Управління невеликими проектами. URL: <http://www.pmtoday/project-management/role/managing-small-projects>
229. Батенко Л. П. Управління проектами. Київ. КНЕУ, 2005. 231 с.
230. Dennis Lock *Project management* (9e ed.) Gower Publishing, Ltd., 2007.
231. Richard E. Just, Darrell L. Hueth, Andrew Schmitz. *The Welfare Economics of Public Policy: A Practical Approach to Project And Policy Evaluation*, Edward Elgar Pub. 2004. 712 p.
232. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80>.

ДОДАТКИ

Еволюція категорії „ризик”

Період	Школа, течія економічної науки	Вклад у розвиток теорії економічного ризику
ХІІ-ХІV ст.	Теорія відсотка	Каноністи (церковне вчення): відсоток за кредит – плата за ризик.
ХVІ ст.	–	Епоха середньовіччя (сфера мореплавства та морської торгівлі): позначення проблемних питань у різних сферах суспільного життя, окреслення яких не могло бути чітко здійснене за допомогою визначень.
ХVІІ ст.	–	Російська імперія: перше тлумачення терміну „ризик” та опублікування його в тлумачному словнику (В. І. Даль та С. І. Ожегов): „ризик” – можливість небезпеки.
Початок ХVІІІ ст.	Класична економічна теорія	Фома Аквінський: ризик – це втрата позичених грошей, тобто певна негативна дія, котра може настати, якщо позикові кошти будуть втрачені. Адам Сміт: „ризик” – чинник формування частини ирибутку, як плата за управлінські здібності капіталіста.
Друга половина ХVІІІ ст.	Школа фізіократів	Жак Тюрго: прибуток – це заробітна плата за ризик. Становлення підприємця як людини, що ризикує своїм капіталом, землею та ін. для отримання підприємницького доходу.
Кінець ХVІІІ ст.	Класична теорія ризику	Ризик – збиток завданий здійсненням обраного рішення. Ризик – ймовірність отримання збитків.
Початок ХІХ ст.	Марксистська теорія	Карл Маркс: ризик – це страх втрати чи псування цінних матеріалів чи робочої сили.
Друга половина ХІХ ст.	Неокласична школа	Ральфа Джорджа Хоутрі: ризик – це певна сукупність здібностей підприємця чи торговця, при виробництві та реалізації товарів.
Середина ХІХ ст.	Кепсіанська теорія ризику	Дж. Кейнс: ризик – фактор задоволення, який полягає в очікуванні великого прибутку.
Кінець ХІХ ст.	Неолібералізм	Ризик стає вирішальним фактором формування прибутку.
Початок ХХ ст.	Інституціоналізм, інноваційна теорія	Інновація виступає як компенсація ризику.
Кінець ХХ ст.	Сучасна теорія ризику	Ризик – це небезпека потенційно можливої, ймовірної втрати ресурсів або недоотримання доходів у порівнянні з варіантом, який розрахований на раціональне використання ресурсів у конкретній бізнесовій діяльності.
Початок ХХІ ст.	Інформаційна теорія ризику	Ризик – це загрози, які можуть негативно вплинути на безпеку інформаційної системи та вивести її з ладу в цілому.

Змістове наповнення трактування різними дослідниками поняття „ризик”

Визначення	Джерело
Термін „ризик” передбачає будь-яку подію або дію, що можуть негативно позначитися па досягненні підприємством її намічених цілей і завадити йому успішно реалізувати свою стратегію.	А. Андерсен
Під ризиком розуміється можлива небезпека втрат, що витікає зі специфіки тих чи інших явищ природи та видів діяльності людського суспільства.	І. Т. Балабанов
Ризик ситуація, коли мають місце невизначеність, конфлікт, наявна багатоваріантність, і коли одночасно не всі альтернативні варіанти і є складовим елементом будь-якої управлінської діяльності.	В. В. Вітлінський, Г. Великовансько
Ризик – це можливість події, неочікуваної для активного суб’єкту, яка може виникнути в період переходу суб’єкта із даної початкової ситуації до заздалегідь визначеною цим суб’єктом кінцевої ситуації.	В. Н. Вяткін, І. Вяткін
Ризик діяльність, пов’язана з подоланням невизначеності в ситуації неминучого вибору, у процесі якого є можливість якісно і кількісно оцінити ймовірність досягнення передбаченого результату, невдачі, відхилення від мети.	Л. І. Донець
Ризик – це єдність обставин та індивідуально-групових критеріїв оцінки ситуації, на основі яких приймається оперативне рішення.	Загальнонаукове значення
Ризик – це усвідомлення можливості небезпеки виникнення непередбачених втрат очікуваного прибутку, майна, грошей у зв’язку з випадковими змінами умов економічної діяльності, несприятливими обставинами.	А. Г. Загородній, Г. Л. Вознюк
Ризик – це можливість відхилення від передбачуваної мети, заради якої здійснюється вибрана альтернатива.	І. Ю. Івченко
Ризик у загальному випадку слід розглядати як можливість або загрозу відхилення результатів конкретних рішень або дій від очікуваних.	С. М Ілляшенко
Ризик це ймовірність виникнення страт, недоотримання прибутків, небажаного розвитку середовища функціонування, відхилення від установлених цілей.	О. Є. Кузьмін, О. Мельник
Ризик – це ситуація невизначеності, неоднозначності, яка може призвести як до позитивного, так і до негативного результату того чи іншого економічного дії.	М. Г. Лапуста, Л. Шаршукова
Ризик – це об’єктивно-суб’єктивна категорія, пов’язана з подоланням невизначеності, випадковості, конфліктності в ситуації неминучого вибору, що відображає ступінь досягнення суб’єктом очікуваного результату.	В. Лук’янова, Т. Головач
Ризик – імовірність втрати підприємством частини своїх ресурсів, недоотримання доходів чи появи додаткових витрат у результаті здійснення певної виробничої і фінансової діяльності	Н. І. Машина
Ризик – це можливість виникнення неблагополучних ситуацій в ході реалізації планів і виконання бюджетів підприємства.	Л. Н. Тепман
Ризик в економічному розумінні передбачає втрати, ймовірність котрих пов’язана з наявністю невизначеності, а також зиск і прибуток, отримати які можливо завдяки діям, пов’язаним з ризиком.	А. В. Шегда, О. Голованенко

Сучасні моделі та концепції економічного розвитку [56, 124, 125, 170]

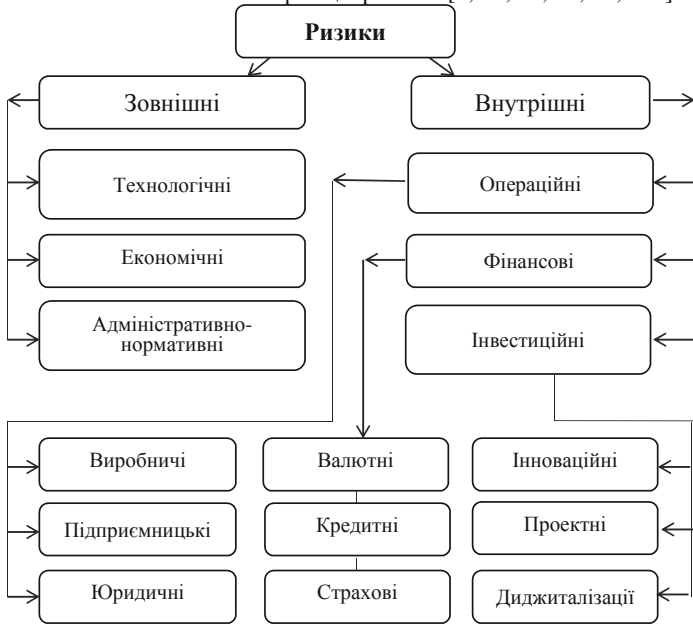
Назва моделі	Характеристика
<i>Моделі економічного розвитку</i>	
Модель лінійних стадій розвитку	будь-яка економічна система в процесі свого розвитку має пройти певні етапи, за умови включення її в світову систему взаємозв'язків.
Теорія структурних трансформацій	відображає процес переходу від аграрної до індустріальної моделі економічного розвитку
Теорія зовнішньої залежності	взаємозалежність країн світу є наслідком залежності колоній від метрополій та інших розвинутих країн. Тому між ними сформовані відносини нееквівалентного обміну у взаємній торгівлі.
Неокласична модель вільного ринку	необхідність лібералізації економіки, її зовнішньої відкритості, приватизації власності, інституційної перебудови тощо
Теорія ендогенного зростання	орієнтації на внутрішні чинники і механізми господарського розвитку.
Модель сталого розвитку	спрямована на зміну стосунків людини і природи задля розширення можливостей економічного зростання, та на створення скоординованої глобальної стратегії виживання людства, орієнтованої на збереження і відновлення природних спільнот.
Концепція життєвих циклів А.Адзіеса	в ефективній організації повинні бути представлені усі чотири управлінські функції: Р – орієнтована на результати, А - адміністративна, Е – підприємницька і І – інтеграційна. Отже, підприємство повинно оптимальним чином задовольняти споживачів, вчасно змінюватись та попереджувати потреби, що змінюються, створивши для цього структуру з взаємозамінних елементів
Концепція еволюційного розвитку підприємства Л.Грейнера	На кожній стадії діяльність підприємства фокусується на якомусь конкретному аспекті, і кожна стадія завершується кризою, що несе загрозу виживанню підприємства. Якщо підприємство справляється з кризою успішно, то воно вступає в наступну стадію

Переваги та недоліки використання наукових підходів в управлінні економічним розвитком підприємства [56, 124, 125, 170]

Назва підходу	Переваги підходу	Недоліки підходу
Системний підхід	<p>Визначення цілей та критеріїв управління та підпорядкування встановлених критеріїв загальній меті;</p> <p>Розгляд усіх елементів системи у взаємозв'язку;</p> <p>Застосування на різних рівнях — від одного підрозділу до всього підприємства. У кожному випадку об'єкт управління розглядається як цілісна система;</p> <p>Спрямування на слабо структуровані проблеми, пошук оптимального варіанта їх вирішення</p>	<p>Потребує високого професіоналізму персоналу;</p> <p>Використання дорогих технологій, автоматизованих систем управління; - Не передбачає розкладання на взаємопов'язані процедури як на «вході» з постачальниками, так і на «виході» з покупцями і замовниками</p>
Програмно-цільовий підхід	<p>Робить більш зрозумілою організаційну структуру управління організацією;</p> <p>Забезпечує цілеспрямовану мотивацію робітників;</p> <p>Допомагає опрацювати ефективні методи контролю (винагороджується результат, а не процес діяльності). Найкращим орієнтиром для контролю є комплекс чітко сформульованих цілей.</p>	<p>Керівникам іноді важко встановлювати кількісно визначені цілі діяльності для кожного підлеглого.</p> <p>Вищим керівникам не завжди вигідно доводити цілі до кожного підлеглого.</p> <p>Потребує встановлення короткострокових цілей; значної бюрократії; високої кваліфікації персоналу.</p>
Ситуаційний підхід	<p>Досягнення мети підприємства в даних умовах часу;</p> <p>Визначення умов формування концепції підприємства щодо розвитку системи управління;</p> <p>Враховання конкретного набору обставин, що впливають на підприємство у визначений проміжок часу;</p> <p>Знаходження оптимальних рішень у конкретних ситуаціях;</p> <p>Суттєва економія часу, коли потрібно оперативно прийняти рішення</p>	<p>Орієнтація виключно на стандартні завдання;</p> <p>Відсутність стратегічного планування;</p> <p>Складність формування критеріїв оцінки ефективності управління враховуючи широкий спектр ситуацій, що виникають на підприємстві, у зв'язку з чим звужується керованість управлінського процесу;</p> <p>Управління виконується на рівні ситуації, коли вона керує процесом, а не процес ситуацією.</p>

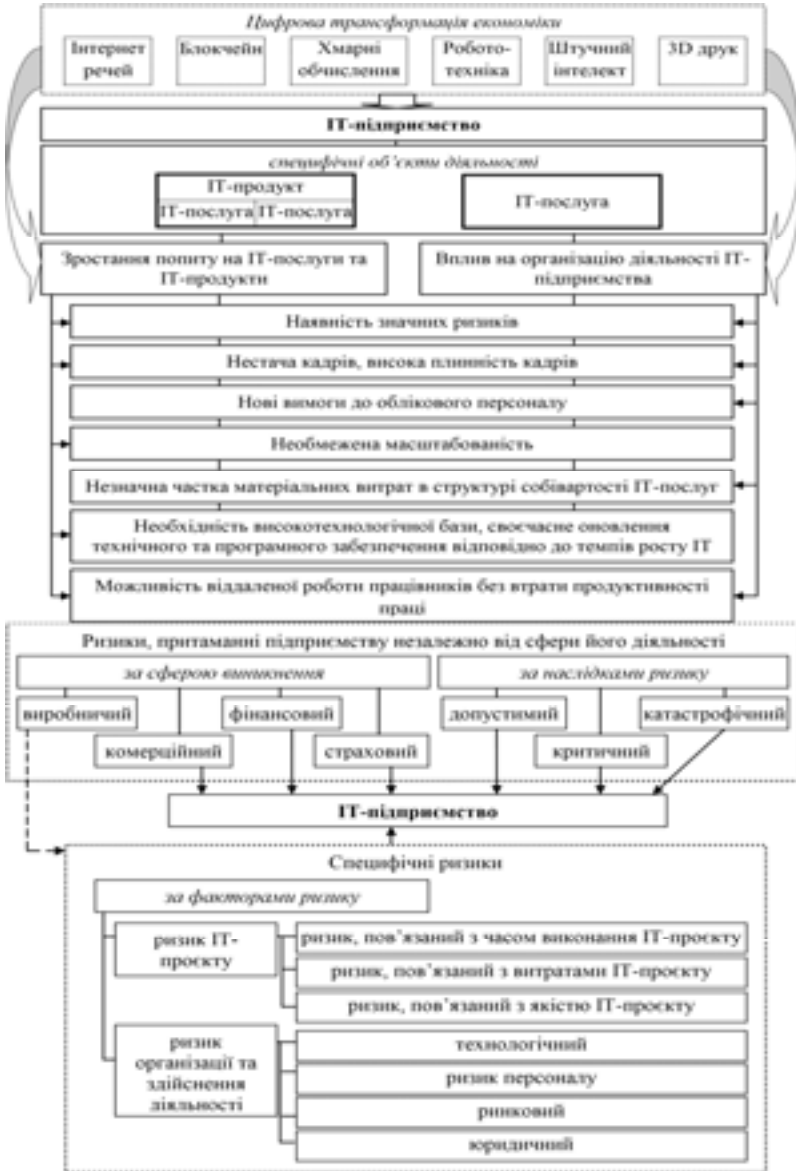
1	2	3
<p>Функціональний підхід</p>	<p>Управління здійснюється сукупністю підрозділів, що спеціалізуються на виконанні конкретного виду робіт; Високий рівень професіоналізму працівників; Отримання механізму найшвидшої реакції на зміни умов господарювання; чіткий розподіл функцій дає можливість забезпечити стійкий розвиток підприємства; Зростання якості управління основною діяльністю</p>	<p>Обмежені зони відповідальності; Надмірний рівень бюрократії (погоджень, контролю, делегування повноважень і т.д.); Працівники зосереджені на процесі виконання роботи, а не на кінцевому результаті; Велика кількість узгоджень, що збільшує термін виконання роботи до одержання кінцевого результату</p>
<p>Процесний підхід</p>	<p>Високий рівень якості управління; Мінімізація функцій, що контролюються; Оптимізація централізованого та децентралізованого підходів; Зниження ризику субоптимізації при управлінні цілісним процесом; Відхід від фрагментарної відповідальності; Управління процесами дозволяє створити кращі підстави для контролю ресурсів і часу виконання робіт; Урахування динамічного характеру розвитку організацій; Істотне скорочення витрат на управління</p>	<p>Високий рівень фінансування при переході на управління за процесним підходом; Труднощі сприйняття працівниками нового підходу до управління; Складність реалізації підходу; Недостатність відображення взаємозв'язку між елементами управління; Зниження можливості професійного зростання та звуження компетенції робітників</p>

Класифікація ризиків [9, 13, 23, 34, 37, 167]



Продовження додатку Е. Ризики проекту [98, 99 с. 723]

Специфічні об'єкти та характерні риси діяльності ІТ- підприємства, зумовлені специфікою сфери та впливом процесу цифровізації [99]



Додаток 3. Систематизація ризиків телекомунікаційних підприємств [99]

Опис специфічних ризиків для функціонування телекомунікаційних підприємств [99]

Блоки специфічних ризиків	Ризик	Систематизований опис ризику
Ризики проєктів	Ризик, пов'язаний з часом виконання проєкту	Характеризується недотриманням встановлених строків проєкту
	Ризик, пов'язаний з витратами проєкту	Проявляється при порушенні встановленого бюджету проєкту як з вини замовника, так і виконавця
	Ризик, пов'язаний з якістю проєкту	Характеризується помилками при виконанні проєкту, можливістю їх виправлення та відповідністю поставленим завданням
Ризик організації та здійснення бізнес-процесів	Технологічний	Зумовлений помилками при технічних розрахунках, збоїв в програмному забезпеченні, втратою бази даних
	Ризик персоналу	Пов'язаний з плінністю кадрів та необхідним високим рівнем їх підготовки та перепідготовки
	Ринковий	Зумовлений нестабільністю економічної кон'юнктури та швидкими змінами прогнозів розвитку
	Юридичний	Визначений частими змінами законодавства та коригуванням напрямів розвитку

Загальні принципи управління на підприємстві
(систематизовано авторами на основі [144 с.25-27])

Принцип управління	Характеристика принципу управління
Принцип наукової обгрунтованості управління	Цей принцип – основний в системі загальних принципів управління. Науковий підхід до менеджменту вимагає комплексного вивчення всієї сукупності факторів, що впливають на ефективність функціонування організації, з подальшим застосуванням отриманих знань у практиці управління
Принцип системного підходу до вирішення управлінських завдань	Системний підхід вимагає, щоб керівники розглядали організацію як сукупність взаємопов'язаних, взаємозалежних і постійно взаємодіють один з одним елементів (люди, структура; завдання і технології), орієнтованих на досягнення різних цілей
Принцип оптимальності управління	Принцип оптимальності управління встановлює вимогу досягнення цілей управління з мінімальними витратами часу і коштів
Принцип гнучкості управління	З вищезазначеним принципом нерозривно пов'язаний принцип гнучкості управління, практична реалізація якого дозволяє забезпечити своєчасну адаптацію організації до мінливих умов зовнішнього середовища або її швидку перебудову відповідно до новими цілями функціонування
Принцип демократизації управління	Із зростанням ролі соціальних факторів в менеджменті на перший план вийшов принцип демократизації управління, який містить вимогу задоволення на справедливій основі інтересів власників, керівників, трудового колективу і окремих працівників організації
Принцип регламентації управління	Відповідно до принципу регламентації всі процеси, що відбуваються в системі управління, повинні бути жорстко регламентовані, тобто в будь-якій організації повинна бути розроблена розгорнута система правил і норм, що визначають порядок функціонування як організації в цілому, так і її окремих структурних підрозділів
Принцип формалізації управління	Принцип формалізації передбачає формальне закріплення норм і правил функціонування організації у вигляді наказів, вказівок і розпоряджень керівника, а також у вигляді положень про конкретні структурні підрозділи та посадових інструкцій

Принципи управління ризиками в наукових працях
(систематизовано авторами)

Автори	Рік	Назва праці	Принципи згідно із стандартом
Карасва Н.В., Войтко С.В., Сорокіна Л.В. [86 с.60]	2013	Ризик-менеджмент сталого розвитку енергетики: інформаційна підтримка прийняття рішень	1) принцип масштабності; 2) прагнення до врахування якомога більшої кількості сфер можливого виникнення ризиків; 3) принцип мінімізації; 4) необхідність зменшення спектра проявів ризиків і ступеня їх впливу; 5) принцип адекватності реакції; 6) необхідність швидко і ефективно реагувати на зовнішні зміни в ризикованій ситуації; 7) принцип розумного прийняття; 8) прийняття ризику тільки у випадку його обґрунтованої необхідності.
Семенова К.Д., Тарасова К.І. [146 с.46-47]	2017	Ризики діяльності промислових підприємств: інтегральне оцінювання	1) принцип максимальності виграшу, який полягає в тому, що з можливих варіантів ризикових вкладень капіталу обирається той, який дає найбільшу ефективність результату при мінімальному чи прийнятному для підприємства рівні ризику; 2) принцип оптимальної ймовірності результату, який стверджує, що з усієї сукупності можливих рішень обирають те, при якому вірогідність результату є прийнятною для підприємства; 3) принцип оптимального сполучення виграшу та величини ризику, згідно якого з усіх варіантів, що забезпечують прийнятний для підприємства ризик, обирається той, у якого співвідношення прибутку до втрат (збитку) є найбільшим; 4) принцип оптимального коливання результату полягає в тому, що з можливих рішень обирається те, при якому ймовірності виграшу чи програшу для самого ризикового проекту мають найменший розрив; 5) принцип мінімізації спектру можливих ризиків і ступеня їх впливу на діяльність господарюючого суб'єкта; 6) принцип адекватності реакції, який зводиться до того, що необхідно адекватно та швидко реагувати на зміни, які можуть призвести до виникнення ризику; 7) принцип прийняття – підприємство може прийняти на себе лише обґрунтований ризик
Коваленко В.В. [147 с.17]	2017	Система ризик-менеджменту в банках: теоретичні та методологічні аспекти	1) ефективність; 2) своєчасність; 3) структурованість; 4) розподіл обов'язків (відокремлення функції контролю від здійснення операцій банку); 5) усебічність та комплексність; 6) пропорційність;

			7) незалежність; 8) конфіденційність; 9) прозорість
Боровик М.В. [14 с.27]	2018	Ризик-менеджмент	1) принцип лояльного ставлення до ризиків; 2) принцип прогнозування; 3) принцип страхування; 4) принцип резервування; 5) принцип мінімізації втрат і максимізації доходів
Мороз В.М., Мороз С.А. [112 с.63]	2018	Ризик-менеджмент	1) системність та безперервність дій щодо виявлення та оцінювання ризиків; 2) персональна відповідальність суб'єктів управління за якість ризик-менеджменту на рівні структурного підрозділу; 3) комплексне сприйняття впливу ризиків в процесі прийняття управлінських рішень; 4) аналіз рівня прояву ризиків на всіх етапах управлінської діяльності; 5) обов'язковість дотримання регламенту внутрішнього та зовнішнього контролю процедур ризик-менеджменту; 6) оцінювання ефективності ризик-менеджменту; 7) колегіальність в обговоренні та прийнятті рішень
Герасименко О.М. [27 с.166-168]	2021	Ризик-орієнтоване управління в системі економічної безпеки підприємства	1) інтегрованість; 2) структурованість та комплексність; 3) адаптованість; 4) інклюзивність; 5) динамічність; 6) надійність інформації; 7) людський та культурний фактори; 8) постійне вдосконалення.

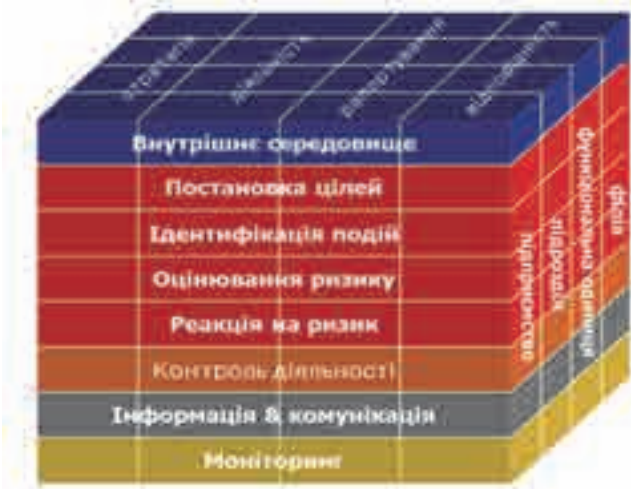
Процес управління ризиками згідно ISO 31000:2018 [53]



Порівняльна характеристика основних теоретичних концепцій управління ризиками підприємств [9, 13, 23, 34, 37, 167]

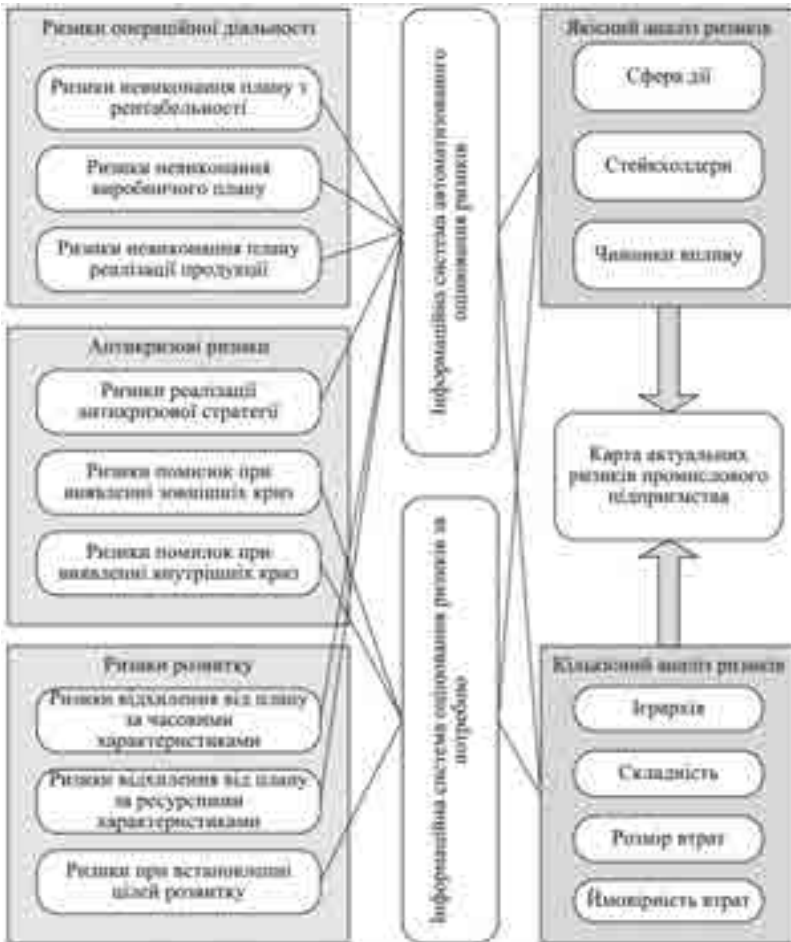
Назва концепції			
Основні характеристики	Інтуїтивна	Фрагментарна	Комплексна (ERM)
Мета управління	Уникнення ризиків	Захист від негативного впливу ризиків	Використання висхідних можливостей створюваних невизначеністю
Ризики, що підлягають розгляду	Мінімальна кількість ризиків	Обмежена кількість ризиків	Всі ризики підприємства
Підхід до управління	Хаотичний (розгляд окремих ризиків)	Дезінтегрований підхід (окремий розгляд ризиків)	Комплексний підхід (портфель ризиків)
Аспекти управління	Фінансові наслідки	Фінансові наслідки	Стратегічні можливості та наслідки, що проходять через всі функції фірми
Процес управління	Орієнтований на захист	Орієнтований на продукт	Орієнтований на процес ідентифікації характеристики ризику
Характер взаємодії	Реактивний	Реактивний	Проактивний
Результат управління	Повне або часткове уникнення ризику	Зниження волатильності прибутку, виручки, грошових потоків або вартості фірми.	Зростання вартості фірми в коротко- і довгостроковій перспективі.
Вплив на діяльність підприємства	Мінімальний вплив	Обмежений вплив на стратегії	Підтримка стратегічного і бізнес-планування
Основні методи управління	Відмова / страхування	Страхування	Використання переваг високої волатильності

Модель COSO ERM [119]



Додаток П. Фактори ризику згідно FERMA RMS [53]

Система оцінювання ризиків підприємства [5, 34, 91, 99, 101, 154, 160]





Додаток С. Комплексна оцінка ризиків підприємства та прийняття управлінських рішень на основі результатів оцінки [5, 34, 91, 98, 99, 101, 154, 160]

Обґрунтування системи показників для визначення рівня економічної стійкості підприємства з урахуванням структурованих факторів ризику
(авторська розробка)

Показник	Алгоритм розрахунку	Умовне позначення	Логіка обґрунтування цільових та граничних значень
1	2	3	4
1. Показники, що характеризують економічну стійкість підприємства з позицій фінансово-економічних факторів ризиків			
1.1. Коефіцієнт поточної ліквідності	$K_{пл} = \frac{OA}{ПЗ},$ де OA – оборотні активи $ПЗ$ – поточні зобов'язання	$K_{пл}$	Залежить від обраних політик формування та фінансування оборотних активів
1.2. Коефіцієнт швидкої ліквідності	$K_{шл} = \frac{ДЗ + ГК}{ПЗ},$ де $ДЗ$ – дебіторська заборгованість $ГК$ – грошові кошти	$K_{шл}$	Залежить від обраної політики формування оборотних активів
1.3. Коефіцієнт негайної ліквідності	$K_{нл} = \frac{ГК}{ПЗ},$	$K_{нл}$	Залежить від обраної політики формування оборотних активів
1.4. Середньозважений період обертання оборотних активів	$K_{лоа} = \frac{Ч_3 * ПО_3 + Ч_{дз} * ПО_{дз} + Ч_{зк} * ПО_{зк}}{Ч_3 * ПО_3 + Ч_{дз} * ПО_{дз} + Ч_{зк} * ПО_{зк}}$	$K_{лоа}$	Залежить від структури оборотних активів та обраної політики
1.5. Коефіцієнт автономії	$K_{фа} = \frac{ВК}{ЗК}$ де $ВК$ – власний капітал $ЗК$ – загальний обсяг задіяного капіталу	$K_{фа}$	Залежить від політики формування капіталу
1.6. Коефіцієнт маневреності капіталу	$K_{мк} = \frac{ВOK}{ВК}$ де $ВOK$ – власний оборотний капітал	$K_{мк}$	Залежить від обраної політики фінансування оборотних активів
1.7. Коефіцієнт збалансованості поточних зобов'язань	$K_{зз} = \frac{КЗ}{ДЗ}$ де $КЗ$ – кредиторська заборгованість	$K_{зз}$	Співвідношення непрострочених кредиторської і дебіторської заборгованостей має бути 1-1,5
1.8. Коефіцієнт синхронності грошових потоків	$K_{сен} = \frac{\sqrt{\sum_{t=1}^m \frac{(N_t - V_t)}{n}}}{V}$ де N_t - надходження грошових коштів за період	$K_{сен}$	Вхідні та вихідні потоки повинні бути збалансованими, тому оптимальне значення має

	V_t - витрачання грошових коштів за період n - кількість досліджуваних періодів V - загальний обсяг вихідного грошового потоку		наближуватись до 0
1.9. Коефіцієнт кратності відсотків	$K_{кв} = \frac{\Pi_{до} + B_{фин} + AM}{B_{фин}}$ де $\Pi_{до}$ - прибуток від звичайної діяльності до оподаткування $B_{фин}$ - фінансові витрати AM - амортизаційні витрати	$K_{кв}$	Максимізація даного коефіцієнту свідчить про зниження фінансових ризиків
1.10 Індекс стабільності фінансових результатів	Середньоквадратичне відхилення фінансових результатів (прибутку) протягом досліджуваного періоду / середній обсяг фінансового результату	$I_{сн}$	Мінімізація даного коефіцієнту свідчить про зниження ризиків
2. Показники, що характеризують економічну стійкість підприємства з позицій цифровізаційних факторів ризиків			
2.1. Коефіцієнт цифровізації адміністративних і повторюваних бізнес-операцій (у загальній системі бізнес-процесів підприємства)	$K_{цан} = \frac{АП_{циф}}{АП_{заг}}$ де $АП_{циф}$ - кількість адміністративних і повторюваних бізнес-операцій, у які запроваджені механізми цифровізації $АП_{заг}$ - загальна кількість адміністративних і повторюваних бізнес-операцій	$K_{цан}$	Чим вищим є значення показника тим вищим є загальний рівень цифровізації бізнес-процесів на оперативному рівні
2.2. Коефіцієнт цифрової трансформації підприємства	$K_{мр} = \frac{ЕО_{циф}}{ЕО_{заг}}$ де $ЕО_{циф}$ - кількість бізнес-процесів, які здійснюються з використанням інтегрованих цифрових технологій $ЕО_{заг}$ - загальна кількість бізнес-процесів	$K_{мр}$	Чим вищим є значення показника тим вищим є загальний рівень цифровізації бізнес-процесів на стратегічному рівні
2.3. Коефіцієнт інноваційного розвитку	$K_{інр} = \frac{Зін}{Ззаг}$ де $Зін$ - кількість інноваційних технологічних змін, впроваджених у діяльність $Ззаг$ - загальна кількість технологічних змін	$K_{інр}$	Наближення даного коефіцієнта до 1 свідчить про найбільш високий рівень інноваційної активності
2.4. Коефіцієнт прогресивності технологій надання	$K_{пт} = k_e^{отех} * \frac{Y_{во}}{Y_o} + k_e^{стех} * \frac{Y_{ос}}{Y_c}$	$K_{пт}$	Максимізація даного коефіцієнту свідчить про високий рівень

<p>телекомунікаційних послуг</p>	<p>де k_{θ}^{omex}, k_{θ}^{cmex} - коефіцієнт вагомості використання високотехнологічного обладнання в основних та супроводжуючих бізнес-процесах процесів відповідно</p> <p>$Y_{\theta o}$, $Y_{\theta c}$ - вартість високотехнологічного обладнання основних та супроводжуючих технологічних процесів відповідно</p> <p>Y_o, Y_c - загальна вартість обладнання основних та супроводжуючих технологічних процесів відповідно</p>		<p>застосування провідних технологій в процесі надання телекомунікаційних послуг підприємствами</p>
<p>2.5. Коефіцієнт модернізації технологій</p>	$K_{MT} = k_{\theta}^o * \frac{Y_{MO}}{Y_o} + k_{\theta}^c * \frac{Y_{MC}}{Y_c}$ <p>де k_{θ}^o, k_{θ}^c - коефіцієнт вагомості використання обладнання в основних та супроводжуючих технологічних процесів відповідно</p> <p>Y_{MO}, Y_{MC} - вартість модернізованого обладнання основних та супроводжуючих технологічних процесів відповідно</p> <p>Y_o, Y_c - загальна вартість обладнання основних та супроводжуючих технологічних процесів відповідно</p>	<p>K_{MT}</p>	<p>Максимізація даного коефіцієнту свідчить про достатній рівень застосування сучасних технологій у діяльності підприємства</p>
<p>3. Показники, що характеризують економічну стійкість підприємства з позицій інтелектуалізаційних факторів ризиків</p>			
<p>3.1. Коефіцієнт відповідності організаційної культури організаційній структурі підприємства</p>	$K_{BCK} = \left(\frac{K_{HCTP}}{K_{CTP}} \right) / \left(\frac{K_{HKYJL}}{K_{KYJL}} \right)$ <p>де K_{HCTP} - кількість належних жорстких (гнучких) елементів, що відповідають типології організаційної структури</p> <p>K_{CTP} - загальна кількість ключових елементів організаційної структури</p> <p>K_{HKYJL} - кількість належних жорстких (гнучких) елементів, що відповідають типології організаційної культури</p> <p>K_{KYJL} - загальна кількість ключових елементів організаційної культури</p>	<p>K_{BCK}</p>	<p>Наближення коефіцієнта до 1 свідчить про достатню відповідність структури культури.</p> <p>Якщо $K_{BCK} > 1$ - більшого удосконалення потребує культура; якщо $K_{BCK} < 1$ - реформації потребує структура</p>
<p>3.2. Рівень розвитку культури інтелекто-</p>	$K_{PK3} = \frac{Y_B + Y_K + Y_C}{Y_{zag}}$	<p>K_{PK3}</p>	<p>Наближення даного коефіцієнту до 1 свідчить про</p>

орієнтованості на підприємстві	<p>де $Ч_B$ - кількість співвласників, ініціюючих та підтримуючих інтелектуорієнтованість</p> <p>$Ч_K$ - кількість штатних працівників, що координують процес інтелектуалізації</p> <p>$Ч_C$ - кількість штатних фахівців, задіяних у інтелектуалізацію</p> <p>$Ч_{заг}$ - загальна середньооблікова кількість працівників</p>		високий рівень розвитку культури інноваційних змін на підприємстві
3.3. Рівень заохочення працівників до підвищення рівня інтелектуалізації	$K_{зпз} = \frac{УЧ_{мз} + УЧ_{кп}}{УЧ_{заг}}$ <p>де $УЧ_{мз}$ - кількість працівників-, які отримали матеріальне заохочення після підвищення професійних і цифрових компетенцій</p> <p>$УЧ_{кп}$ - кількість працівників, які отримали кар'єрне просування після підвищення професійних і цифрових компетенцій</p> <p>$УЧ_{заг}$ - загальна кількість працівників підприємства</p>	$K_{зпз}$	Наближення даного коефіцієнту до 1 свідчить про високий рівень заохочення працівників до підвищення рівня інтелектуалізації
4. Показники, що характеризують економічну стійкість підприємства з позицій ринкових факторів ризиків			
4.1. Рівень споживчої прихильності	$K_{спп} = \frac{Ч_{пзак}}{Ч_{загз}}$ <p>Де $Ч_{пзак}$ - кількість споживачів, які робили повторні придбання ТК послуг</p> <p>$Ч_{загз}$ - кількість споживачів, які робили одноразові придбання телекомунікаційних послуг</p>	$K_{спп}$	Наближення даного коефіцієнту до 1 свідчить про високу прихильність споживачів
4.2. Потенціал життєвого циклу телекомунікаційної галузі	Значення встановлюється за результатами експертної оцінки	$П_{жцп}$	Наближення коефіцієнту до 1 свідчить про високий потенціал ринку
4.3. Потенціал життєвого циклу телекомунікаційних послуг	Значення встановлюється за результатами експертної оцінки	$П_{жцп}$	Наближення коефіцієнту до 1 свідчить про високий потенціал послуг

Опитувальний лист виявлення основних чинників, які впливають розвиток управління ризиками телекомунікаційних підприємств у 2018-2020рр.

1. Назва телекомунікаційного підприємства

2. Основний сегмент ринку

	Економ сегмент
	Масовий сегмент
	Люкс-сегмент
	Змішаний

3. Вкажіть кілька найбільш значущих, на вашу думку, факторів, що впливають на зниження кількості послуг.

- Зниження рівня доходів населення (1)
 - Зниження смності внутрішнього ринку (2)
 - Зростання інфляції (3)
 - Зростання цін на послуги (4)
 - Сезонні коливання (5)
 - Інше (вказати) (6)
- Розподіліть фактори за рівнем їхньої значущості

4. Вкажіть можливі причини недостатнього фінансування телекомунікаційних підприємств.

- Труднощі отримання банківських кредитів, внаслідок негативної кредитної історії (1)
 - Зменшення надходження коштів від господарських операцій через підвищення ринкових цін та скорочення обсягів реалізації (2)
 - Зміна структури витрат на підприємстві (3)
 - Зростання процентної ставки на кредит (4)
 - Зростання тарифів та податків (5)
 - Зниження прибутку (6)
 - Інше (вказати) (7)
- Розподіліть фактори за рівнем їхньої значущості

5. Укажіть що на Вашу думку оказує вплив на умови цифровізації підприємстві

Рівень розвитку ІТ-технологій (1)

Рівень розвитку технологічного забезпечення процесів цифровізації (2)

Рівень інтелектуалізації систем управління знаннями суб'єктів господарювання (3)

Якість систем інтелектуального управління клієнтським капіталом (4)

Інше (вказати) (5)

Розподіліть фактори за рівнем їхньої значущості

6. Укажіть що на Вашу думку вплинуло на вибір обладнання Вашого підприємства

Рівень потужності і покриття (1)

Рівень впливу на навколишнє середовище (2)

Рівень високопродуктивності персональних систем (3)

Врахування всіх вимог до вхідних потоків даних (навантаження, швидкість, а також вже наявна техніка) (4)

Ємність середовища передачі даних:
телефонні лінії, волоконно-оптичні кабелі,

коаксіальні кабелі, бездротові та інші канали зв'язку (5)

Інше (вказати) (6)

Розподіліть фактори за рівнем їхньої значущості

7. Вкажіть можливі причини невідповідності телекомунікаційної продукції Вашого підприємства вимогам міжнародних норм стандартизації та сертифікації

Рівень відповідністю екологічним стандартам (1)

Рівень об'єднаності специфічних для галузей стандартів (2)

Рівень життєвого циклу телекомунікаційної продукції в системі екологічного управління (3)

Рівень надання телекомунікаційних послуг за встановленими показниками якості (4)

Інше (вказати) (5)

Розподіліть фактори за рівнем їхньої значущості

Додаток Ф

Значення індикаторів «Фінансово-економічні фактори» телекомунікаційних підприємств за 2018-2020рр.

Назва показника	ПраТ «Київстар»		ПраТ «ВФ Україна»		ТОВ «Укртелеком»		ТОВ «Lifeseil»					
	2018	2019	2020	2018	2019	2020	2018	2019	2020			
Коефіцієнт фінансового ризику	0,38	0,62	0,94	0,68	0,78	0,96	0,41	0,39	0,41	1,92	1,90	1,32
Коефіцієнт автономії	0,73	0,62	0,51	0,59	0,60	0,51	0,70	0,62	0,71	0,34	0,35	0,43
Коефіцієнт ліквідності	0,26	0,27	0,3	0,53	0,57	3,74	0,89	0,78	0,99	0,17	0,12	0,21
Рентабельність (збитковість) активів	29,22	36,43	40,11	9,55	10,15	3,83	3,75	3,57	2,31	-4,25	-8,18	17,17
Рентабельність (збитковість) власного капіталу	40,24	56,53	77,98	16,09	17,75	7,48	5,34	8,19	3,25	-12,41	-23,7	39,77
Коефіцієнт маневреності власного оборотного капіталу	0,08	-0,35	-0,78	-0,36	-0,44	-0,35	-0,022	-0,08	0,08	-1,77	-1,73	-1,17

Значення індикаторів оцінки концепту «Фактори цифровізації» телекомунікаційних підприємств за 2018-2020рр.

Назва показника	ПраТ «Київстар»			ПраТ «ВФ Україна»			ТОВ «Укртелеком»			ТОВ «Lifeseil»		
	2018	2019	2020	2018	2019	2020	2018	2019	2020	2018	2019	2020
Рівень впровадження цифрових технологій	0,9	0,9	1	0,8	0,9	0,9	0,7	0,8	0,8	0,8	0,82	0,84
Коефіцієнт використання цифрових технологій	0,81	0,86	0,91	0,89	0,88	0,89	0,77	0,75	0,74	0,87	0,88	0,91
Рівень інформаційної відкритості	1,1	1,2	1,3	0,9	0,8	0,9	0,87	0,86	0,83	0,72	0,75	0,81
Рівень повноти використання цифрових послуг	0,88	0,87	0,87	0,79	0,8	0,81	0,78	0,79	0,78	0,64	0,65	0,65

Значення індикаторів оцінки концепту «Еколого-енергетичні фактори» телекомунікаційних підприємств за 2018-2020рр.

Назва показника	ПраТ «Київстар»			ПраТ «ВФ Україна»			ТОВ «Укртелеком»			ТОВ «Lifecell»		
	2018	2019	2020	2018	2019	2020	2018	2019	2020	2018	2019	2020
Рівень енергозабезпечення	0,29	0,38	0,48	0,13	0,18	0,15	0,14	0,16	0,15	0,11	0,11	0,12
Рівень диверсифікації екосистем	0,58	0,57	0,61	0,59	0,58	0,56	0,49	0,48	0,48	0,34	0,35	0,36
Рівень впливу діяльності на екосистему	0,55	0,57	0,59	0,63	0,64	0,65	0,65	0,65	0,66	0,71	0,71	0,72
Коефіцієнт енергетичності продукції	0,33	0,37	0,38	0,41	0,41	0,42	0,34	0,35	0,35	0,46	0,44	0,46
Індекс відповідності вимогам сертифікації	0,5	0,5	0,7	0,4	0,5	0,5	0,4	0,5	0,6	0,5	0,5	0,6

Значення індикаторів «Фактори інтелектуалізації діяльності» телекомунікаційних підприємств за 2018-2020рр.

Назва показника	ПраТ «Київстар»			ПраТ «ВФ Україна»			ТОВ «Укртелеком»			ТОВ «Lifecell»		
	2018	2019	2020	2018	2019	2020	2018	2019	2020	2018	2019	2020
Рівень інтелектоорієнтованої компоненти	0,9	0,94	0,96	0,96	0,96	0,84	0,29	0,29	0,31	0,96	0,96	0,92
Рівень соціальної компоненти	0,76	0,84	0,64	0,6	0,88	0,88	0,068	0,11	0,14	0,88	1	0,92
Рівень кваліфікації персоналу	0,67	0,71	0,81	0,76	0,88	0,84	0,56	0,62	0,63	0,84	0,84	0,72
Рівень можливості персоналу	0,88	0,84	0,76	0,68	0,88	0,88	0,25	0,25	0,31	0,4	0,44	0,64
Рівень розвитку здібностей персоналу	0,55	0,56	0,53	0,61	0,74	0,67	0,23	0,24	0,24	0,67	0,72	0,77

Наукове видання

ГУДЗЬ Олена Євгенівна
ЗАХАРЖЕВСЬКА Аліна Анатоліївна

**РОЗВИТОК УПРАВЛІННЯ РИЗИКАМИ
ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ
В РЕАЛІЯХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ**

Монографія

Технічний редактор Лисенко В.Ф.

Формат 60x84 1/16. Ум. друк. арк 11,63. Тираж 98. Зам. 157.

Видавець і виготовлювач СПД ФО Лисенко В. Ф.
25029, м. Кропивницький, вул. Пацаєва, 14, корп. 1, кв. 101. Тел.: (0522) 322-326
Свідоцтво суб'єкта видавничої справи ДК № 3904 від 22.10.2010
E-mail: kod@kod.kr.ua

