



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Український державний університет науки
і технологій

НАУКОВІ ТА ПРИКЛАДНІ АСПЕКТИ ОБЛІКОВО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ РИЗИК-ОРІЄНТОВАНОГО УПРАВЛІННЯ

(колективна монографія)

Дніпро, 2022 рік

УДК 005.52 : 005.334

Н 34

Автори:

**Марценюк Л. В., Дронь М. А., Бобиль В. В.,
Топоркова О. А., Ломтева І. М., Сначов М. П.**

Рецензенти:

Косова Т. Д. – доктор економічних наук, професор, завідувач кафедри фінансів, обліку та оподаткування Національного авіаційного університету

Жадько К. С. – доктор економічних наук, професор, завідувач кафедри підприємництва та економіки підприємства Університету митної справи та фінансів

Рекун І. І. – доктор економічних наук, доцент, професор кафедри фінансів та економічної безпеки Українського державного університету науки і технологій

Рекомендовано до друку вченою радою Українського державного університету науки і технологій (протокол №3 від 28 грудня 2021 року)

Головний редактор: **Бобиль В. В.**, доктор економічних наук, професор, завідувач кафедри обліку і оподаткування Українського державного університету науки і технологій

Н 34 Наукові та прикладні аспекти обліково-аналітичного забезпечення ризик-орієнтованого управління [Текст] / під заг. ред В. В. Бобиля. – Укр. держ. ун-т науки і технологій, Дніпро, 2022. – 164 с.

ISBN

У монографії досліджуються теоретико-економічні, організаційні та прикладні основи формування інформаційного забезпечення бухгалтерського обліку та ризик-орієнтованого управління в різних галузях економіки.

Теоретичною і методологічною базою наведених в монографії досліджень є наукові концепції і теоретичні розробки провідних вітчизняних і закордонних вчених в галузі управлінського обліку, ризик-менеджменту, а також чинне законодавство, нормативно-правові акти з питань господарської діяльності, обліку та оподаткування, в тому числі результати досліджень міжнародних професійних організацій бухгалтерів та аудиторів. Монографія розрахована на широке коло вітчизняних фахівців, науковців, державних службовців у сфері управлінського обліку та ризик-менеджменту, студентів, аспірантів та викладачів, що цікавляться даною сферою.

УДК 005.52 : 005.334

© Марценюк Л. В., Дронь М. А.,
Бобиль В. В., Топоркова О. А.,
Ломтева І. М., Сначов М. П.

© Укр. держ. ун-т науки і технологій,
2022

ПЕРЕДМОВА

Бізнес-середовище завжди пов'язане з різноманітними ризиками, які узагальнено поділяються на внутрішні та зовнішні. Традиційно вважається, що внутрішні фактори визначаються технологічною специфікою та є наслідками роботи менеджменту підприємств та організацій. До зовнішніх факторів відносять регуляторні зміни, політичну ситуацію, природні явища, конкуренцію в галузі та інші економічні чинники. Спрогнозувати такі фактори досить складно. І, ситуація з COVID-19 це наочно підтверджує. Отже вміння виявляти, ідентифікувати ризики і знижувати їх негативні наслідки є важливим аспектом функціонування підприємств в умовах нестабільності та невизначеності.

Наразі, до бізнесу все більше висувається вимога соціальної відповідальності, екологічності, відповідального споживання ресурсів тощо. Потенційних користувачів все більше цікавить інформація щодо впливу компанії на суспільство, економіку, навколишнє середовище, взаємозв'язок стратегії її розвитку із загальносвітовими тенденціями та орієнтація на майбутнє. Сучасні вимоги до менеджменту та інформаційної бази управління підприємством виходять за межі суто фінансових звітів і потребують даних про інші аспекти діяльності, а саме: економічні, соціальні та екологічні. Найближчим часом нефінансова звітність буде ефективним інструментом внутрішньої та зовнішньої політики фінансово-господарської діяльності підприємств, що стане базисом для розробки та реалізації стратегічних проектів бізнесу.

Умови господарювання економічних суб'єктів характеризуються наявністю значної кількості інформації, яка слугує для різних управлінських потреб. Особлива роль в цьому належить бухгалтерській інформації, до якої висуваються вимоги зіставності, можливості узагальнення, групування, порівнювання. Стрімкий розвиток цифровізації нашого суспільства впливає на усі можливі сфери діяльності. Але, інтеграція у світовий простір вимагає застосування уніфікованих підходів до формування звітності в такому форматі, який буде зрозумілий потенційним користувачам з інших країн також. Особливої актуальності в цьому контексті набуває перевірка такої звітності та можливості її аналітичної інтерпретації. Реалії сьогодення вимагають від апарату управління новітніх підходів до ризик-менеджменту, створення відповідних засад організації і ведення бухгалтерського обліку, узагальнення і подання інформації у звітності, виокремлення центрів відповідальності для раціонального використання наявних ресурсів тощо, тому актуальність обраних авторами напрямів досліджень не викликає сумнівів.

Монографія являє собою систематизовані результати досліджень науково-педагогічних працівників кафедри «Облік і оподаткування» й «Економіка та менеджмент» Українського державного університету науки і технологій.

У монографії досліджуються теоретико-економічні, організаційні та прикладні основи формування інформаційного забезпечення бухгалтерського обліку та ризик-орієнтованого управління в різних галузях економіки.

Перший розділ «Проблемні аспекти ризик-орієнтованого управління» присвячений питанням економічної безпеки бізнесу, а саме таким специфічним видам ризиків, як: економічний, інформаційний, фінансовий. Також наведений вичерпний перелік юридичних ризиків суб'єктів господарювання, запропоновано напрямки їх мінімізації з урахуванням міжнародного досвіду.

Другий розділ «Обліково-аналітичне забезпечення ухвалення управлінських рішень» зосереджує увагу на засобах комунікації зі стейкхолдерами. Зазначено, що у період фінансової нестабільності підприємства роблять акцент на інформативність звітності, її прозорість, зіставність, зручність для користувачів. Наголошено на доречності переходу до інтегрованої звітності, яка традиційно повинна містити показники, що характеризують фінансовий стан і фінансові результати діяльності підприємства. Також розглянуто облікову систему суб'єктів зовнішньоекономічної діяльності в контексті інформаційного підґрунтя менеджменту. Основну увагу зосереджено на складових такої системи та формуванні простору ризик-оцінювання.

У третьому розділі «Наукові та прикладні аспекти управлінського обліку» проаналізовано шляхи впровадження стратегічного управлінського обліку залізничної галузі України в умовах реформування та структурних змін. Акцент зроблено на виокремлення центрів відповідальності з урахуванням зарубіжного досвіду та євроінтеграційних процесів, що відбуваються в Україні. Систематизовано підходи до управління витратами та можливості їх застосування в умовах АТ «Укрзалізниця». Розглянуто базові напрями запровадження бюджетування на залізничному транспорті.

У даній монографії автори узагальнили і доповнили результати багатьох наукових досліджень та розробок із вищезазначеної проблематики. Значну увагу приділено дослідженню питань ризик-менеджменту та якості обліково-аналітичного забезпечення в різних секторах економіки, наголошено на доцільності впровадження управлінського обліку. Розкрито необхідність ідентифікації, аналізу та оцінювання ризиків в умовах невизначеності.

Наукова праця може бути корисною здобувачам вищої освіти, аспірантам, науково-педагогічним працівникам закладів вищої освіти, а також бухгалтерам, менеджерам, економістам, фінансистам тощо.

Авторський колектив висловлює щирі вдячності рецензентам: доктору економічних наук, професору, завідувачу кафедри фінансів, обліку та оподаткування Національного авіаційного університету Тетяні Дмитрівні Косовій; доктору економічних наук, професору, завідувачу кафедри підприємництва та економіки підприємства Університету митної справи та фінансів Костянтину Степановичу Жадько; доктору економічних наук, доценту, професору кафедри фінансів та економічної безпеки Українського державного університету науки і технологій Івану Івановичу Рекуну.

РОЗДІЛ 1. ПРОБЛЕМНІ АСПЕКТИ РИЗИК-ОРІЄНТОВАНОГО УПРАВЛІННЯ

1.1. Напрями мінімізації юридичних ризиків суб'єктів господарювання

Ризик – це ймовірність настання наслідків в результаті небажаної, незапланованої події. В повсякденному житті суб'єкти господарювання часто стикаються із незапланованими подіями, а отже і з наслідками цих подій. Передбачити ризики в той чи іншій мірі за допомогою відповідних методик дослідження цілком можливо. Якщо фізична чи юридична особа зможе вчасно передбачити або прорахувати ризик, то в неї буде час і на підготовку до прийняття відповідних мір задля зниження негативних наслідків. Теж саме стосується і національної безпеки України – існує безліч ризиків та їх наслідків, що гіпотетично можуть вплинути на безпеку держави, тому вчасно передбачити ризики, прорахувати небажані наслідки та провести захисні або превентивні дії є складним завданням, але таким, що може бути реалізованим, за умови відповідних грамотно побудованих у правовому полі заходів з боку держави.

В літературі виділяють дві основні теорії ризику – класичну та неокласичну. У *класичній теорії* економічний ризик ототожнюється з математичними очікуваннями втрат, які супроводжують процес реалізації обраного рішення. Основні положення даної теорії криються у визначенні ризику як ймовірності збитків і втрат, які супроводжують обрану стратегію або рішення. Однак, подібне одностороннє тлумачення ризику, на наш погляд, не є об'єктивним.

Згідно *неокласичної теорії*, ризик – можливість відхилення від поставлених завдань.

Варто зазначити, що поняття «ризик» може трактуватися по-різному в залежності від конкретної сфери дослідження. Під ризиком в науці ризикології розуміють небезпеку втрат, можливість яких виникає з особливостей видів діяльності людини або природних явищ.

Американський економіст Френк Найт в 1921 році у своїй роботі «Ризик, невизначеність і прибуток» висловив думку, що ризик є кількісним виміром невизначеності [1].

Ризик – існування або ж можливість виникнення ситуації, за якої формуються передумови протидії реалізації національних цінностей, інтересів та цілей забезпечення національної безпеки [28].

З економічної точки зору можна виокремити безліч потенційних ризиків, наприклад, ресурсний, операційний, кредитний, репутаційний, стратегії, проекту,

інновацій, якості, зміни валютних курсів, зміни облікової ставки, податкових змін, переривання процесу та інші.

Господарський ризик виникає при будь-яких видах діяльності. Він характеризується як небезпека потенційно можливої, ймовірної втрати ресурсів чи не доодержання доходу порівнянно з варіантом, розрахованим на раціональне використання ресурсів [2]. Підприємницький ризик – діяльність суб'єктів господарювання, пов'язаної з подоланням невизначеності в ситуації неминучого вибору, в процесі якої є можливість оцінити вірогідність досягнення бажаного результату, невдачі і відхилення від мети, що містяться у вибраних альтернативах всіх видів підприємницької діяльності. Основними функціями підприємницького ризику є: регулююча, з виділенням негативного та позитивного аспектів; захисна (історико-генетичний і соціально-правовий аспекти) [3].

Вчасне усвідомлення ризиків того чи іншого бізнес-напряму або проекту чи окремої господарської операції та застосування інструментів мінімізації таких ризиків може допомогти уникнути зайвих фінансових втрат.

Саме нехтування визначенням внутрішніх (організаційних та юридичних) ризиків та їх попередженням є результатом настання негативних для підприємства наслідків.

Ризик розглядається як правова категорія, пов'язана з питаннями відповідальності, для визначення характеру вчиненого правопорушення і тому досліджується в межах адміністративного, господарського, кримінального, цивільного права тощо [4].

Національна безпека – це комплексне поняття, яке складається з багатьох компонентів, серед яких: політична, економічна, громадська, екологічна, військова, технологічна, інформаційна та інші види безпеки, які охоплюють різні сфери життя окремих громадян, суспільства та держави в цілому та покликані сприяти сталому розвитку та функціонуванню держави.

В статті 7 Закону України «Про основи національної безпеки України» – Загрози національним інтересам і національній безпеці України – наголошено, що на сучасному етапі основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві є [29]:

у зовнішньополітичній сфері: посягання на державний суверенітет України з боку інших держав;

у сфері державної безпеки: загроза посягань на територіальну цілісність, економічний, науково-технічний і оборонний потенціал України, права і свободи громадян; поширення корупції в органах державної влади, зростання організованої злочинної діяльності;

у воєнній сфері та сфері безпеки державного кордону України: поширення зброї масового ураження; недостатня ефективність існуючих структур і механізмів забезпечення міжнародної безпеки та глобальної стабільності; нарощування іншими державами поблизу кордонів України угруповань військ та озброєнь;

у внутрішньополітичній сфері: порушення з боку органів державної влади та органів місцевого самоврядування Конституції і законів України, прав і свобод людини і громадянина, в тому числі при проведенні виборчих кампаній, недостатня ефективність контролю за дотриманням вимог Конституції і виконання законів України;

в економічній сфері: істотне скорочення внутрішнього валового продукту; зростання кредитних ризиків; нераціональна структура експорту; велика торгова залежність держави; небезпечне для економічної незалежності України зростання частки іноземного капіталу у стратегічних галузях економіки; «тінізація» національної економіки;

у сфері цивільного захисту: зростання ризиків виникнення надзвичайних ситуацій техногенного та природного характеру;

в інформаційній сфері: прояви обмеження свободи слова та доступу до публічної інформації; комп'ютерна злочинність та комп'ютерний тероризм.

Правову основу національної безпеки становлять Конституція та інші нормативно-правові акти, які гарантують захист фундаментальних прав людини і громадянина, організацію державної влади, утвердження загальнолюдських цінностей.

До первинних нормативних актів у галузі національної безпеки належать: Декларація про державний суверенітет України, ухвалена Верховною Радою 16 липня 1990 р., Постанова Верховної Ради «Про проголошення незалежності України» від 24 серпня 1991 р., Акт проголошення незалежності України, ухвалений 24 серпня 1991 р., що отримав підтримку на Всеукраїнському референдумі 1 грудня 1991 р. Ці нормативні акти стали правовою базою, якою врегульовувалися суспільні відносини суверенної Української держави та її національної безпеки. Ряд нормативних актів у галузі законодавства про національну безпеку виступають похідними конституційного права, оскільки виражають політичну волю Української держави.

Нормативні акти в галузі законодавства про національну безпеку за законом і за юридичною силою поділяються на конституційні, законодавчі; укази та розпорядження Президента України; постанови та розпорядження Кабінету Міністрів України; нормативні акти міністерств і відомств; міжнародні договори, згода на які була надана Верховною Радою України.

Конституція України як джерело найвищої юридичної сили забезпечення національної безпеки містить найголовніші установчі норми, якими регулюються суспільні відносини. Більше того, установчий характер мають не тільки окремі її положення, які слугують правовим підґрунтям у галузі національної безпеки, а й уся Конституція в цілому, її положення сприяють становленню більшості основних інститутів конституційного права, насамперед державного і суспільного ладу, прав і свобод людини і громадянина, форм безпосередньої демократії, організації державної влади й місцевого самоврядування та ін. Конституція визначає також механізм здійснення функцій забезпечення державної безпеки.

В системі національного права України провідною галуззю є конституційне право, адже воно закріплює суспільні відносини, що становлять основи повновладдя народу України в сфері національної безпеки.

Загальними принципами забезпечення державної безпеки є: суверенність і незалежність держави, державного ладу України; утвердження і забезпечення прав і свобод людини і громадянина; верховенство права; мирне врегулювання конфліктів; своєчасність засобів забезпечення державної безпеки загрозам; постійність забезпечення державної безпеки; професійність, наукова обґрунтованість, чітке розмежування функцій і повноважень та взаємодії органів державної влади у забезпеченні державної безпеки; використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки; максимальне врахування внутрішніх і зовнішніх умов забезпечення державної безпеки.

Стан державної безпеки і її забезпечення в кожній країні, у тому числі в Україні, зумовлюється рядом чинників. Основні чинники, які впливають на державну безпеку та її забезпечення, можна умовно поділити на три групи: державні (національні) інтереси; загрози державній безпеці і пріоритетним державним (національним) інтересам; інші.

Конституція України визначає та забезпечує захист фундаментальних цінностей — незалежність, територіальну цілісність і суверенітет, гідність, демократію, людину, її права і свободи, верховенство права, добробуту, миру та безпеку [30].

Розрізняють різні типи безпеки: за масштабом (міжнародна, регіональна, локальна); за суб'єктами (особиста, суспільна, національна, колективна); за суспільними сферами (політична, економічна, військова, екологічна, радіаційна тощо). Національна безпека України забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, військовій, екологічній, науково-технологічній, інформаційній та інших сферах.

Економічна безпека є важливою складовою національної безпеки України, вона визначає стан, або рівень національної безпеки держави. Складовими економічними безпеки є: макроекономічна безпека, фінансова безпека, зовнішньоекономічна (експортна, імпортна, митна безпека) безпека, інвестиційна безпека, виробнича безпека, продовольча безпека та ін.

Згідно з абз. 2 ст. 1 Закону України «Про основи національної безпеки України» від 19 червня 2003 р. № 964-IV «національна безпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у тому числі, у сфері податково-бюджетної політики та інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам».

Економічна безпека – стан економіки, при якому забезпечується стійке економічне зростання; ефективне задоволення економічних потреб; контроль держави за рухом і використанням національних ресурсів; захист економічних інтересів країни на національному та міжнародному рівнях. Економічна безпека України – здатність національної економіки до відтворення та протистояння дестабілізуючій дії чинників, що створюють загрозу збалансованому розвитку країни, здатність до забезпечення конкурентоспроможності національної економіки у світовій системі господарювання, здатність реалізувати власні економічні інтереси [31].

Сутність економічної безпеки України полягає у мінімізації можливих суперечностей та протиріч між державою, суб'єктами підприємницької діяльності та громадянами в процесі їх функціонування та взаємодії. Потрібно врахувати інтереси суспільства, країни, держави, регіону, підприємства, людини [4, с. 235]. При цьому є ймовірність виникнення різного роду ризику, і в першу чергу, юридичного. Юридичний ризик – це наявний або потенційний ризик для надходжень та капіталу, який виникає через порушення або недотримання банком вимог законів, нормативно-правових актів, угод, прийнятої практики або етичних норм, а також через можливість двозначного їх тлумачення.

Юридичний ризик – це діяльність суб'єкта права в умовах невизначеності та неможливості точного прогнозування своїх дій, що може призвести до негативних наслідків, наприклад, завдання шкоди третій стороні, що призведе до настання негативних юридичних наслідків у вигляді кримінальної, адміністративної або дисциплінарної відповідальності [5].

Юридичні ризики розрізняються в залежності від своєї природи, походження, структури тощо. *Керовані* (природні, кримінальні, технічні) та *некеровані*

(договірні, маркетингові, фінансові, юридичні, політичні); *внутрішні* (невідповідність діяльності організації, установчих документів, практик укладення угод актуальним вимогам і нормам законодавства, недостатньо ефективна діяльність юридичного департаменту суб'єкта господарювання, відсутність належної координації з керівним складом, непроведення юридичної експертизи кожної угоди, законодавчо грубі помилки при укладанні різного роду угод) та *зовнішні* (законодавчі зміни, вимушене або умисне невиконання зобов'язань контрагентами тощо).

В економічній діяльності суб'єктів господарювання, на наш погляд, вкрай важливо виявити саме юридичні ризики. Під юридичними ризиками розуміємо можливість настання подій, не передбачених сторонами угоди, що впливають на результати діяльності.

Оцінити та мінімізувати ризики – одне з найважливіших завдань для успішного функціонування підприємства.

Більшості юридичних ризиків можна уникнути, вірно розставивши пріоритети вже на початковому етапі підписання тієї чи іншої угоди.

Ситуацію ризику (при здійсненні діяльності певних посадових осіб відповідної правової компетентності) утворюють наступні компоненти: умови небезпеки та виникнення конфлікту інтересів; неможливість точного прогнозування та передбачення потенційних ризиків та їх наслідків; ймовірність як негативних, так і позитивних наслідків настання умов ризику; ймовірність заподіяння шкоди третім особам; ймовірність юридичної відповідальності суб'єкта господарювання внаслідок негативних наслідків ризикованих дій.

Складовими правовими компонентами поняття «юридичного ризику» є: наявність компетенції у суб'єкта ризику щодо впливу на ситуацію; наявність джерел права, що передбачають дії суб'єкта в умовах ризику; юридична відповідальність за спричинення шкоди третім (невинним) особам внаслідок своєї неправомірної ризикової діяльності.

Щодо економічного ризику, то його трактують як кількісна міру здатності підприємця творчо використовувати елемент невизначеності в процесі відтворення або окремих його моментах для отримання додаткової вартості [6].

Основними економічними ризиками науковці вважають такі [7, с. 26]:

- операційний ризик – це ризики нестабільності функціонування банківської системи;

- ринковий ризик – ризики можливостей зміни параметрів ризику в негативний бік, що сприятиме втратам на всіх рівнях економіки;

- кредитний ризик – ризик відсутності можливості виконання зобов'язань контрагентом кредитних відносин, унаслідок чого можуть виникнути ризики

прямих фінансових втрат (державний ризик, наприклад, дефолт, ризик банківської системи й усіх учасників фінансових операцій);

–діловий ризик – ризик втрати ділової репутації;

–ризик ліквідності – це ризик неможливості покриття певних збитків власним капіталом;

–ризик, пов'язаний із регулювальними органами – різка зміна політики уряду, що призведе до підвищення небезпеки банкрутства приватних компаній (наприклад, підвищення податків або політики протекціонізму) [8].

Основним юридичним складником цієї групи ризиків є можливість настання втрат у сфері суспільного відтворення через помилково або лобістські прийняті законодавчі акти у сфері економіки. Методами зниження переважної більшості економічних ризиків є стимулювання розвитку страхування, правова формалізація економічних взаємовідносин між суб'єктами економіки, ефективне функціонування системи господарського судочинства.

Кількість і якість ризиків зростає пропорційно до «ступеня свободи» суспільства й кількості виборів можливих варіантів подальшого розвитку. «Там, де немає вибору, не виникає ризикована ситуація і, відповідно, не буде ризику», – зазначає А. П. Альгін [9, с. 14].

Модель юридичного ризику в сучасному суспільстві має такий вигляд: народ (джерело влади) – реалізація влади (через політичні ініціативи) – законодавче закріплення соціальних (суспільних) норм у чинному законодавстві – реалізація цих норм – юридичні ризики.

На державному рівні юридичні ризики проявляються в прийнятті неправильних господарських законів або допущенні помилок у державному управлінні фінансами, що може призвести до погіршення макроекономічної ситуації в країні й виникнення системних кризових явищ, подолання яких буде вимагати додаткових ресурсів (дефіцит бюджету, інфляція, криза виробничої сфери економіки, безробіття та ін.). Для зниження цих ризиків використовуються різноманітні методи планування й прогнозування: статистичний вимір прожиткового мінімуму та потреб у ресурсах, планування бюджетних доходів і видатків тощо [10, с. 101].

В процесі своєї діяльності суб'єкти господарювання укладають різного роду угоди, які передбачають певні обов'язки перед особами, які його укладають та надають їм відповідні права. В сучасних мінливих умовах завжди є ризик невиконання контрагентами тих чи інших зобов'язань. Цивільний кодекс України (далі – ЦК України) регулює відносини між сторонами Договору. Ризик у цивільному праві – ценесприятливі наслідки, які можуть наступити і за які

не відповідають ані сторони, ані треті особи [11].

Юридичні ризики можна поділити на: 1) *суб'єктивні* (усвідомлення особою можливого виникнення шкоди внаслідок здійснення нею правомірних дій, спрямованих на досягнення корисного результату); 2) *об'єктивні* (загроза виникнення негативних наслідків майнового або немайнового характеру, причому зміст ризику пов'язується з можливістю нанесення шкоди певним благам та інтересам, тому ризик існує незалежно від того, усвідомлюють люди його наявність чи ні, враховують чи ігнорують його); 3) *суб'єктивно-об'єктивні* (ризик породжується процесами, що залежать та не залежать від волі чи свідомості людини) [12].

На наш погляд, ризик має суб'єктивно-об'єктивну природу, тому повинен розглядатися як можливість свідомого вибору певного варіанта дій з урахуванням об'єктивної та невідвортної небезпеки, яка загрожує цивільним правам та інтересам, а також можливих наслідків ймовірного характеру.

Як убачається із низки статей ЦК України, ризик як правова категорія отримує нормативну конкретизацію як поняття та інститут на нормативному рівні (ризик підприємництва, страховий ризик, ризик у підрядних відносинах тощо). Тобто можна припустити існування окремих груп «ризиків» при здійсненні особами суб'єктивних цивільних прав.

В чинному законодавстві надано різні варіанти тлумачення цього поняття, пов'язані з: ризиком у підприємницькій діяльності; ризиком у страховій діяльності; зобов'язальним ризиком тощо [11].

Наведені ризики у науці цивільного права класифікуються залежно від джерел небезпеки, що кваліфікується як ризик. Поділ ризиків на види може проводитися й за іншими критеріями. Так, за місцем у правовідношенні можна виділити ризик невиконання зобов'язання від «зовнішніх» обставин та алеаторний ризик настання випадку як «внутрішньої» умови зобов'язання; за характером – ризик абсолютний і відносний; за вольовою ознакою – ризик підприємництва, ризик випадку; а також штучний ризик.

До групи ризику підприємництва, виходячи зі змісту ЦК України та Господарського кодексу України (далі – ГК України), належить: а) ризик підприємництва (ст. 42 ГК України); б) ризик збитків учасників товариства з обмеженою відповідальністю, пов'язаних з діяльністю ТОВ (абз. 1 ч. 1 ст. 140 ЦК України, ч. 3 ст. 80 ГК України); в) ризик збитків акціонерів, пов'язаних з діяльністю акціонерного товариства (абз. 1 ч. 2 ст. 152 ЦК України, ч. 2 ст. 80 ГК України); г) ризик збитків вкладників командитного товариства, пов'язаних із діяльністю товариства (ч. 1 ст. 133 ЦК України) [11].

Група страхових ризиків включає в себе: 1) ризик випадкової загибелі або

пошкодження майна (ст. 323 ЦК України); 2) ризик випадкового знищення або пошкодження товару (ст. 668 ЦК України); 3) ризик випадкового знищення або пошкодження предмета застави (ст. 580 ЦК України); 4) ризик випадкового знищення або пошкодження майна, переданого під виплату безстрокової ренти (ст. 742 ЦК України); 5) ризик випадкового знищення або пошкодження майна, переданого під виплату ренти на певний строк (ст. 743 ЦК України); 6) ризик випадкового знищення або пошкодження речі, переданої у найм (ст. 772 ЦК України); 7) ризик випадкового знищення або пошкодження предмета договору лізингу (ст. 809 ЦК України); 8) ризик випадкового знищення або пошкодження матеріалу, переданого для виготовлення, переробки, обробки, ремонту речі (статті 837, 842 ЦК України); 9) ризик підрядника щодо неможливості використання наданого ним матеріалу або устаткування (ч. 2 ст. 879 ЦК України); 10) ризик випадкового знищення або пошкодження об'єкта будівництва (ст. 880 ЦК України) [11].

Група зобов'язальних ризиків поділяється на ризики забезпечувального характеру і ризики, що забезпечують безперервність правового впливу на учасників зобов'язальних правовідносин (вони стосуються як предметної складової зобов'язання, так і договірної складової). Ці ризики компенсуються за механізмом страхування відповідальності (ст. 979 ЦК України) [11].

Грунтовне дослідження провела науковець І. В. Волосенко, яка класифікувала юридичні ризики на: а) ризики, пов'язані із невиконанням або неналежним виконанням зобов'язання (ризики строку виконання, місця виконання, способу виконання, предмета виконання тощо); б) ризики, пов'язані із предметом надання (ризик невиконання грошового і майнового зобов'язання); в) ризики, пов'язані із правовими наслідками (ризик припинення зобов'язання, ризик відповідальності і звільнення від неї); г) ризики, пов'язані із видом зобов'язання (ризики з одностороннього правочину і договірною зобов'язання); ґ) ризики, пов'язані із суб'єктним складом зобов'язального правовідношення (ризик невиконання зобов'язання з боку боржника або кредитора).

До основних видів зобов'язального ризику нею пропонується відносити ризик випадкової загибелі або випадкового пошкодження речі і ризик зміни обставин договору [13].

В сучасному цивільному праві зазначена категорія має важливе значення при вирішенні питання про притягнення неналежного боржника до відповідальності. Відповідальність особи, що не виконала або неналежним чином виконала зобов'язання при здійсненні підприємницької діяльності, за чинним законодавством не ставиться у залежність від її вини. Так, щодо випадку невиконання або неналежного виконання зобов'язання чинним законодавством

передбачено загальне правило, згідно з яким враховується лише невинуватість боржника, яка обумовлена непереборною силою.

Так, В. О. Тархов під випадком як підставою невинуватості розуміє «наслідки, які не охоплюються і не повинні охоплюватися передбаченням зобов'язаної особи, не можуть бути поставлені їй у вину»[14].

В юридичній літературі всі види випадку традиційно поділяють на простий і кваліфікований у вигляді непереборної сили – форс-мажору. Відповідно дост. 617 ЦК України особа, яка порушила зобов'язання, звільняється від відповідальності за порушення зобов'язання, якщо доведе, що це порушення сталося внаслідок випадку або непереборної сили [15].

У теорії права випадок інколи визначають через ризик як передумову виникнення такої ймовірної обставини. Особливість правового режиму ризику в ризикових зобов'язаннях полягає в тому, що обставини непереборної сили, інші види випадків включаються до переліку умов диспозитивно-ризикових договорів як правомірної, штучно передбаченої умови, настання якої є підставою припинення зобов'язання, а не загальною підставою звільнення від відповідальності [16].

Одним із видів зобов'язального ризику вважається договірний ризик, який полягає в ймовірності виникнення істотних змін обставин, з яких сторони виходили при укладенні договору, настання яких є підставою для його зміни або розірвання, якщо інше не передбачено договором або не впливає із його сутності (п. 1 ч. 2 ст. 652 ЦК України). До таких змін обставин можуть бути віднесені дії або події, що перебувають поза впливом суб'єктів відносин, які тягнуть за собою неможливість виконання договору, втрату інтересу до нього однієї зі сторін тощо (політичні, законодавчі зміни тощо) [11].

Ризик зміни обставин договору означає обтяження сторони господарсько-невигідними наслідками при зміні обставин, причому, якщо ризик припадає на одну із сторін, вона повинна виконати договір, навіть якщо для неї це збитково [17].

Грунтовні дослідження в площині теорії ризиків провели автори у статті [18], які розробили модуль для оцінки інвестиційних ризиків (на прикладі віртуальної ІТ-компанії). За допомогою методу експертної оцінки дослідники розробили відповідну модель, що дозволяє швидко проаналізувати 23 параметри ризику та пропонує напрями прийняття оптимального рішення інвестування [18].

На питаннях збільшення дохідності та зменшення ризикованості портфелю активів при прийнятті управлінських рішень зосередили свою увагу науковці у статті [19].

Науковці в статті [20] вказують, що посилення конкуренції на внутрішньому та зовнішньому ринках призводить до великої кількості факторів, що впливають

на розвиток та ефективність банківської діяльності. Це супроводжується банківськими ризиками, основним компонентом яких є ринковий ризик. Автори запропонували набір інструментів, орієнтованих на якісне управління ризиками [20].

Пошуку ефективних шляхів управління ризиками присвятили своє дослідження і науковці у статті [21]. На їхню думку, використання інструментів управління ризиками дозволить уникнути зайвих витрат та вжити запобіжних заходів, співмірних з ризиками. Автори пропонують обрати суб'єкту господарювання одну з трьох стратегій: прийняти ризик (залучити підрядника), пом'якшити ризик (залучити підрядника, але зберігати при цьому контроль) або уникати ризику (надавати послуги самостійно). В будь-якому випадку, наголошують автори, не потрібно нехтувати теорією управління ризиками, адже оцінка та врахування ризиків може стати запорукою досягнення поставленої суб'єктом господарювання мети.

Проблемам соціального ризику та інструментам управління його можливим проявам присвятили свої дослідження науковці у статті [22].

Як бачимо, аналізу та мінімізації наслідків різного роду ризиків присвятили свої дослідження чимало науковців. Так, Науковець І.В. Маркова, О.М. Лук'янова, В.А. Волохов наполягають на необхідності вивчення, передбаченні та розподілу ризиків внаслідок державно-приватного партнерства у різних сферах господарювання [23; 24].

Черевиков Є. Л. та Єрофеева Т. А. вважають, що ключовим у ефективному розподілі ризиків є принцип, відповідно до якого певні види ризиків мають закріплюватися за тими учасниками, які найбільш пристосовані до оцінки, контролю та управління ризиками [25].

Управління ризиками у проектах державно-приватного партнерства надзвичайно важливий та складний процес, ефективний механізм якого заснований на забезпеченні партнерам належних умов для виконання своїх зобов'язань; перекладанні партнером частини своїх ризиків на осіб, які залучаються для виконання проекту; наданні гарантій повного виконання своїх зобов'язань особам, які також залучаються для реалізації проекту в рамках ДПП тощо [26].

Сутність *юридичних методів управління ризиками* полягає у використанні основних положень чинного законодавства з метою профілактики ризиків і нейтралізації їх негативних наслідків. До складу юридичних методів ризик-менеджменту входять: кримінально-правові; адміністративно-правові; цивільно-правові. Адміністративні методи управління ризиками це методи управління, дія

яких заснована на силовому примусі. Група адміністративних методів управління ризиками включає в себе організаційні, розпорядчі та дисциплінарні методи.

Економічні методи управління ризиками засновані на раціональному розподілі фінансових ресурсів організації з метою мінімізації потенційних втрат і максимізації можливих доходів, що виникають в ситуаціях ризику. Діапазон економічних методів управління ризиками досить різноманітний і включає в себе методи: компенсації; спекулювання; стимулювання; стримування [27].

На нашу думку, щоб передбачити ризики та відповідно, уникнути негативних наслідків від них, потрібно володіти повною та достовірною інформацією про предмет, що досліджується, інтуїцією, а також мати достатній запас знань задля проведення аналітичної обробки даних, що є в наявності.

В умовах карантинних обмежень внаслідок поширення коронавірусної хвороби у світі питання національної безпеки кожної країни стало на перший план. Економічний спад на фоні падіння обсягів у багатьох сферах призвів до збільшення агресії як всередині держави, між громадянами єдиного суспільства, так і по відношенню до інших держав. Екологічна, медична, інформаційна, економічна та інші види безпеки стали першочерговим питанням на нарадах найвищого рівня керівників держав.

Ситуація з пандемією коронавірусу, що виникла в Україні у березні 2020 року, викрила недоліки медичної системи; загострила питання економічної безпеки внаслідок скорочення обсягів виробництва, тотального скорочення кадрів, уходу багатьох підприємств в тіньову економіку; виявила недостатній розвиток діджиталізації в країні тощо [32].

На наш погляд, науковець Нікітін Ю.В. слушно зауважує, що утопічно створювати раціональні протидії загрозам на всі випадки життя, їх неможливо закріпити в юридичних актах. Адже законодавець, так само, як і інші, не в змозі точно передбачити майбутнє. Але законодавство можна побудувати на встановлених закономірностях відомої частини причин і наслідків загроз та небезпек. Тому право здатне конструювати лише загальні принципи – сталість виявлення, пізнання і подолання національних загроз [33].

На наш погляд, в Україні потрібно запровадити дієву систему оцінювання ризиків і загроз у сфері національної безпеки. Для цього на національному, регіональному та місцевому рівнях пропонуємо залучити широке коло компетентних осіб (представників міністерств і відомств, профільних наукових та експертно-аналітичних установ, органів місцевого самоврядування, представників бізнесу, громадянського суспільства тощо).

Задля мінімізації юридичних ризиків суб'єктів господарювання потрібно: мати в штаті компетентного відповідального працівника, який оцінюватиме

юридичні ризики та їх наслідки; визначати усі можливі ризики при укладанні угод; визначати критерії допустимості ризику при укладанні угод; сформувати оперативну інформаційну систему, в межах якої можлива передачі інформації між підрозділами стосовно ймовірності настання того чи іншого ризику; постійний моніторинг не тільки внутрішніх, а й зовнішніх ризиків; страхування юридичних ризиків. Крім того, ефективним захистом суб'єкта господарювання від недоброчесних контрагентів можуть стати уніфіковані, розроблені саме фахівцями-юристами конкретного підприємства типових угод, контрактів, договорів тощо; облік та аналіз усіх контрагентів підприємства із створенням бази доброчесних та недоброчесних партнерів; підвищення кваліфікації юридичного персоналу організації.

Ми припускаємо, що недоброчесні контрагенти можуть приховувати негативну інформацію про свою організацію, тому при укладанні угод потрібно вивчити інформацію про ймовірного контрагента із доступних джерел, наприклад, з різного роду реєстрів, в тому числі звернутися до ресурсів прокуратури, трудової інспекції, а також моніторити інформацію із засобів масової інформації.

Окремо хотілося б зупинитися на господарюванні залізниць. В умовах хронічного недофінансування з боку держави в останні десятиліття та внаслідок цього катастрофічного зносу рухомого складу та транспортної інфраструктури, доцільним є впровадження державно-приватного партнерства на залізницях.

Успішний досвід подібного співробітництва можна спостерігати у багатьох розвинених країнах світу. Міжнародний досвід свідчить про високу ефективність партнерських відносин між державою та приватним сектором, а також про доцільність залучення зовнішніх інвестиційних ресурсів під час реалізації складних масштабних проєктів у різних галузях. Аналіз світової практики державно-приватного партнерства дозволяє зробити висновок про те, що найбільш затребуваною є співпраця між державою та приватними інвесторами в соціальній сфері, транспортній сфері та у сфері енергетики.

Основною причиною зацікавленості держави в участі приватних інвесторів є дефіцит фінансів, оскільки, як правило, ініціативи в соціальній сфері та сфері інфраструктури є надзатратними. Водночас, зважаючи на стрімкий розвиток технологій, трансформацію суспільства та економічних процесів, неможливим є ігнорування адекватного розвитку рівня інфраструктури. Таким чином, у держави з'являється потреба розділити з кимось тягар капіталовкладень у розвиток вказаних сфер, який є об'єктивно непосильним для державного бюджету навіть найбільш розвинених держав.

До того ж світовий досвід доводить, що залучення приватного капіталу до реалізації важливих, але затратних інфраструктурних та соціальних проєктів,

дозволяє досягти стрімкого розвитку та економічного зростання без значних капіталовкладень з боку держави, які можуть бути використані більш раціонально на інші цілі.

За умови ґрунтовного підходу до планування проєктів державно-приватного партнерства можна досягти достатньо високих показників [36].

В Україні ж подібна форма співпраці тільки набирає оберти, адже не так давно затверджено новий Закон «Про концесію», який регулює відносини між учасниками інвестиційних проєктів, якими є як державні, так і приватні контрагенти.

На українських залізницях державно-приватне партнерство поки що спостерігається лише при організації вантажних перевезень та є наміри стосовно допуску концесіонерів до вокзалів деяких міст-мільйонників.

На наш погляд, такий точковий процес не зможе вивести залізничний транспорт із кризи. Задля оновлення транспортної інфраструктури та рухомого складу необхідно залучати інвесторів на умовах концесії в якомога більших сферах діяльності залізниць, при чому в такому разі, на наш погляд, виграють і залізничники, і пасажирів, і бюджети усіх рівнів.

Формування системи управління залізничного транспорту України на основі державно-приватного партнерства є визначальним чинником його демонополізації та наближення до інтеграції в загальноєвропейську транспортну мережу. Дослідження ризиків на основі визначення функцій держави та приватних структур при виконанні залізничних перевезень та утриманні інфраструктури, діючих в межах державно – приватного партнерства, обумовлюють подальший розвиток соціально значимих пасажирських перевезень, вантажних перевезень, збільшення парку власних вагонів, модернізацію об'єктів інфраструктури, створення умов для використання власних магістральних локомотивів, розвиток конкуренції на залізничному транспорті [35].

Заслуговує на увагу наступна класифікація ризиків у процесі реалізації ДПП-проєктів:

Ризики

1. Проектування та розробка: придатність дизайну; проблеми розробки; проблеми впровадження; варіації проектування та розробки; надання послуг проектування.

2. Будівництво: фіксований термін та вартість проєкту; графік постачання; затвердження плану; безпечність для навколишнього середовища; порушення наявних методів роботи; підготовка будівельного майданчика; перевезення будівельних засобів до буд майданчика; варіації будівництва; трудові суперечки.

3. Фінанси: забезпечення фінансування; збереження фінансування (включаючи позики); відсоткова ставка та податкові поправки; податкові правила; ціна ескалації капітальних вкладень.

4. Управління: надання послуг / побудова об'єкту інфраструктури; наявність послуг / засобів виробництва; ремонт та витрати на технічне обслуговування; безпека; навчання персоналу; пристосування до вимог споживачів; операційні витрати; приховані недоліки наявних засобів будівництва; зміни у попиті.

5. Власність: застраховані збитки або пошкодження активів; моральне та фізичне зношення; державне та місцеве законодавство; громадські обов'язки; форс-мажорні обставини; реалізація залишкової вартості активів [39].

На підставі досліджень інших науковців можна класифікувати ризики, які виникають у процесі реалізації проектів державно-приватного партнерства, наступним чином:

1) ризики, викликані дією зовнішніх факторів: форс-мажорні ситуації, здатні впливати на цілісність об'єкта державно-приватного партнерства; зміна макроекономічної ситуації, що може позначитися на виконанні умов угоди;

2) політичні ризики: дії державних органів стосовно майна, переданого приватному партнеру за умовами угоди; зміни у чинному законодавстві, які можуть відобразитися на можливості приватного партнера погашати фінансові зобов'язання; розробка нових стандартів відносно 20 продукції приватного партнера або модернізація порядку надання дозволів або погоджень тощо;

3) ризики невиконання сторонами партнерства покладених на них зобов'язань: несвоєчасне здійснення інвестицій або будь-яких інших передбачених виплат; невиконання зобов'язань щодо якості і кількості товарів або послуг, передбачених угодою; порушення строків виконання робіт;

4) комерційні ризики: ризик неотримання доходу від підприємницької діяльності внаслідок зміни ринкових цін або зменшення попиту на товари або послуги; виникнення непередбачуваних витрат для реалізації проекту державно-приватного партнерства; зміна умов угоди в односторонньому порядку під час реалізації проекту тощо [26, с. 360].

Задля визначення потенційних ризиків, а також їх розподілу між учасниками інвестиційного проекту в Україні рекомендовано застосовувати Методику виявлення ризиків здійснення державно-приватного партнерства, їх оцінки та визначення форми управління ними.

Ці рекомендації можуть бути корисними для усіх контрагентів на всіх етапах співробітництва, починаючи від моменту укладання угоди та закінчуючи розподілом прибутку.

В результаті аналізу дослідники намагатимуться виявити ймовірність настання тих чи інших негативних наслідків в результаті настання тих чи інших подій.

Після визначення потенційних ризиків кожен з них оцінюється з точки зору ймовірності настання. Ймовірність ризику може бути визначена як низька, середня або висока. Крім ймовірності ризиків, рекомендується оцінити вплив кожного ризику за шкалою: низький-помірний-високий.

Безумовно, маючи уяву про ймовірні ризики та наслідки від них, суб'єкт господарювання може завчасно прийняти превентивні заходи задля пом'якшення негативних наслідків того чи іншого виду ризиків [34].

По мірі того, як організації у всьому світу намагаються адаптуватися до віддаленої роботи своїх співробітників, серйозне зростання числа витоків даних стало повсякденним явищем.

Зверніть увагу на ці факти:

1. 47% співробітників назвали відволікання уваги причиною того, що вони потрапили на фішингову аферу під час роботи з дому (Tessian).
2. Число порушень в веб-додатках з 2019 року подвоїлась і тепер становить 43% від числа всіх порушень (Verizon).
3. 52% керівників стурбовані сторонніми кібер-ризиками через віддаленої роботи співробітників під час пандемії коронавірусу COVID-19 (Gartner).
4. Дистанційна робота збільшила середній збиток від порушення даних на 137 000 доларів США (IBM).
5. 81% фахівців з інформаційної безпеки повідомили, що їх посадові функції змінилися під час пандемії ((ISC).
6. У квітні 83% технологічних компаній повідомили про нові запитах клієнтів, 36% з яких належать до сектору інформаційної безпеки (CompTIA)
7. Кількість пошукових запитів «Як видалити вірус» в березні 2020 року збільшився на 42% (Google Trends).
8. З січня по березень 2020 року використання мобільного VPN виросло на 8,3% (WatchGuard).
9. 76% віддалено працюючих співробітників говорять, що робота з дому збільшить час на виявлення і стримування порушення ІБ (IBM).

Крім того:

1. У США в травні 33 000 заявників на допомогу з безробіття зіткнулися з порушенням інформаційної безпеки в рамках програми допомоги безробітним під час пандемії (телекомпанія NBC).
2. У березні шахрайство зросла на 400%, що зробило COVID-19 найбільшою загрозою безпеці в історії (ReedSmith).

3. У квітні Google заблокувала 18 мільйонів щоденних шкідливих і фішингових листів, пов'язаних з коронавірусів (Google).

4. Півмільйона облікових записів користувачів Zoom були зламані і продані на форумі в «тіньовому Інтернеті» (CPO Magazine).

5. Кожен день створюється 1 767 тематичних доменних імен про коронавірус з високим рівнем ризику (Palo Alto Networks).

6. У Великобританії був знищений 471 підроблений інтернет-магазин, який торгує підробленими товарами, пов'язаними з COVID-19 (ZDNet).

7. У квітні стався витік 450 активних адрес електронної пошти з Всесвітньої організації охорони здоров'я (ВООЗ) і тисячі адрес електронної пошти співробітників групи реагування COVID-19 (ВООЗ).

8. Відвідуваність популярних хакерських сайтів і форумів збільшилася на 66% в період з березня по травень 2020 роки (cybernews).

Є над чим замислитися і стосовно наступних фактів:

1. У середньому кібер-атака обходиться компаніям в 3,86 мільйона доларів США, а на її виявлення і усунення потрібно до 280 днів (IBM).

2. У 2020 році загальносвітові державні витрати на ІТ склали 438 мільярдів доларів США (Gartner).

3. 54% британців, які зазнали втрату доходу через COVID-19, також постраждали від кібер-афер (Computing).

4. Облікові дані користувачів Zoom продаються всього за \$ 0,0020 центів за один акаунт в «тіньовому Інтернеті» (CPO Magazine).

5. До 2021 року щорічний загальносвітовий збиток від кібер-злочинності досягне 6 трлн. доларів США (Cybersecurity Ventures)

6. В 2020 році загальносвітові витрати організацій на інформаційну безпеку скоротилися на 8% (Statista).

7. 70% керівників по ІБ і покупців рішень безпеки прогнозують, що бюджети на інформаційну безпеку скоротяться в 2021 році, але при цьому вони все одно планують запросити значне збільшення бюджету (McKinsey).

8. У середньому персонально ідентифіковані дані клієнтів стоять 150 доларів США за одну запис (IBM).

1. Північна Америка витратила найбільше грошей на державні ІТ у всьому світі в 2020 році, досягнувши рівня в 191 мільярд доларів США (Gartner).

2. Сплеск атак на Республіку Корея був вище, ніж в середньому по світу, на початку березня, після раннього проникнення вірусу в країну (Microsoft).

3. У Великобританії жертви шахрайства, пов'язаного з COVID-19, втратили більше 11 мільйонів фунтів стерлінгів в сукупності станом на 8 липня (Action Fraud).

4. 85% жертв і авторів загроз проживають в одній і тій же країні (Verizon).
5. ФБР і CISA повідомили, що Китайська Народна Республіка націлилася на інтелектуальну власність дослідних організацій в сфері коронавірусу COVID-19 (ФБР).
6. 65% організацій в США зізналися в досягненні нульового або мінімального відповідності американським правилам конфіденційності та безпеки даних (SC Media).
7. Євросоюз розкритикував Великобританію за відсутність законодавства про конфіденційність даних щодо її програми тестування і відстеження в сфері національної охорони здоров'я (DARKreading).
8. Чеська Республіка повідомила про кібер-атаці на Госпіталь Університету в Брно, в результаті якої була відключена вся її IT-мережу (Europol).
9. В 2020 році за півроку в Азіатсько-Тихоокеанському регіоні була здійснена в цілому 216 001 мережева атака (WatchGuard).
10. Середній збиток від порушень інформаційної безпеки в США став найвищий серед усіх інших країн світу - 8,64 мільйона доларів США (IBM)

Ці статистичні дані про інформаційну безпеку в епоху коронавірусу COVID-19 дають можливість заглянути в майбутнє комп'ютерних тенденцій. Цілком можливо, що сервіси стануть більш орієнтовані на хмари. Час покаже, що нове покоління технологій матиме для домашніх користувачів, органів влади або підприємств, але в будь-якому випадку завжди необхідно залишатися пильним і використовувати комплексний антивірусний захист [37].

В процесі господарювання підприємства, в тому числі і залізниці, повинні намагатися передбачити та запобігти інформаційним ризикам. Найбільш популярні Методології оцінки IT ризиків наступні: Методологія оцінки ризиків Національного Інституту Стандартів та Технологій США (National Institute of Standards and Technology – NIST), Методологія аналізу інформаційних ризиків Міжнародного Форуму з інформаційної безпеки (Information Risk Analysis Methodology – IRAM), Методологія аналізу факторів ризиків інформаційних технологій (Factor Analysis of Information Risk - FAIR), Методологія пропорційного аналізу ризиків (MESARI), Метод оцінки операційно критичних загроз, активів та уразливостей (Operationally critical threats, assets and vulnerability evaluation – OCTAVE).

Методики оцінки IT ризиків повинні враховувати специфіку роботи суб'єкта господарювання. Окремі етапи оцінки IT ризиків повністю автоматизовані; розроблені (або розробляються) системні утиліти для оцінки ризиків; надаються утиліти для моделювання загроз та уразливостей; є програмне забезпечення та документи для проведення оцінки.

Необхідно готувати персонал для проведення аудиту інформаційної безпеки (внутрішнього та зовнішнього) та управління ризиками ІТ. Необхідно забезпечити впровадження методики та консультаційну підтримку.

Управління інформаційними ризиками включає такі етапи: аналіз та оцінку ризиків; вибір та оцінку рішень за результатами аналізу ризиків; створення та впровадження набору заходів та засобів для своєчасного зменшення рівня ризиків до припустимої величини згідно з міжнародними стандартами ISO; впровадження моніторингу, аудиту та контролю стану інформаційної безпеки для оцінки ефективності процесу управління ризиками. Під час виконання оцінки ризиків здійснюється: інвентаризація й оцінка цінності інформаційних активів; ідентифікація відповідних вимог законодавства та нормативної бази; ідентифікація загроз і вразливостей інформаційної безпеки та оцінка ймовірності їх здійснення; детальний технічний аналіз уразливостей інформаційних систем організації щодо загроз та оцінка величини ідентифікованих загроз; визначення системи організаційних заходів із підтримки режиму інформаційної безпеки; визначення величини та ймовірності завдання шкоди в результаті здійснення загроз безпеки.

Необхідно отримати достовірні дані про ймовірність реалізації загрози. Оцінка ризиків інформаційної безпеки складається з таких етапів: визначення переліку об'єктів, що потребують захисту, інформаційною службою підприємства; формування повної множини загроз інформації за методологією; аналіз і вибір переліку загроз, з огляду на особливості функціонування підприємства; виявлення можливих джерел цих загроз; визначення ймовірності здійснення потенційних загроз із використанням експертні оцінки; оцінка можливих збитків в разі здійснення ідентифікованих загроз. Ці збитки будуть складатися з витрат на відновлення інформації, заміну чи ремонт устаткування, комунікацій та програмного забезпечення, на впровадження нових структурних елементів, на навчання і перепідготовку персоналу, на відновлення позицій на ринку та іміджу підприємства тощо [38].

Інформація, яка є у відкритих інтернет-ресурсах, свідчить про те, що в умовах коронавірусу COVID-19 багато підприємств виявили пробоїни у власній кібербезпеці.

Багато організацій перейшли на спонтанні незаплановані хмарні рішення і змушені були терміново придбати додаткові ІТ-продукти і сервіси для адаптації до нових реалій «дистанційки». Прагнучи забезпечити безперервність бізнес-операцій, багато компаній поспішили і змушені були послабити ряд заходів безпеки (або взагалі відмовитися від деяких з них), створивши нові рівні вразливостей і ризиків.

На думку багатьох експертів, навіть після ослаблення карантинних заходів, робота вже не буде на 100% очна, частково робота буде віддалена. А в такому випадку підприємствам просто необхідно розробляти довгострокову стратегію віддаленої безпеки в майбутньому.

Крім обов'язкових антивірусних програм і моніторингу потенційних загроз і наслідків від них на поверхневому рівні, потрібно підійти до питання інформаційної безпеки підприємства системно. Наприклад, необхідно вжити заходи щодо захисту від шифрувальників. Шифрувальники – це одна з найбільш поширених загроз безпеки даних в будь-якій організації, і ця загроза буде продовжувати розвиватися як головна тенденція інформаційної безпеки. Атаки шифрувальників здійснюють крадіжку даних в організаціях, завдаючи по ним серйозні фінансові удари, змушуючи їх нести додаткові витрати на відновлення після цих атак. У 2020 році атаки шифрувальників в середньому обійшлися світу дорожче, ніж середній збиток від всіх видів порушень даних, досягнувши позначки в 4,44 мільйона доларів США.

Методи, які використовуються злочинцями, також стають все більш складними і витонченими. Все більше уваги приділяється атакам, коли злочинці крадуть дані компанії і шифрують їх, щоб ті не змогли отримати до них доступ. Після цього кібер-злочинці починають шантажувати компанію, погрожуючи оприлюднити її дані, якщо не буде виплачено викуп.

У той час як багато компаній покладаються на віртуальні приватні мережі (VPN) для полегшення доступу до своєї корпоративної мережі, VPN не завжди зможе захистити. Найбільш поширеним серед шифрувальників методом входу є фішинг. Мережевий доступ з нульовим довірою (Zero-Trust Network Access, ZTNA) став найбільш безпечним варіантом управління віддаленим доступом до конфіденційних даних, що дозволяє знизити ймовірність атаки. До 2023 року 60% підприємств, за оцінками експертів, поступово відмовляться від VPN і перейдуть на ZTNA.

Крім паролів в якості інформаційної безпеки рекомендується використовувати багатофакторну аутентифікацію (MFA) в якості додаткового захисту від витоків даних і шкідливих атак. MFA передбачає використання двох або більше окремих факторів при наданні користувачам доступу до захищених даних, змушуючи людей використовувати більше одного пристрою для підтвердження своєї особи. Прикладом MFA в дії є одноразовий код доступу, відправлений на два або більше пристроїв (на телефони співробітників компанії наприклад).

Слід згадати і про штучний інтелект. Штучний інтелект і машинне навчання стають все більш витонченими і потужними, і компанії продовжать «відточувати»

ці технології в майбутньому як частину своєї інфраструктури безпеки. Штучний інтелект все частіше використовується для створення автоматизованих систем безпеки, які замінюють людину, дозволяючи аналізувати величезну кількість даних про ризики набагато швидшими темпами. Це вигідно як великим компаніям, що мають справу з величезними обсягами даних, так і малим або середнім компаніям, чії служби безпеки можуть бути недостатньо забезпечені ресурсами.

У той час як штучний інтелект надає велику можливість для більш ефективного виявлення загроз серед підприємств, еволюція та розширення використання цієї технології йде в обох напрямках. Злочинні мережі використовують переваги штучного інтелекту для автоматизації та вдосконалення своїх атак.

Рекомендуємо підприємствам впровадити в свій бізнес системи безпеки на базі штучного інтелекту задля оптимізації зусиль з виявлення загроз і потенційно заощадити немалі кошти в разі витоку даних.

Потрібно максимально убезпечити хмарні сервіси, якими користується конкретна компанія. Важливо оцінити наслідки для безпеки, пов'язані з хмарою, і визначити існуючі та потенційні вразливості.

З ростом числа гучних кібер-атак, які розкривають мільйони записів персональної інформації, побоювання з приводу конфіденційності, управління і безпеки даних різко зросли. Організації повинні зосередитися на забезпеченні конфіденційності даних в майбутньому.

При формуванні тактики й стратегії захисту суб'єкта господарювання від інформаційних загроз слід приділити увагу не тільки зовнішнім, а й внутрішнім (інсайдерським) потенційним загрозам.

В сучасних умовах на підприємствах різко зростає попит на висококласних фахівців в області інформаційних технологій, а тому організаціям варто заздалегідь укомплектувати свій штат досвідченими в цій сфері співробітниками або організувати відповідне підвищення кваліфікації вже працюючим на підприємстві комп'ютерним геніям.

У зв'язку з вищевикладеним хочемо підкреслити, що інвестиції підприємства в зміцнення власної інформаційної безпеки окупляться в майбутньому і талановитим менеджерам не варто відмовлятися від подібної статті витрат в загальному бюджеті компанії для досягнення блискучих довгострокових перспектив.

Кожному суб'єктові господарювання в разі сумніву стосовно необхідності витрачати відповідні ресурси на прогнозування ризиків та запобігання наслідкам їх впливу потрібно мати на увазі прислів'я: «Якщо ми не управлятимемо ризиками, то вони управлятимуть нами...»

Досвід провідних міжнародних компаній переконливо доводить, що стабільність розвитку бізнесу і підвищення ефективності управління неможливі без активного використання ризик-менеджменту як складової частини системи управління компанією незалежно від її масштабів і специфіки виробництва або надання послуг.

Система управління ризиками спрямована на досягнення необхідного балансу між отриманням прибутку і скороченням збитків підприємницької діяльності і покликана стати складовою частиною системи менеджменту організації, тобто повинна бути інтегрована в загальну політику компанії, її бізнес-плани і діяльність. Тільки при виконанні цієї умови застосування системи ризик-менеджменту є ефективним.

Ризик-менеджмент має на увазі створення необхідної культури та інфраструктури бізнесу для: виявлення причин і основних факторів виникнення ризиків; ідентифікації, аналізу та оцінки ризиків; прийняття рішень на основі проведеної оцінки; вироблення антикризових управляючих впливів; зниження ризику до прийняттого рівня; організації виконання наміченої програми; контролю виконання запланованих дій; аналізу і оцінки результатів ризикового рішення.

Впровадження в практику підприємств системи ризик-менеджменту дозволяє забезпечити стабільність їх розвитку, підвищити обґрунтованість прийняття рішень в ризикованих ситуаціях, поліпшити фінансове становище тощо. Максимально знизити ризики управління можна за допомогою використання жорстких стандартів у частині планування, документування ходу того чи іншого проекту, процедур контролю виконання і управління змінами.

Бібліографічний список до підрозділу 1.1.

1. Основні теорії ризику в економіці. URL: <https://ukr.agromassidayu.com/osnovnie-teorii-riska-v-ekonomike-page-306106>
2. Бондар О. В. Ситуаційний менеджмент: Навч. посіб. К. : Центр учбової літератури. 2010. 326 с.
3. Чуприна І.В. Поняття та класифікація ризиків в підприємницькій діяльності. *Збірник наукових праць ВНАУ Серія: Економічні науки.* 2012. №4 (70). С.187-194.
4. Циба Я.В. Підходи до розуміння поняття «ризик». *Ефективна економіка.* 2012. № 2. URL: <http://www.economy.nayka.com.ua/?op=1&z=2761>
5. Беззубов Д.О. Парадигма юридичного ризику в системі національної безпеки України (прикладний аспект). *Держава і право.* 2010. №47. С. 176-182.

6. Вишняков Я.Д. Общая теория рисков: учеб. пособие для студ. высш. учеб.заведений / Я.Д.Вишняков, Н.Н.Радаев. 2-е изд., испр. М. : Издательский центр «Академия», 2008. 368 с.
7. Старостіна А Ризик – менеджмент: теорія та практика : [навч. посіб.] / А. Старостіна, В. Кравченко. К. : Видавництво «Політехніка», 2004. 200 с.
8. Коренева М. Юридичні складники поняття ризику в адміністративному примусі. *Юридичний вісник*. 2014. №6. С.301-305.
9. Альгин А. Новаторство, инициатива, риск. М. : Знание, 1987. 64 с.
10. Хантингтон С. Столкновение цивилизаций. *Политические исследования*. 1994. № 1. С. 7–14.
11. Цивільний кодекс України [Електронний ресурс] / Верховна Рада України. 2003. URL: <http://zakon3.rada.gov.ua/laws/show/435-15>.
12. А. Б. Гриняк, М. Д. Пленюк. Правова природа ризику в договорах з виконання робіт. *Вісник Національної академії правових наук України*. 2018. Т. 25. № 1. С. 29–49.
13. Волосенко І. В. Ризик у цивільному праві (поняття, природа, види) : автореф. дис. ... канд. юрид. наук :12.00.03 / Волосенко Ірина Василівна; Нац. ун-т ім. Т. Шевченка. Київ, 2011. 19 с.
14. Тархов В. А. Гражданское право. Общая часть Курс лекций. Чебоксары : Чув. кн. изд-во, 1997. 331 с.
15. Книга перша. Загальні положення (ст. 1–268). URL: <https://i.factor.ua/ukr/law-54/section-296/>
16. Тімуш І. С. Цивільно-правове регулювання ризикових (алеаторних) договорів : дис. ... канд. юрид. наук : 12.00.03. Київ, 2004. 198 с.
17. Зейц А. Г. Влияние изменившихся обстоятельств на силу договоров. Иркутск : ИНГ, 1928. 65 с.
18. Lipyanina H., Maksymovych V., Sachenko A., Lendyuk T., Fomenko A., Kit I. (2020) Assessing the Investment Risk of Virtual IT Company Based on Machine Learning. In: Babichev S., Peleshko D., Vynokurova O. (eds) Data Stream Mining & Processing. DSMP 2020. *Communications in Computer and Information Science*, vol 1158. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-61656-4_11
19. Shvets V., Tryfonova O., Solomina H., Petrova Ya. Theoretical and methodological foundations for the evaluation of management efficiency of joint investment institutions. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, 2020. № 5. Pp. 178-183. URL: <https://doi.org/10.33271/nvngu/20205/178>
20. Yana Kuznichenko, Serhiy Frolov, Fedir Zhuravka, Mykola Yefimov and Volodymyr Fedchenko (2018). Regulatory assessment of the bank market risk: international approaches and Ukrainian practice. *Banks and Bank Systems*, 13(4), 73-84.

URL: [https://doi.org/10.21511/bbs.13\(4\).2018.07](https://doi.org/10.21511/bbs.13(4).2018.07)

21. Iryna Bashynska, Olena Sokhatska, Tetiana Stepanova, Marina Malanchuk, Sergii Rybianets, Oksana Sobol (2019) Modelling the Risks of International Trade Contracts. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, Volume-8. Pp.2815-2820. URL: <https://doi.org/10.35940/ijitee.K2313.0981119>

22. Migration risk management as a factor of national security [Electronic resource] / O. Reznik, O. Muzychuk, O. Yunin [and others] // *Journal of security and sustainability issues*, 2020. Vol.94. URL: [https://doi.org/10.9770/jssi.2020.9.4\(29\)](https://doi.org/10.9770/jssi.2020.9.4(29)).

23. Маркова І.В. Ризики та проблеми державно-приватного партнерства на залізничному транспорті. *Ефективна економіка*. 2013. № 11. URL: <http://www.economy.nayka.com.ua/?op=1&z=2471>

24. Маркова І.В., Лук'янова О.М., Волохов В.А. Визначення функцій та розподіл ризиків державно-приватного партнерства на залізничному транспорті. *Вісник економіки транспорту і промисловості*. 2013. № 42. С. 164-168.

25. Черевиков Є. Л., Єрофеева Т. А. Управління ризиками проектів державно-приватного партнерства. *Наукові праці НДФІ*. 2010. № 4 (53). С.48-53.

26. Мостепанюк А.В. Ризики реалізації проектів державно-приватного партнерства: причини виникнення та механізм управління. *Збірник наукових праць Національного університету державної податкової служби України*. 2011. №1. С. 356-367.

27. Боровик М. В. Ризик-менеджмент : конспект лекцій для студентів магістратури усіх форм навчання спеціальності 073Менеджмент. ХНУМГ ім. О. М. Бекетова, 2018. 65 с.

28. О. В. Олійник. Сутність державної політики забезпечення інформаційної безпеки щодо джерел загроз та інших безпекогенних чинників. *Юридичний вісник*. 2016. № 1 (38). С.71-78.

29. ЗАКОН УКРАЇНИ «Про основи національної безпеки України» №964-IV від 18 червня 2003 р. <http://www.spfu.gov.ua/ua/documents/1819.html>

30. Антонов В. О. А Конституційно-правові засади національної безпеки України: монографія. Київ: ТАЛКОМ, 2017. 576 с. С.455-480.

31. Шиян Д.С., Шиян О.Ю. Економічна безпека як об'єкт кримінального правопорушення щодо нецільового використання бюджетних коштів. Сучасні проблеми забезпечення національної безпеки держави: тези III Міжнародної науково-практичної конференції (26 листопада 2020 року). К.: Інститут УДО України КНУ імені Тараса Шевченка, 2020. 391 с. С.220-222.

32. Єремєєва А.М. Тугарова О.К. Економічна складова інформаційної безпеки держави в умовах пандемії. Актуальні проблеми управління

інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. Київ : НА СБУ, 2021. 346 с. С.262-263.

33. Нікітін Ю. В. Національна безпека України в сучасних умовах: ризики і фактори впливу. *Юридична наука*. 2015. № 2. С. 141-147.

34. Про затвердження Методичних рекомендацій щодо застосування Методики виявлення ризиків здійснення державно-приватного партнерства, їх оцінки та визначення форми управління ними. Методичні рекомендації. наказ міністерства економічного розвитку і торгівлі України від 7 червня 2016 року N944. <https://ips.ligazakon.net/document/ME160668>

35. І. В.Маркова. Ризики та проблеми державно-приватного партнерства на залізничному транспорті. *Ефективна економіка* № 11, 2013. <http://www.economy.nayka.com.ua/?op=1&z=2471>

36. Юлія Зуєва. Закордонні кейси з ДПП: порівняльний аналіз. URL: yur-gazeta.com/publications/practice/derzhavnoprivatne-partnerstvo/zakordonni-keys-i-z-dpp-porivnyalniy-analiz.html

37. 43 статистических факта про ИБ во время COVID-19. <https://www.cloudav.ru/mediacenter/news/covid-cybersecurity-statistics/>

38. Л.Ф. Єжова. Економічні аспекти ризиків інформаційної безпеки. *Сучасна спеціальна техніка*. 2011. № 3(26). С. 80-91.

39. Department of Defence 2001, Private Financing Manual, Organizational Effectiveness Branch, Interim Version, 25 February. – Режим доступу: <http://www.defense.gov>.

ВІДОМОСТІ ПРО АВТОРІВ КОЛЕКТИВНОЇ МОНОГРАФІЇ

РОЗДІЛ 1. ПРОБЛЕМНІ АСПЕКТИ РИЗИК-ОРІЄНТОВАНОГО УПРАВЛІННЯ

1.1. Напрями мінімізації юридичних ризиків суб'єктів господарювання

Марценюк Лариса Володимирівна, доктор економічних наук, доцент, професор кафедри «Економіка та менеджмент», Український державний університет науки і технологій

1.2. Облік і управління фінансовими ризиками банку в умовах економічної нестабільності

Дронь Марина Анатоліївна, аспірантка кафедри «Облік і оподаткування», Український державний університет науки і технологій

РОЗДІЛ 2. ОБЛІКОВО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ УХВАЛЕННЯ УПРАВЛІНСЬКИХ РІШЕНЬ

2.1. Вплив міжнародних стандартів бухгалтерського обліку на розвиток консолідованої фінансової звітності підприємств України

Бобиль Володимир Володимирович, доктор економічних наук, професор, завідувач кафедри «Облік і оподаткування», Український державний університет науки і технологій

2.2. Облікова система та простір ризик-оцінювання суб'єктів ЗЕД

Топоркова Олена Анатоліївна, кандидат економічних наук, доцент, доцент кафедри «Облік і оподаткування», Український державний університет науки і технологій

РОЗДІЛ 3. НАУКОВІ ТА ПРИКЛАДНІ АСПЕКТИ УПРАВЛІНСЬКОГО ОБЛІКУ

3.1. Впровадження стратегічного управлінського обліку на залізничному транспорті

Ломтєва Ірина Миколаївна, старший викладач кафедри «Облік і оподаткування», Український державний університет науки і технологій

3.2. Удосконалення обліку відповідальності на залізничному транспорті України

Сначов Микола Павлович, кандидат технічних наук, доцент, доцент кафедри «Облік і оподаткування», Український державний університет науки і технологій

ЗМІСТ

ПЕРЕДМОВА.....	3
РОЗДІЛ 1. ПРОБЛЕМНІ АСПЕКТИ РИЗИК-ОРІЄНТОВАНОГО УПРАВЛІННЯ	
1.1. Напрями мінімізації юридичних ризиків суб'єктів господарювання.....	6
1.2. Облік і управління фінансовими ризиками банку в умовах економічної нестабільності.....	31
РОЗДІЛ 2. ОБЛІКОВО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ УХВАЛЕННЯ УПРАВЛІНСЬКИХ РІШЕНЬ	
2.1. Вплив міжнародних стандартів бухгалтерського обліку на розвиток консолідованої фінансової звітності підприємств України	59
2.2. Облікова система та простір ризик-оцінювання суб'єктів ЗЕД.....	85
РОЗДІЛ 3. НАУКОВІ ТА ПРИКЛАДНІ АСПЕКТИ УПРАВЛІНСЬКОГО ОБЛІКУ	
3.1. Впровадження стратегічного управлінського обліку на залізничному транспорті	111
3.2. Удосконалення обліку відповідальності на залізничному транспорті України	138
ВІДОМОСТІ ПРО АВТОРІВ КОЛЕКТИВНОЇ МОНОГРАФІЇ	163

Наукове видання

*Марценюк Лариса Володимирівна,
Дронь Марина Анатоліївна,
Бобиль Володимир Володимирович,
Топоркова Олена Анатоліївна,
Ломтева Ірина Миколаївна,
Сначов Микола Павлович*

Наукові та прикладні аспекти обліково-аналітичного забезпечення ризик-орієнтованого управління

КОЛЕКТИВНА МОНОГРАФІЯ

Технічний редактор: Топоркова О. А., к.е.н., доцент, Український державний університет науки і технологій

Головний редактор Бобиль В. В., д.е.н., професор, завідувач кафедри обліку і оподаткування, Український державний університет науки і технологій

Матеріали подано в авторській редакції.
При повному або частковому відтворенні матеріалів даної монографії посилання на видання обов'язкове

Підписано до друку

Формат 60x84/16. Папір офсетний.

Ум. Друк. арк.

Тираж

Український державний університет науки і технологій

Свідоцтво суб'єкта видавничої справи ДК № 1315 від 31.03.2003 р.

Адреса видавництва та дільниці оперативної поліграфії:

49010, Дніпропетровськ, вул. Лазаряна, 2