МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

АЕРОКОСМІЧНИЙ ФАКУЛЬТЕТ

Кафедра машинознавства, стандартизації та сертифікації

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

д.т.н., професор Кіндрачук М.В.

“___” _____ 2020 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИЦІ ОСВІТНЬОГО СТУПЕНЮ

“МАГІСТР”

Тема: Процеси управління та оцінки ризиків в системах менеджменту якості

Виконавиця: Смага І.Ю.

Керівник: к.т.н., доц. Мельник В.Б.

Консультанти з окремих розділів пояснювальної записки:

розд. “Охорона навколишнього середовища”: к.т.н., доц. Мельник В.Б.

Нормоконтролер: к.т.н., доц. Мельник В.Б.

Київ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Аерокосмічний факультет

Кафедра машинознавства, стандартизації та сертифікації
Спеціальність: «Метрологія та інформаційно-вимірювальна техніка»
Освітньо-професійна програма: «Якість, стандартизація та сертифікація»

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.т.н., професор
Кіндрачук М.В.
"___" _____ 2020 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

Смаги Ірини Юріївни

1. Тема кваліфікаційної роботи: «**Процеси управління та оцінки ризиків в системах менеджменту якості**», затверджена наказом ректора від 02. жовтня 2020 року №1901/ст.

2. Термін виконання роботи: з 05 жовтня 2020 р. по 31 грудня 2020 року.

3. Вихідні дані до роботи: удосконалення організації управління ризиками в системах управління якістю на основі дослідження теоретичних основ управління якістю та сучасних концепцій і методів управління ризиками (відповідно до вимог ДСТУ ISO 9001:2015, ДСТУ ISO 31000:2018; ISO 31010:2019; ДСТУ ISO/TR 31004:2018).

4. Зміст пояснювальної записки: Вступ. Розділ 1. Теоретичні основи управління якістю. Розділ 2. Аналіз сучасних концепцій та методів управління ризиками. Розділ 3. Удосконалення процесів управління ризиками в системах управління якістю. Розділ 4. Охорона навколишнього середовища. Висновки.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: схема процесу СУЯ згідно з ISO 9001:2015; куб COSO 2004; процес управління ризиками згідно з стандартом FERMA; тріада «Принципи, структура та процес РМ» згідно із стандартом ISO 31000:2018; алгоритм управління ризиками; класифікація ризиків / можливостей за рівнем; модель Septigon; алгоритм аналізу впливу людського фактора за допомогою методу HRA; узагальнена класифікація кібер-ризиків

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Ознайомитися з літературою та сформувати структуру дипломної роботи.	05.10.11.10.20р.	
2.	Написати вступ та розділ 1: «Теоретичні основи управління якістю».	12.10.-25.10.20р.	
3.	Розробити розділ 2: «Аналіз сучасних концепцій та методів управління ризиками».	26.10-06.11.20 р.	
4.	Розробити розділ 3: «Удосконалення процесів управління ризиками в системах управління якістю».	09.11.-20.11. 20р.	
5.	Розробити розділ 4: «Охорона навколишнього середовища».	23.11.-30.11. 20р.	
6.	Сформулювати висновки по роботі.	02.12-11.12. 20 р.	
7.	Оформити дипломну роботу та здати на рецензію	12.12.-20.12.20 р.	

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняла
Охорона навколишнього середовища	Доцент кафедри машинознавства Мельник В.Б.		

8. Дата видачі завдання: “_____”_____ 2020 р.

Керівник дипломної роботи (проекту) _____ Мельник В.Б.
(підпис керівника) (П.І.Б.)

Завдання прийняла до виконання _____ Смага І.Ю.
(підпис випускника) (П.І.Б.)

.

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Процеси управління ризиками в системах управління якістю»: 114 сторінок, 16 рисунків, 12 таблиць, 73 використані джерела, 12 додатків.

ПРОЦЕС, РИЗИК, СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ, ІМОВІРНІСТЬ, ЗНАЧУЩІСТЬ, ОЦІНЮВАННЯ, ЛЮДСЬКИЙ ФАКТОР

Об’єкт дослідження – управління ризиками в системах управління якістю.

Предмет дослідження – процедури, методи управління ризиками в системах управління якістю.

Мета дослідження – удосконалення організації управління ризиками в системах управління якістю на основі дослідження теоретичних основ управління якістю та сучасних концепцій і методів управління ризиками.

У роботі досліджено теоретичні основи управління якістю; визначено сутність поняття ризику та проведена класифікаціяю його видів; проаналізовано сучасні концепції та методи управління ризиками; розроблено пропозиції щодо удосконалення організації управління ризиками в системах управління якістю.

Розроблені у роботі пропозиції призначені для використання у практичній діяльності підприємств бідь якого розміру, сфери діяльності та форм власності.

Застосування розроблених заходів на практиці дозволить суттєво підвищити ефективність функціонування систем управління якістю суб’єктів надання адміністративних послуг за рахунок запровадження у їх діяльність процесного підходу та єдиних стандартів роботи, одержання об’єктивної інформації щодо якості наданих послуг, оперативного ухвалення управлінських рішень з урахуванням ризиків з метою реального поліпшення та наближення рівня якості адміністративних послуг до потреб замовників. Це дозволить органам місцевого самоврядування відігравати важливу роль у створюванні сталих місцевих громад, в яких надання якісних, економічно ефективних та узгоджених публічних послуг сприяє сталому економічному розквіту і соціальній справедливості на місцевому рівні, розгортаючись та взаємодіючи послідовно й узгоджено з національною та регіональною політикою.

ЗМІСТ

ВСТУП

Управління організацією, поряд з іншими аспектами менеджменту, включає в себе управління якістю. Система управління якістю, впроваджена на підприємстві, спонукає організації аналізувати вимоги споживачів, визначати процеси, які сприяють створенню продукції, прийнятної для споживачів, а також підтримувати ці процеси в керованому стані, що в комплексі сприяє підвищенню задоволеності споживачів. Система управління якістю є основою постійного поліпшення діяльності підприємства та являє собою сукупність політики і цілей в області якості, організаційних документів, процесів, процедур, ресурсів, необхідних для управління якістю та забезпечення зумови відповідності продукції, послуг встановленим вимогам, що відповідають потребам і очікуванням споживача. Вимоги до системи управління якістю нормативно закріплені в міжнародних стандартах ISO серії 9000.

У сучасних умовах мінливості світової економіки функціонування економічної системи України та діяльність її суб'єктів є непрогнозованою та непередбачуваною. Існуюче натепер ринкове середовище неухильно формує умови активізації конкурентних дій, непередбачуваності зовнішнього стану, постійного збільшення обсягів інформації, посилення інтеграційних процесів та розширення глобальних ринкових кордонів, що призводить до високої невизначеності прогнозів щодо можливого попиту, собівартості продукції, рівня рентабельності та кінцевого результату всієї господарської діяльності. Діяльність організацій у невизначеному середовищі завжди пов'язана з виникненням ризиків та можливими втратами, які мають негативний вплив на цю діяльність.

Управління ризиками насьогодні є ключовим аспектом діяльності будь-якої організації, що функціонує в ринковій економіці. Це пов'язано з тим, що фактор ризику виникає в різних сферах діяльності, а своєчасне виявлення, аналіз і прийняття відповідного рішення щодо способу управління тим чи іншим ризиком, дозволяє організації уникнути кризових явищ і тим самим є як захисним

механізмом, так і фактором успіху компанії.

Сучасна версія стандарту ISO 9001 вимагає від організації чіткого розуміння свого контексту та виявлення ризиків як основи для планування системи управління якістюё. Концепція мислення, заснованого на ризик-менеджменті, спрямована на оцінювання ризиків і можливостей, отже, процедури системи управління якістю, зокрема процедура внутрішнього аудиту повинні бути актуалізовані з урахуванням оцінки ризиків.

Зважаючи на важливість та значні потенціні можливості застосування менеджменту ризику для поліпшення функціонування системи управління якістю організацій з одного боку, та недостатній рівень обізнаності керівників вітчизняних підприємств щодо методів і засобів управління ризиками, і, відповідно, недостатній рівень їх упровадження в Україні, актуальним є дослідження сучасних концепцій та методів управління ризиками з подальшим наданням на цій основі рекомендацій щодо їх практичної реалізації.

Виходячи з вищезазначеного, *метою дипломної роботи* є удосконалення організації управління ризиками в системах управління якістю на основі дослідження теоретичних основ управління якістю та сучасних концепцій і методів управління ризиками.

Для досягнення поставленої мети необхідно вирішити наступні *задачі дослідження:*

1. Дослідити теоретичні основи управління якістю.
2. Визначити сутність поняття ризику та провести класифікацію його видів
3. Проаналізувати сучасні концепції та методи управління ризиками.
4. Узагальнити результати досліджень та розробити пропозиції удосконалення організації управління ризиками в системах управління якістю.

Об'єкт дослідження – управління ризиками в системах управління якістю.

Предмет дослідження – процедури, методи управління ризиками в системах управління якістю.

Розроблені у роботі пропозиції можуть бути використаними всіма організаціями, які бажають досягти конкурентної переваги на ринку, які прагнуть до досягнення стійкого успіху, зведення до мінімуму впливу невизначеності на їх

діяльність, а також отримання вигоди від ризиків в організації.

Застосування розроблених заходів на практиці дозволить організаціям визначати фактори, які можуть спричиняти відхилення її процесів та її системи управління якістю від запланованих результатів, щоб установлювати запобіжні заходи контролю для зменшення негативних впливів та якнайбільшого використання можливостей у міру їх виникнення. Окрім того, буде мінімізовано вплив людського фактора на процеси управління та виробничої діяльності організації, що, у кінцевому рахунку, призведе до зменшення її матеріальних збитків від виробництва продукції (надання послуг) невідповідної якості, підвищить довіру споживачів і сприятиме зростанню її конкурентоздатності та стійкому прибутковому функціонуванню.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ЯКІСТЮ

1.1 Основні поняття у сфері управління якістю

Витоки зародження проблеми забезпечення належного рівня якості продукції, послуг, навколишнього середовища і, врешті решт, життя людини можна знайти ще на етапі формування людства як спільноти. Людина завжди прагнула забезпечення належної якості, особливо коли це стосувалося гарантування безпеки використання продукції, користування послугами, збереження її здоров'я, навколишнього природнього середовища і т.і. Сьогодня, в умовах глобалізації ринку, використання надскладної техніки, біо- та нанотехнологій, атомних електростанцій, великої кількості об'єктів підвищеної небезпеки, погіршення екології, загострення безпекових питань, проблема якості стала вкрай актуальною для будь-якої галузі економіки як на національному, так і на міжнародному рівнях. Причому підвищення якості повинно бути безперервним та плануватися на найближчу, середню та довготермінову перспективу.

Поняття якості історично формувалося під впливом виробничих відносин, адже кожне суспільне виробництво мало свої, актуальні для певного історичного періоду розвитку цих відносин вимоги до якості продукції.

Взагалі поняття «якість» – універсальна філософська категорія, яка охоплює як явища зовнішнього світу, так і свідомість людини. Одним з перших досліджував цю категорію давньогрецький філософ Аристотель. Він визначав її як видову відмінність однієї сутності від іншої, що належить до того ж виду [1] та вказував на мінливість якості як зміну стану речей, їх здатність перетворюватись у свою протилежність (справне – пошкоджене, тепле – холодне тощо).

Німецький мислитель Гегель вважав, що «якість є взагалі тотожною з існуванням визначеності… Щось, завдяки своїй якості, є те, що воно є, і, втрачаючи свою якість, перестає бути тим, чим воно є» [1].

Китайський ієрогліф, яким позначається якість, містить дві складові –

«рівновага» та «гроші», тобто за китайською версією якість ототожнюється з чимось висококласним та дорогим [2].

Взагалі можна навести багато визначень, які надавалися поняттю «якість» різними філософами, теоретиками і практиками. Це поняття має безліч аспектів: одні автори виокремлюють філософський, соціальний, економічний, правовий [1, 2, 4], інші додають національний, політичний, моральний, технічний [5-7], тому у кожному з визначень поняття «якість» переважає один з них і жодне з визначень не володіє необхідною повнотою і точністю.

Прикладне визначення якість має для конкретних об'єктів, таких як продукція (послуга), процес, система тощо, а задля його тлумачення використовують традиційний (технократичний) та інноваційний підходи.

За першого підходу якість продукції розглядають як сукупність властивих їй «об'єктивних» характеристик або ступінь їхньої відповідності певним вимогам. Якість тут пов'язується, у першу чергу, з певною виробничою технологією, кваліфікованим персоналом, матеріально-технічною базою. Уся складність розуміння при цьому полягає в тому, яке навантаження бере на себе цей термін стосовно будь-якого об'єкта (виробу, продукції) чи суб'єкта (людини, що виробляє і сприймає об'єкт): розглядаються структура або побудова речі, її вигляд, властивості речі (сутність) чи властивості, що привносяться (на рівні явища, прояву).

Другий підхід припускає інтегрування до процесу формування якості постачальників ресурсів, споживачів, будь-яких зацікавлених осіб, що відповідає сучасним поглядам на управління якістю.

Європейська організація з контролю якості (European Organization for Quality) вважає, що продукція є хорошої якості, якщо «при мінімальних витратах протягом усього її життєвого циклу вона максимально сприяє здоров´ю і щастю людей, які залучені до її проектування і відновлення (повторного використання) за умови мінімальних витрат енергії та інших ресурсів і при допустимій (прийнятній дії на навколишнє середовище і суспільство)» [8]. Це формулювання установлює зв'язок проблеми забезпечення високої якості продукції з такими не менш важливими для всього людства проблемами, як збереження навколишнього природнього

середовища, раціональне використання природних ресурсів тощо.

У стандарті ДСТУ ISO 9000:2015 якість визначена як «ступінь, до якого сукупність власних характеристик об'єкта задовольняє вимоги» [9]. У цьому визначенні вже можна побачити намір кількісного оцінювання якості, як міри відповідності чогось запропонованого та реальної потреби.

Розглянемо основні поняття стосовно управління якістю, надані у [9].

Управління якістю – скоординовані дії щодо спрямовування та контролювання діяльності організації стосовно якості.

Управління якістю включає:

1) формування політики у сфері якості;

2) встановлення цілей щодо якості;

3) процеси для досягнення цілей щодо якості шляхом:

- планування якості;
- контролювання якості;
- забезпечування якості;
- поліпшування якості [9].

Політика у сфері якості – це наміри та спрямованість організації щодо якості, які є офіційно сформульованими її найвищим керівництвом. Як правило, вона є невід'ємною частиною загальної політики компанії, узгоджена з її баченням та місією, є структурним підгрунтям для встановлення цілей щодо якості.

Ціль щодо якості – результат, пов'язаний з якістю, який має бути досягнено.

Планування якості є складовою частиною управління нею, сфокусованою на встановленні цілей щодо якості, визначенні операційних процесів, а також відповідних ресурсів, необхідних для досягнення цих цілей.

Контролювання якості – складовий елемент управління якістю, сфокусований на виконанні вимог стосовно якості.

Забезпечування якості – складовий елемент управління якістю, сфокусований на створюванні впевненості у виконанні вимог стосовно якості.

Поліпшування якості – складовий елемент управління якістю, сфокусований на збільшенні здатності виконання вимог стосовно якості.

Процес – сукупність взаємопов'язаних або взаємодіючих робіт, що

використовують входи для створення запланованого результату, який, залежно від контексту, може називатися виходом, продукцією або послугою.

Вихід є результатом процесу. Чим він є – продукцією чи послугою, залежить від, характеристик які переважають. Наприклад, автомобіль для продажу в автосалоні – продукція, а постачання автомобіля на замовлення – це вже послуга.

Продукція – вихід організації, який може бути виготовлено без будь-якої ділової угоди між організацією та замовником.

Послуга – вихід організації за умови обов'язкового виконання хоча б одного виду робіт між організацією та замовником.

Система управління якістю (СУЯ) є частиною загальної системи управління і являє собою сукупність взаємопов'язаних або взаємодіючих елементів організації для формування політик стосовно якості, установлення цілей стосовно якості і процесів, щоб досягати ці цілі [9].

Для оцінювання дієздатності СУЯ та рівня досягнення поставлених перед нею завдань, визначають такі характеристики системи, як результативність та ефективність.

Під *результативністю* розуміють ступінь реалізації запланованих видів робіт, а також досягнення запланованих результатів.

Ефективність являє собою відношення досягнутих результатів до використаних ресурсів [9].

Звичайно, якщо розглядати питання управління якістю комплексно, то необхідно надати визначення найбільш загальному у цьому сенсі поняттю – концепції.

Отже, *концепція управління якістю* – це система теоретико-методологічних засад (поглядів) щодо розуміння і визначення сутності, змісту, цілей, завдань, критеріїв, принципів і методів управління якістю, а також організаційно-практичні підходи до формування механізму її реалізації в конкретних умовах функціонування організації. Вона повинна включати розроблення методології управління якістю, формування СУЯ і розроблення технологій (методів, методик) управління якістю.

1.2 Ретроспективний огляд підходів до управління якістю

Для кращого розуміння ролі та місця управління якістю у діяльності організації будь-якої форми власності доцільно проаналізувати еволюцію наукової думки та практичної реалізації заходів щодо розвитку підходів до управління якістю порівняно із тенденціями розвитку загального управління підприємством.

Основні історичні етапи розвитку концепцій управління якістю є: індивідуальний, цеховий, приймальний, статистичний контроль якості, комплексне управління якістю, концепції TQC, CWQC, TQM, забезпечення якості на базі стандартів ISO 9000. Кожний з цих етапів має власну логіку та відповідні закономірності розвитку.

За індивідуального контролю якості (діяв на виробництві до кінця XIX ст.), один робітник (невелика їх група) відповідав за виготовлення певних виробів. Кожний з них повністю міг контролювати результат своєї праці, що забезпечувало кінцеву якість виробу. Робітники при цьому виконували роботу за заданим шаблоном (кресленням, моделлю тощо). Цей принцип організації роботи запроваджував перехід від ремісного до індустріального виробництва, коли якість уже визначав не лише талант, майстерність, уміння та навички робітника, а й спроможність його порівнювати результати своєї роботи із заданою моделлю.

На початку XX ст. з'явився цеховий контроля якості, коли функції та відповідальність за якість розподілялася між працівниками та цеховими майстрами або керівниками. Цеховий майстер встановлював загальні вимоги до якості певної продукції та відповідав за якість кінцевого результату роботи цеху. Такий підхід спирався на принципи управління якістю, які запропонував американський фахівець Ф. Тейлор (1856 – 1915): при контролі використовували дві межі припустимої якості; у кресленнях зазначали нижню та верхню межі допусків; шаблони мали пропускні та непропускні типи калібрів; жорсткий економічний та адміністративний контроль виконавців, вимога чіткого дотримання норм щодо якості.

У період Другої світової війни масове промислове виробництво та збільшення

обсягів виробленої продукції спричинили відокремлення технічного контролю від інших виробничих операцій та його оформлення як самостійного професійного виду діяльності. На підприємствах промисловості почали створювати окремі незалежні служби технічного контролю, які мали штатний персонал. Так розпочався етап приймального контролю якості.

З метою забезпечення належної якості процесів виробництва набув розвитку статистичний контроль якості [10]. У середині 30-х років XX-ст. фахівці американської фірми Bell Telephone Laboratories У. А. Шухарт та Дж. Джуран вперше застосували у своїй практичній діяльності один із статистичних методів контролю – контрольну карту Шухарта з регульованими границями[11]. Найважливіша характеристика цього виду контролю якості – перехід від суцільного до вибіркового контролю, коли у процесі виробництва згідно із затвердженим планом систематично підлягають моніторингу визначені контрольні дані, які у наступному обробляються з використанням методів матстатистики.

Проте, через обмеження виробничими рамками, застосування статистичного контролю якості поширювалося дуже повільно. Контроль проводили у рамках цеху, а заданий рівень якості продукції, в основному, досягали завдяки удосконаленню методів та засобів технічного контролю.

На початку 1960-х років новостворювані служби технічного контролю орієнтувалися вже на зростання обсягів випущеної продукції з одночасним зниженням витрат на забезпечення якості та витрат матеріальних ресурсів.

Контроль якості виокремився у сферу спеціалізованої діяльності, завданням якої є управління якістю, аналіз причин виникнення дефектів, розроблення заходів щодо їх усунення, планування та реалізація профілактичних заходів. На підприємствах почали створювати служби управління якістю, до яких входили відділ технічного контролю та група відповідальна за планування та координацію діяльності щодо якості для усіх без виключення підрозділів підприємства. Ці служби були незалежними від інших підрозділів підприємства, а підпорядковувалися напряму вищому керівництву організації.

Загострення конкурентної боротьби та інтенсифікація науково-технічного

прогресу змусили керівників промислових підприємств перейти на принципово новий підхід: треба не виявляти дефектив продукції, а попереджувати їх. Механізм комплексного управління якістю доповнював статистичні методи контролю якості методами збору та обробки інформації про якість, мотивацією персоналу, стандартизацією та сертифікацією.

Базуючись методології комплексного управління якістю, у 1960-1970-х роках ряд провідних країн світу, враховуючи свої національні та економічні особливості, сформували власні організаційні підходи до менеджменту якості на рівні підприємств. Найвідоміші з цих концепцій –TQC (загальний контроль якості) у США та CWQC (управління якістю у межах усієї компанії) у Японії.

Основою для першої є впроваджена на підприємстві СУЯ, яка охоплює усі сфери його діяльності. Тоді рішення проблеми якості є сферою діяльності окремого структурного підрозділу, який займається тільки забезпеченням якості продукції виходить.

Згідно з другою концепцією у роботі щод управління якістю приймає участь весь персонал організації – від керівника до рядового робітника. Отже, методами управління якістю повинні володіти працівники усіх рівнів управління та підрозділів підприємства. Передбачені застосування статистичних методів, внутрішнх перевірок СУЯ, діяльність гуртків якості тощо.

Наприкінці 1980-х рр. з’явилася концепція управління якістю продукції на базі міжнародних стандартів ISO серії 9000, яка визначає, що створення в організації ефективної СУЯ, яка відповідає вимогам цих стандартів, гарантує задоволення вимог споживачів. Одночасно на території колишнього СРСР розвивалися свої концепції управління якістю, серед яких зазначимо Львівську систему бездефектної праці (СБП), Саратовську систему бездефектного виготовлення продукції (БВП), Горьківську систему «Якість, надійність, ресурс з перших виробів» (ЯНАРЗПВ), Ярославську систему наукової організації праці з підвищення моторесурсу (НОРМ), Львівську комплексну систему управління якістю продукції (КС УЯП).

З початку 1990-х рр. починають створювати галузеві версії стандартів щодо управління якістю, які частково є модифікаціями ISO серії 9000. Наприклад, «велика

трійка» американських автомобільних компаній розробила в 1990 р. стандарт QS-9000 «Вимоги до систем якості». Розробляється серія стандартів ISO 14000 з вимогами до системи екологічного управління організації.

У цей же період значного розвитку набуває концепція загального управління якістю (Total Quality Management, TQM) [12]. Ідея концепції полягає у тотальному цілеспрямованому та відповідно скоординованому застосуванні методів та систем управління якістю в усіх сферах діяльності та на всіх стадіях життєвого циклу продукції (від досліджень та розробки до утилізації) за участі персоналу усіх рівнів з оптимальним використанням технічних та інших можливостей.

Складові елементи концепції показані на рис. 1.1.

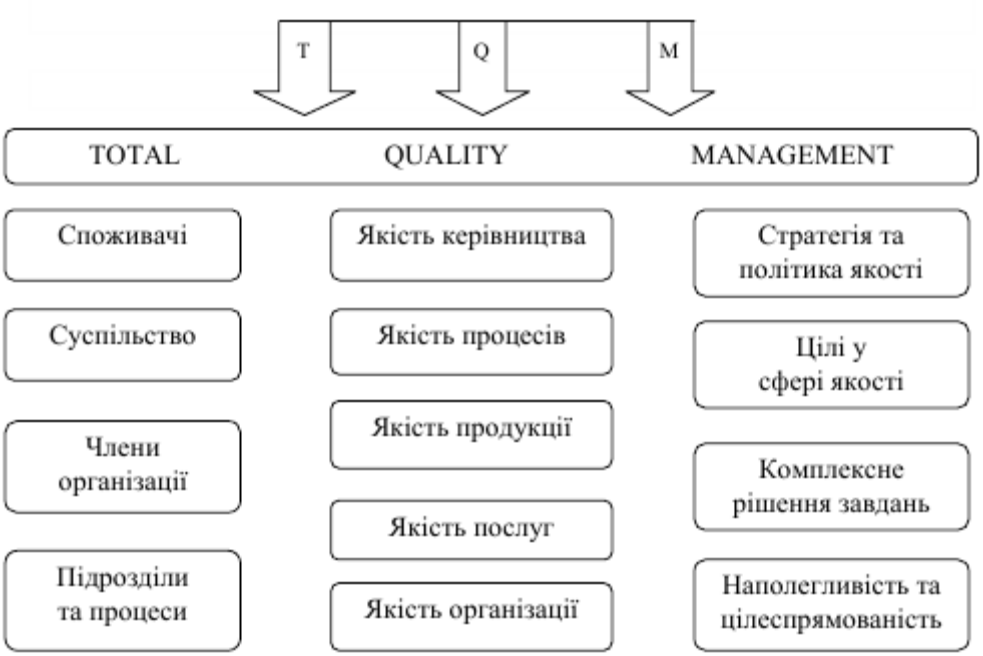

Рис. 1. 1. Складові елементи концепції TQM

Сенс TQM можна інтерпретувати так: T – всеохоплюючий (стосовно видів діяльності) підхід; Q – якість як якість управління, M – управління за принципами, що охоплюють керівників усіх рівнів.

Концепція TQM дозволяє ширше зрозуміти сутність якості, яка містить невловимі відчуття споживача, пов’язані з характеристиками продукції, якістю послуг (терміни надання, умови обслуговування, інформування тощо) та зумовлені якістю процесів.

TQM вимагає орієнтації виробника на задоволення поточних та потенційних потреб споживачів; надання якості рангу основної цілі виробника; раціонального використання усіх наявних ресурсів організації.

Трьома ключовими умовами ефективності TQM є: 1) вища посадова особа організації підтримує та активно пропагує ідею підвищення якості; 2) першочергові інвестиції здійснюються у персонал, а не в обладнання; 3) організаційні структури перетворяться або створюються спеціально під TQM.

Підходи концепції TQM до управління якістю значною мірою збігаються з підходами, зазначеними у нових версіях стандартів ISO серії 9000. З огляду на те, що на сьогодняшній день ці стандарти визнані найбільш ефективними у сфері управління якістю, розглянемо основні їх положення та вимоги до СУЯ більш детально.

1.3 Системи управління якістю на базі стандартів ISO серії 9000

Стандарти ISO серії 9000 були розроблені з метою сприяння організаціям у впровадження та забезпечення функціонування ефективних та результативних СУЯ. Універсальність цих стандартів дозволяє застосовувати їх вимоги і рекомендації підприємствам та організаціям будь-якої сфери діяльності (виробничої, сфери надання послуг), розмірів та складності організаційної структури.

1 версія серії стандартів ISO 9000 була підготовлена в 1987 р.

2 версія серії була видана у 1994 р., являючи собою уточнену версію попередньої.

3 версія серії була розроблена у 2000 р. і радикально відрізнялася від попередньої.

4 версія стандартів ISO 9000 була видана у різні роки: у 2005 р. стандарт ISO 9000, у 2008 та 2009 р.р. – стандарти ISO 9001та 9004 відповідно.

5 версія стандартів, яка є актуальною на цей час, видана протягом трьох років:

ISO 9000:2015 (в Україні діє як ДСТУ ISO 9000:2015 [9]), ISO 9001:2015 (в Україні діє як ДСТУ ISO 9001:2015 [13]) та ISO 9004:2018 (в Україні діє як ДСТУ ISO 9004:2015 [14]).

Логічним доповненням міжнародних стандартів серії ISO 9000 є стандарт ISO 19011:2018 [15] (в Україні перебуває на стадії розроблення першої редакції, планується прийняти методом перекладу [16]), який містить настанови щодо здійснення аудитів систем управління, у тому числі, управління якістю.

Стандарт ДСТУ ISO 9000:2015 являє собою звід основних принципів та положень з управління якістю, а також словник термінів у сфері СУЯ.

Згідно з цим стандартом основними принципами менеджменту якості є:

1. Орієнтація на замовника.
2. Лідерство.
3. Залучення персоналу.
4. Процесний підхід.
5. Поліпшення.
6. Прийняття рішень на підставі фактів.
7. Управління взаємовідносинами [9].

Основні вимоги до структури та функціонування СУЯ організації викладені у стандарті ДСТУ ISO 9001:2015 [13]. Стандарт не встановлює вимог безпосередньо до продукції або послуг, його вимоги застосовуються під час сертифікації СУЯ організації, тому коротко зупинимося на основних з них.

По-перше, зауважимо, що структура стандарту ДСТУ ISO 9001:2015 містить 10 розділів і відповідає новому шаблону структури високого рівня (SL) для стандартів на системи управління. Мета створення такої єдиної структури – спрощення інтегрування різних систем управління в одну (наприклад, СУЯ за ISO 9001 та системи екологічного управління ISO 14001).

Наступна особливість [13] полягає у введенні у ньому поняття «середовище організації», тобто сукупність внутрішніх і зовнішніх факторів, що потенційно можуть впливати на діяльність організації щодо формування та досягнення своїх цілей. Введення цього поняття передбачає більш широкі рамки дії СУЯ. До

організацій висувається вимога стосовно врахування, моніторингу та аналізування будь-якої інформації щодо всіх факторів, які можуть впливати на СУЯ (наприклад, зовнішні фактори – ціни на ринку, політична ситуація тощо; внутрішні фактори – наявність обладнання, кваліфікованого персоналу тощо) під час планування, формування, упровадження та функціонування СУЯ. Крім того, організація має визначити усі зацікавлені у своїй діяльності сторони, визначити їхні потреби та вимоги, а також здійснювати постійний моніторинг та аналіз інформації щодо цих сторін та відповідних вимог.

Однією з найголовніших вимог ДСТУ ISO 9001:2015 до організації є вимога щодо застосування процесного підходу, який передбачає регулярне визначення процесів та взаємодій між ними, управління ними ними з метою досягнення запланованих результатів згідно з політикою та цілями щодо якості та стратегічним напрямком розвитку організації. Отже, усі види діяльності повинні розглядатися в організації як процеси – логічно упорядковані послідовності кроків (етапів), що перетворять входи у виходи (рис. 1.2) [13].

При цьому процесний підхід

Рис. 1.2. Схема процесу СУЯ згідно з ISO 9001:2015

При цьому процесний підхід спрямований він на виконання бізнес-процесів, а не на управління діяльністю певних функціональних підрозділів. Таке представлення процесів є подібним до представлення алгоритмів, що надає можливість застосування переваг інформаційних технологій для їх візуалізації та своєчасного одержання результатів з метою оперативного прийняття відповідних управлінських рішень.

З огляду на вищезазначене, стандарт вимагає, щоби організація визначила:

- необхідні для СУЯ процеси;
- порядок застосування цих процесів у рамках організації;
- потрібні входи і очікувані виходи цих процесів;
- послідовність і порядок взаємодії цих процесів;
- необхідні для цих процесів ресурси та заходи щодо забезпечення їх постійної наявності;
- необхідні для результативного функціювання та контролю цих процесів методи та критерії (моніторинг, вимірювання, показники дієвості тощо), порядок їхнього застосування.

Також організація має призначити відповідальних за ці процеси осіб з відповідними повноваженнями щодо оцінювання цих процесів та внесення до них будь-яких змін для забезпечування запланованих результатів, розгляду ризиків та можливостей, поліпшення цих процесів та СУЯ.

Стандарт [13] наголошує, що результативно управляти процесами та СУЯ вцілому можна з використанням управлінського циклу PDCA: PLAN – плануй; DO – виконуй; CHECK – перевіряй; ACT – дій (рис. 1.3).

Виділимо п’ять груп процесів, відображених у моделі СУЯ і пов’язаних із п’ятьма главами міжнародного стандарту ISO 9001 (рис. 1.3):

планування;

підтримання системи управління;

виробництво;

оцінювання дієвості;

поліпшення.

Можна побачити, що вони є взаємопов’язаними та «обертаються» за

принципом PDCA навколо лідерства, розуміючи під ним лідерство керівництва.

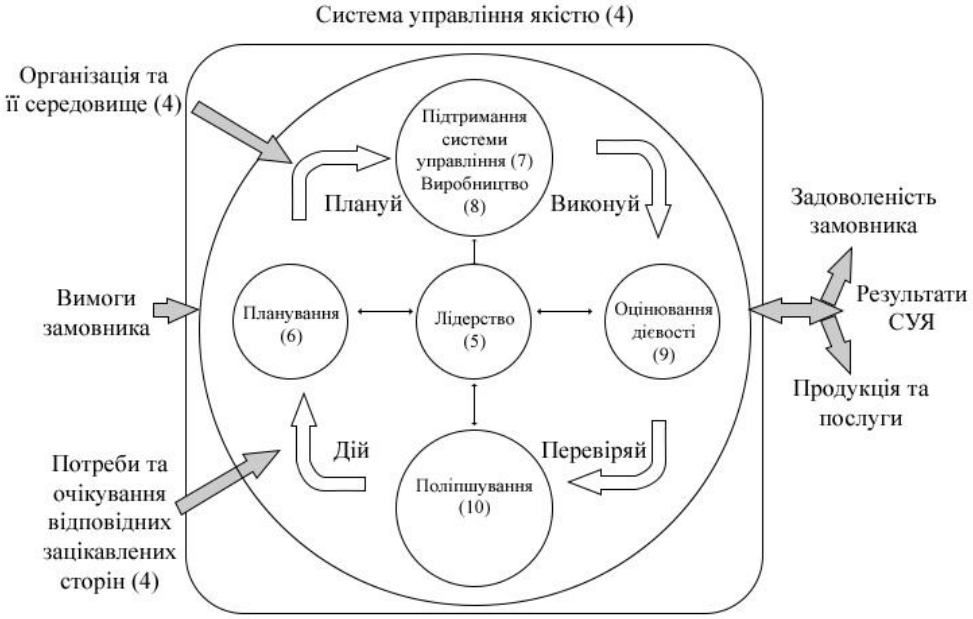

Рис. 1.3. Модель СУЯ з використанням управлінського циклу PDCA за стандартом ISO 9001:2015 [13]

Стандарт вимагає від вищого керівництва організації демонстрації свого лідерства та зобов'язань стосовно СУЯ шляхом накладання на себе відповідальності за її результативність, забезпечення формування політики та цілей щодо якості згідно з середовищем та стратегічним напрямком організації, забезпечення інтегрування до бізнес-процесів організації вимог СУЯ, сприяння застосуванню ризик-орієнтованого мислення і процесного підходу, забезпечення необхідними для СУЯ ресурсами, інформуання персоналу стосовно важливості відповідності вимогам СУЯ та результативного управління якістю, заохочення персоналу за внесок у результативність СУЯ, сприяня поліпшенню СУЯ, підтримання відповідних інших керівників стосовно питань управління якістю на їх управлінських рівнях.

Зовнішня «петля» моделі (рис. 1.3) ілюструє значення чіткого визначення середовища організації, ролі замовників та відповідних зацікавлених сторін. Зворотний зв'язок з останніми необхідний для виявлення їх вимог, потреб та очікувань, що стане вхідними даними для процесу оцінювання задоволеності замовника, результативності СУЯ та якості продукції та послуг, а також потенціалу для подальшого поліпшення СУЯ організації.

Важливою вимогою стандарту [13] є вимога щодо документування процесів

СУЯ, зокрема до задокументованої інформації (ЗІ), під якою розуміють власне інформацію (значущі дані), яку організація повинна постійно контролювати та забезпечувати її актуальність, а також носій, на якому її безпосередньо розміщено.

Незважаючи на відміну вимоги попередньої версії стандарту щодо обов'язкової наявності в організації Настанови з якості та шести задокументованих процедур СУЯ, у чинному стандарті в багатьох його пунктах є вимога стосовно підтвердження результатів певної діяльності тим чи іншим видом ЗІ (табл. 1.1).

Таблиця 1.1

Вимоги ДСТУ ISO 9001:2015 щодо задокументованої інформації організації

Пункт ДСТУ ISO 9001:2015	Найменування задокументованої інформації
1	2
4.3	Сфера застосування СУЯ
4.4.2	Політика у сфері якості
6.2.1	Цілі у сфері якості
7.1.5.1	Інформація, яка доводить, що ресурси для моніторингу та вимірювання відповідають їхній призначеності
7.1.5.2	Інформація про базу, використовувану для калібрування чи перевірення(якщо відсутні еталони, простежувні до міжнародних та національних еталонів)
7.1.6	Знання організації, які необхідні для функціонування процесів забезпечення відповідності продукції та послуг
7.2	Докази компетентності персоналу
7.5.3	Задокументована інформація зовнішнього походження, яку організація вважає необхідною для планування та функціювання системи управління якістю
8.2.3.2	Докази про: - результати аналізування; - будь-які нові вимоги до продукції та послуг.
8.2.4	Якщо вимоги до продукції та послуг змінено, організація повинна забезпечити внесення змін до відповідної задокументованої інформації та ознайомлення відповідного персоналу із зміненими вимогами.
8.3.2	Демонстрування задоволення вимог щодо проектування та розроблення.
8.3.3	Вхідні дані проектування та розроблення.
8.3.4	Інформація стосовно засобів контролю до процесу проектування та розроблення

Закінчення таблиці 1.1

1	2
8.3.5	Вихідні дані проектування та розроблення.
8.3.6	Інформація щодо: -змін у проекті та розробці; -результатів аналізування; -санкціювання змін; -дій, виконаних для запобігання несприятливим впливам.
8.4.1	Результати оцінювання, вибирання, моніторингу дієвості зовнішніх постачальників, а також їх повторного оцінювання, зважаючи на їхню здатність здійснювати процеси чи постачати продукцію й послуги відповідно до вимог.
8.4.3	Інформація для зовнішніх постачальників
8.5.1a)	Інформація, яка визначає: - характеристики продукції, яку виготовлятимуть, послуг, які надаватимуть, або робіт, які виконуватимуть; - результати, які отримуватимуть;
8.5.1j)	Докази затвердження та періодичного повторного затвердження здатності досягати запланованих результатів процесів виготовлення продукції та надання послуг у випадках, коли кінцевий вихід неможливо перевірити подальшим моніторингом або вимірюванням;
8.5.2	Інформація, необхідна для уможливлення простежуваності
8.5.3	Інформація про те, якщо власність замовника чи зовнішнього постачальника втрачено, пошкоджено чи внаслідок інших причин визнано непридатною для використання
8.5.5	Докази діяльності після постачання продукції
8.5.6	Інформація про результати аналізування змін, особу (осіб), яка(-і) санкціює(-ють) зміну, а також будь-які необхідні дії за результатами аналізування
8.6	Інформація про випуск продукції та послуг, яка має охоплювати: доказ відповідності критеріям приймання; простежуваність до особи (осіб), що санкціює(-ють) випуск.
8.7.2	Інформація, яка: описує невідповідність, виконані дії, будь-які одержані поступки; ідентифікує уповноважену особу, що приймає рішення про дію щодо невідповідності
9.1.1	Доказ оцінювання дієвості та результативності СУЯ
9.1.3	Організація повинна аналізувати та оцінювати відповідні дані та інформацію, отримані під час моніторингу та вимірювання.
9.2.2	Докази виконання програми аудиту та результатів аудиту
9.3.3	Результати аналізувань системи управління.
10.2.2	Докази щодо: характеру невідповідностей та будь-яких подальших виконаних дій; результатів будь-якої коригувальної дії.

Причому ЗІ може надаватися у будь-якому форматі, на будь-яких носіях, набходити з будь-якого джерела.

При створенні й актуалізації ЗІ організація має забезпечити відповідні ідентифікування, опис (назва, автор, дата актуалізації, номер тощо), формат (графічне зображення, яка мова, яке програмне забезпечення чи засіб), носії (електронний або паперовий), процеси аналізування та визначення придатності її та адекватності.

Щодо контролю ЗІ стандарт [13] вимагає від організації таких дій, як її сортування, доступ до неї, легкість пошуку та використання, постійний контроль змін, відповідне зберігання та вилучення.

ЗІ зовнішнього походження, яку необхідну для функціювання СУЯ організації, треба відповідно ідентифікувати та контролювати.

ЗІ, що зберігається у якості доказу відповідності, треба захищати від ненавмисної зміни.

Вимоги стосовно оцінювання дієвості СУЯ організації висуваються у 9 главі стандарту [13], де визначено, що підприємство повинно визначити таке: що треба моніторити та вимірювати; необхідні для забезпечення достовірних результатів методи моніторингу, вимірювання, аналізування та оцінювання; коли потрібно здійснювати моніторинг і вимірювання, а також коли потрібно аналізувати та оцінювати їх результати.

Організація має аналізувати та оцінювати дані моніторингу та вимірювання. Результати такого аналізу необхідно використовувати для оцінки:

- відповідності продукції (послуг);
- задоволеності замовника;
- дієвості та результативності СУЯ;
- результативності планування та дій щодо ризиків і можливостей;
- дієвості зовнішніх постачальників;
- потреби у поліпшенні СУЯ.

З метою оцінювання дієвості своєї СУЯ організація має проводити внутрішні аудити згідно із заздалегідь розробленими планами та програмами.

Нарешті, однією з найбільш суттєвих нових вимог стандарту [13] до СУЯ організації є використання ризик-орієнтованого мислення, яке допомагає цій

організації визначати фактори, що можуть призвести до відхилів у її процесах та СУЯ від запланованих результатів. Ризик-орієнтоване мислення також сприяє визначенню запобіжних заходів щодо зменшення негативних впливів і найефективнішому використанню можливостей, які виникають.

ISO 9000:2015 визначає ризик як вплив (позитивний чи негативний відхил від очікуваного) невизначеності [9].

Стандарт ISO 9001:2015 [13] вимагає від організації при плануванні в рамках її СУЯ виявлення ризиків та їх обробки для забезпення впевненості у можливості досягнення запланованих результатів функціонування СУЯ та її поліпшення. Також організація повинна планувати дії з обробки ризиків, інтегруючи ці дії в процеси СУЯ, а також оцінюючи їх результативність. Це надає організації можливість більш ефективно реалізовувати попереджувальні заходи та заходи із поліпшення її діяльності та підвищення конкурентоспроможності.

Для систематизації теоретичних та практичних напрацювань з питань організації управління ризиками міжнародною організацією стандартизації було розроблено серію стандартів ISO 31000, які набули розповсюдження у більшості провідних країн світу, зокрема, в Україні вони відомі як ДСТУ ISO 31000:2018 [36], IEC/ISO 31010:2019 [37] та ДСТУ ISO/TR 31004:2018 [38].

Стандарти ISO серії 31000 належним чином скорельовані зі стандартами ISO серії 9001, тому вони можуть служити методологічним і практичним базисом впровадження у діяльність будь-якої організації заходів щодо задоволення нагальної вимоги сьогодення – використання ризик-орієнтованого підходу для поліпшення результативності СУЯ та підприємства у цілому.

Окрім того, розробленням стандартів з управління ризиками займалися і займаються ряд міжнародних організацій, наприклад Комітетом спонсорських організацій комісії Тредвея (Committee of Sponsoring Organizations of the Treadway Commission, COSO), Федерації європейських асоціацій ризик-менеджерів (FERMA) тощо.

Зважаючи на важливість та значні потенційні можливості застосування менеджменту ризику для поліпшення функціонування СУЯ організацій з одного

боку, та недостатній рівень обізнаності керівників вітчизняних підприємств щодо методів і засобів управління ризиками, і, відповідно, недостатній рівень їх упровадження в Україні, актуальним є дослідження сучасних концепцій та методів управління ризиками з подальшим наданням на цій основі рекомендацій щодо їх практичної реалізації.

1.4 Висновки до першого розділу

У розділі проведено аналіз теоретичних основ управління якістю.

Визначені основні поняття у сфері управління якістю.

Проведено ретроспективний огляд підходів до управління якістю. Установлено, що натепер найбільш розповсюдженими є дієвими у цій сфері є підходи, запропоновані у п’ятій версії стандартів ISO серії 9000, які багато у чому співпадають з концепцією TQM.

Аналіз вимог стандарту ISO 9001:2015 до СУЯ організації показав, що однією з основних вимог, поруч із потребою у застосуванні процесного підходу, є необхідність упровадження ризик-орієнтованого підходу, імплементація якого потребує приймати рішення лише на основі результатів оцінювання ризиків.

Зважаючи на потенціні можливості застосування ризик-менеджменту для поліпшення функціонування СУЯ організацій з одного боку, та недостатній рівень обізнаності керівників вітчизняних підприємств щодо методів і засобів управління ризиками, і, відповідно, недостатній рівень їх упровадження в Україні, зроблено висновок про актуальність дослідження сучасних концепцій та методів управління ризиками з подальшим наданням на цій основі рекомендацій щодо їх практичної реалізації.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНИХ КОНЦЕПЦІЙ ТА МЕТОДІВ УПРАВЛІННЯ РИЗИКАМИ

2.1 Сутність поняття ризику та класифікація його видів

Питанням управління ризиками приділялося і приділяється багато уваги як за кордоном, так і в Україні. Існує достатньо солідний доробок теоретичних та практичних досліджень у цій галузі [20-31], зокрема таких фахівців, як Томас Л. Бартон, А. Маршал, Е. Холмс, Ф. Найт, Б. Райзберг, Т. Райс, П. Бернштайн, П. Верченко, М. Фрідмен, П. Шумпетер, А. Матвійчук, В. Буянов, А. Альгін, В. В. Вітлінський, О. М. Ястремська, Р.Ф. Філіна, О.О. Сосновська та ін. Не зважаючи на таку велику кількість публікацій, треба зазначити, що досі не існує однозначного підходу до визначення сутності поняття «ризик» та класифікації його видів. Тому доцільним є розгляд основних підходів до вирішення даної проблеми.

Необхідно зазначити, що з різноманітними ризиками та невизначеностями у своєму повсякденному житті людство почало стикатися ще на початковому етапі свого існування. Уже первісні люди інстинктивно повинні були обирати найбезпечніший варіант дій. Усвідомлювати ж існуючі ризики, аналізувати їх та розуміти необхідність здійснення певного роду дій для уникнення потенційних негативних наслідків цих ризиків людина змогла лише згодом, коли її розумові здібності почали розвиватися. Зважаючи на значний вплив на свідомість людства релігійних культур, на початковому етапі його розвитку людина відкидала можливість існування певних невизначеностей у своїй долі, а тим більше – можливості власного впливу на неї, вважаючі, що все визначається волею богів.

Однак, що вже тоді існувала гра в кості, яка у подальшому відіграта визначальну роль у становленні теорії ймовірностей, ставши однією з перших моделей для випадкових процесів.

Формування первісних понять щодо ризика та невизначеності відбувалося у давньогрецькій цивілізації, яка розвивалася під впливом місцевої міфології. Один із

давньогрецьких міфів показує світобудову у як гру в кості, коли три брати-боги розігрують між собою будову нашого світу: Зевс виграв собі небеса, Посейдон – море, а Аїд – підземний світ. Отже, можна побачити зародки перших уявлень щодо ймовірності та ризику і стверджувати, що етимологія терміну «ризик» має грецьке коріння і означає «небезпека маневрування поміж скель» [20].

На початковому етапі розвитку наукового напряму менеджменту ризиків, категорія «ризик» досліджувалася у рамках математики, статистики, логіки, деяких економічних та правових дисциплін, згодом – психології, дослідження операцій, теорії ймовірностей, управління, катастроф, прийняття рішень тощо. Приблизно з початку 60-х років минулого століття ризик стає об’єктом міждисциплінарного дослідження та отримує статус важливого загальнонаукового поняття.

Згідно з класичною теорією ризик є тотожним очікуваним у результаті того чи іншого обраного рішення втратам. Один із засновників теорії ризику Ф. Найт позиціонував ризик із ситуацією, результат якої є невизначеним, проте ймовірності можливих подій є відомими, причому він виокремлював три типи таких ймовірностей: апріорну (математичну), емпіричну (статистичну) і оцінки [32]. Ф. Найт розмежовував поняття «ризик» і «невизначеність», стверджуючи, що перше є інструментом зняття другого, тобто за допомогою ризику можна управляти джерелами невизначеності [32].

Webster's Dictionary of English Usage [33] визначає ризик як, з одного боку, небезпеку, можливість зазнати збитків або шкоди, тобто як ймовірність настання якої-небудь несприятливої події, а з іншого боку – як вартісне вираження наслідків несприятливих подій, які мають імовірнісний характер.

М. В. Боровик вважає [25], що ризик є потенційною можливістю виникнення керованої події в умовах невизначеності середовища здійснення економічної діяльності, яка піддається кількісній та якісній оцінці.

Згідно [34] ризик – це ймовірність, частота реалізації негативного впливу в зоні перебування людини.

Міжнародні стандарти з управління ризиками надають такі визначення поняття:

ризик – це ймовірність виникнення чогось, що буде мати вплив на цілі (AZ/NZS 4360:2004 [35]);

ризик – це комбінація ймовірності події та її наслідків (стандарт FERMA [36]);

ризик – це невизначеність щодо досягнення цілей, а його результатом може бути як негативне, так і позитивне відхилення від запланованої цілі (ДСТУ ISO Guide 73:2013 [37]);

ризик – це вплив невизначеності – стану нестачі навіть часткової інформації стосовно розуміння чи знання події, її наслідку чи ймовірності (ДСТУ ISO 9000:2015 [9]);

ризик – це вплив невизначеності на цілі. Ризик зазвичай визначається в термінах джерел ризику потенційних подій, наслідків цих подій та їх ймовірності (ДСТУ ISO 31000:2018 [17]).

Як можна побачити з наведених визначень, поняття ризику тісно пов’язане з таким поняттям як «невизначеність», під якою взагалі розіють неповноту (недостатню ясність) інформації щодо певної діяльності або її результатів, неповне знання щодо будь-чого. Невизначеність є притаманною будь-якій діяльності будь-якого суб’єкта та базується на неможливості точного та повного врахування всієї дотичної до нього інформаці.

Виникає невизначеність через наявність невизначених факторів, тобто обставин, умов, параметрів, явищ, які впливають на певний процес та його результат або на стан об’єкта.

Однією з головних причин невизначеності є випадковість багатьох явищ через їхню природу. Це – стохастична невизначеність [25].

Інші, невипадкові або нестохастичні за своєю суттю явища, є невизначеними через недостатню кількість інформації щодо них. Невизначеність, спричинена такими факторами – нестохастична невизначеність [25].

Фактори ризику умовно можна поділити на об’єктивні, які виникають без участі і незалежно від бажання організації, її персоналу, прийнятих управлінських рішень тощо (стан економіки, політична ситуація, науково-технічний прогрес, форс-мажорні обставини тощо) та суб’єктивні, створені завдяки впливу «людського

фактора» та певних суб'єктів господарювання.

Також фактори ризику класифікують на внутрішні та зовнішні.

Внутрішні фактори ризику безпосередньо визначаються діяльністю підпри ємства (організації). Існують такі види внутрішніх факторів ризику:

організаційні – залежать від прийнятої на підприємстві організаційної структури;

комерційні – залежать від організації маркетингу та реалізації, транспортування продукції та/або послуг підприємства;

пов'язані з впливом людського фактору – залежать від вищого верівництва та решьти персоналу підприємства;

управлінські – залежать від організації функціонування систем управління на підприємстві, у тому числі СУЯ;

виробничі – залежать від організації виробничого процесу на підприємстві;

фінансові – залежать від організації фінансової діяльності підприємства (банківські операції, купівля (продаж) цінних паперів, надання (отримання) кредитів тощо);

операційні – залежать від організації оновлення основних фондів, засобів виробництва, обладнання, навчання персоналу тощо.

Зовнішні фактори ризику впливають на виникнення на підприємстві ризиків безпосередньо чи опосередковано. Їх необхідно враховувати керівництву підприємства та управляти ними для мінімізації їхнього негативного впливу. Зовнішні фактори ризику пов'язані у цілому з політичною та економічною ситуацією у країні (регіоні), наприклад зміна курсу валют, наявність конфліктів на расовій або інших почвах, вплив процесів глобалізації, інвестиційна привабливість цієї країни, рівень інфляції, демографічні показники, законодавча та нормативно-правова база у галузі діяльності підприємства тощо.

З огляду на можливість запобігання фактори ризику бувають форс-мажорними або непереборної сили (природні катаклізми, війни тощр) та не форс-мажорними, впливу яких можлна запобігти певними діями.

За можливістю розпізнавання фактори ризику можна поділити на явні

(реально існуючі, передбачувані, які лежать на поверхні) та латентні (глибоко приховані, ретельно замасковані, такі, що важко підлягають виявленню).

Також варто зазначити, що один фактор ризику може спричинитиу появу та прояв кількох видів ризиків та навпаки – декілька факторів ризику можуть призвести до виникнення одного виду ризику. Саме тому необхідно розрізняти одиничні та інтегральні (комплексні) фактори ризику. Перші впливають тільки на один вид ризику, інші – одночасно на декілька видів ризику [38].

Поняття ризику також тісно пов’язано з поняттями «імовірність» та «значущість наслідків».

Імовірність прояву ризику – об’єктивно існуюча можливість прояву ризику, яка виражається числом від 0 до 1.

Значущість наслідків ризику – величина збитків (людських жертв, матеріальних, фінансових втрат тощо) яких зазнав об’єкт, стосовно якого ми розглідіємо ризик.

Ризики класифікують за великою кількістю ознак: ступенем імовірності виникнення, джерелом походження, видом діяльності, ступенем небезпечності наслідків реалізації, об’єктом (суб’єктом) впливу, можливостями управління ним тощо.

За джерелом виникнення ризики поділяють на зовнішні внутрішні.

За ступенем небезпеки для організації ризик поділяють на допустимий (втрата прибутку), критичний (поточні збитки) та катастрофічний (банкрутство).

З точки зору доцільності прийняття управлінського рішення розрізняють виправданий та невиправданий ризики.

За причинами виникнення ризики класифікують як: політичні ризики; організаційні ризики; технологічні ризики; технічні ризики; соціальні ризики; екологічні ризики; безпекові ризики; виробничі ризики; підприємницькі ризики; кадрові ризики; галузеві ризики; природні ризики; комерційні ризики; інфляційні ризики; інформаційні ризики; валютні ризики; інвестиційні ризики; корупційні ризики; кредитні ризики; іміджеві ризики.

За ступенем ризику (ймовірності настання втрат) він буває допустимий,

критичний. катастрофічний.

За часом виникнення ризики бувають:

давні – які мали місце у минулому, проте вчасно не були виявлені;

поточні – ризики, які виникають у поточний момент діяльності організації;

майбутні (потенційні) – прогнозовані ризики, що можуть з'явитися у перспективі.

Залежно від періоду існування бувають:

постійні ризики, які діють протягом усього часу існування об'єкта;

тимчасові ризики, які періодично виникають та існують протягом періоду, меншого за період існування об'єкта.

За частотою реалізації ризики бувають з низькою, середньою та з високою ймовірністю виникнення.

Об'єктами ризику можуть бути організація, система управління, в тому числі СУЯ, процеси, проекти, діяльність, персонал, продукція і послуги, безпека тощо.

2.2 Огляд стандартизованих концепцій управління ризиками

Розуміння того факту, що у сучасному економічному середовищі ефективність діяльності будь-якого підприємства та його конкурентоспроможність безпосередньо залежать від рівня реалізації ризиків, з якими воно стикається протягом свого існування, визначає необхідність використання науково-обґрунтованих підходів до їх мінімізації чи усунення. Очевидно, що цю проблему можна вирішити лише шляхом управління цими ризиками або ризик-менеджменту (РМ), який, згідно з ДСТУ ISO 31000:2018, являє собою скоординовані дії з управління організацією з урахуванням ризику [17].

Управління ризиками – складний безперервний процес, який включає в себе ряд етапів, протягом яких одночасно на регулярній основі здійснюється виявлення та ідентифікування ризиків, їх аналіз, вимірювання, пошук способів впливу на нього і оцінка ефективності прийнятих коригувальних заходів.

Для успішного та беззбиткового функціонування організацій будь-яких форм власності, розмірів та видів діяльності тощо на довгострокову перспективу потребує застосування системного підходу до менеджменту ризиків. Зарубіжна практика свідчить, що керівники компаній успішно використовують систему управління ризиками (СУР) як в окремих сегментах, так і в цілому. Згідно з опитуванням, проведеним Федерацією європейських асоціацій з ризик-менеджменту, 79% підприємств проводять картографування ризиків, при цьому 44% з них виокремили управління ризиками у підсистему менеджменту підприємства [31].

Система управління ризиками повинна стати складовою частиною системи управління організації, тобто інтегруватися до її політики, місії, цілей та планів роботи тощо. Зазначимо, що ризик безпосередньо пов'язаний із ефективністю функціонування СУЯ організації, адже, з одного боку, за ефективної роботи першої фактори ризику мають менший вплив на діяльність другої, а з іншого боку, якщо фактори ризику призводять до зниження конкурентоспроможності та дохідності організації, виникає необхідність у суттєвому коригуванні її СУЯ. Тому дослідження питань щодо управління ризиками в СУЯ організації насьогодні є вкрай актуальним.

Ключовим фактором успіху в управлінні ризиками СУЯ будь-якої організації є інтеграція механізмів та методів менеджменту ризиків у всі процеси, процедури та рівні цієї СУЯ. Нажаль, натепер під об'єктом ризик-менеджменту СУЯ часто розуміють лише якість продукції (послуг), що не відповідає концепції TQM, яка натомість враховує якість планування процесів в організації, якість її персоналу та також ряд інших важливих елементів СУЯ, які так само значно залежать від впливу факторів ризику та потребують постійного його контролю та управління.

На нашу думку, на сьогодняшньому етапі розвитку РМ найбільш ефективною формою його використання у розрізі управління якістю продукції (послуг) підприємства є інтеграція СУР і СУЯ, коли перша буде виступати додатковим дієвим інструментом, спрямованим на поліпшення результативності функціонування другої, що, у свою чергу, забезпечить:

підвищення якості виробленої продукції (наданих послуг) підприємства;

підвищення задоволеності клієнтів і споживачів;

підвищення ефективності роботи СУЯ шляхом зменшення кількості внутрішніх невідповідностей у функціонування її процесів.

Стрімкий розвиток теорії ризиків та формування різних концепцій РМ на початку 90-х років минулого століття зумовив активний розвиток процесів стандартизації у цій галузі. Почали виникати професійні національні та міжнародні стандарти з управління ризиками, причому кожний з них віддзеркалював певну концепцію ризик-менеджменту.

Стандартизації підлягали термінологія щодо управління ризиками, етапи (елементи) процесу ризик-менеджменту та підходи до побудови його алгоритму й оргструктури. Проте, не дивлячись на спробу уніфікації зазначених вище понять, у різних стандартах як термінологія, так і засадничі питання (цілі, принципи, алгоритм, елементи тощо) процесу управління ризиками відрізняються.

Розглянемо основні сучасні концептуальні положення РМ, викладені у найбільш відомих та розповсюджених стандартах з управління ризиком.

Спочатку розглянемо стандарти «Управління ризиками організацій. Інтегрована модель», розроблені Комітетом спонсорських організацій комісії Тредвея, США (Committee of Sponsoring Organizations of the Treadway Commission, COSO) [39-42].

Версія стандарту «COSO II» [41], розроблена Комітетом після спільного проекту з компанією «Price Water House Cooper» з розробки принципів РМ (Enterprise Risk Management (ERM) Integrated Framework), отримала у світовій практиці управління ризиками назву «Куб COSO» (рис. 2.1).

У стандарті викладені концептуальні засади РМ та надані рекомендації щодо створення СУР на підприємствах. Згідно з COSO, управління ризиками є безперервним та складається з 8 основних компонентів: 1. Визначення внутрішнього середовища. 2. Постановка цілей. 3. Визначення подій. 4. Оцінювання ризиків. 5. Реагування на ризики. 6. Засоби контролю. 7. Інформація та комунікація. 8. Моніторинг.

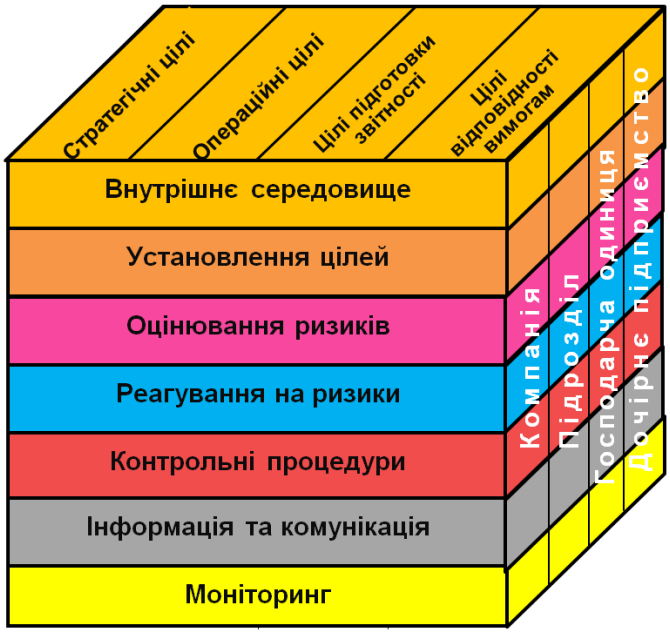

Рис. 2.1. Куб COSO 2004

Згідно із стандартом, процес управління ризиками є багатовекторним та циклічним, а всі компоненти мають вплив один на одного.

Основною метою стандарту проголошений баланс дохідності та ризику, а його основними завданнями є: визначення рівня ризику згідно з стратегією організації; поліпшення процесів прийняття рішень щодо реагування на ризики; мінімізація непередбачуваних ситуацій та збитків; управління усією сукупністю ризиків; використання усіх сприятливих можливостей; раціональне використання капіталу.

«Куб COSO» встановлює взаємний зв'язок між чотирма цілями підприємства (стратегічні та операційні цілі, цілі з підготовки звітності та з дотримання законодавства), вісьмома компонентами управління ризиками та оргструктурою підприємства (управлінські рівні компанії, підрозділу, господарської одиниці, дочірнього підприємства).

Актуальна версія стандарту COSO ERM 2017 зміщує акцент з процесів, компонентів та функцій ризик-менеджменту на його інтегрування в загальну систему стратегічного управління організацією (рис. 2.2) [40, 42].

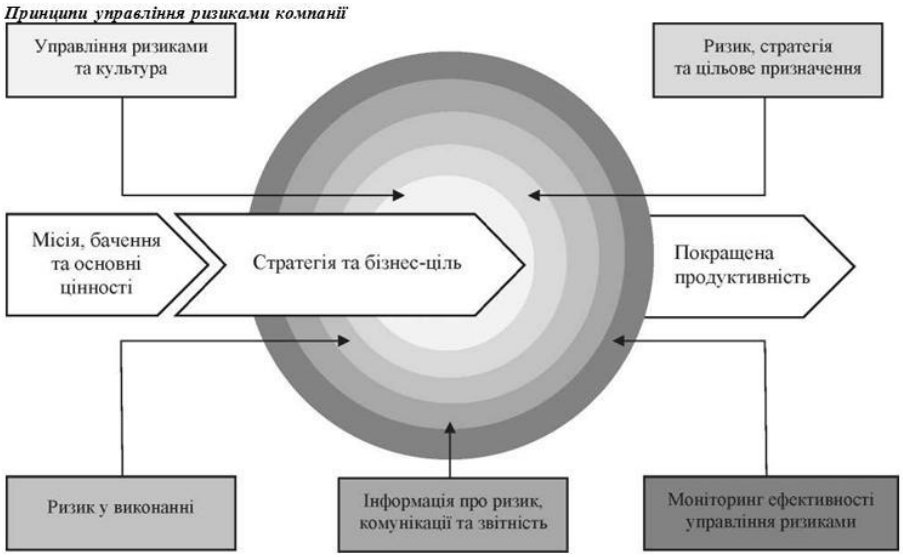

Рис. 2.2. Управління ризиками компанії згідно з COSO ERM 2017

Модель COSO ERM описує основні компоненти діяльності компанії: конкретизацію її місії, базових цінностей, місця в соціумі; розробку організаційної стратегії; встановлення бізнес-цілей в рамках обраної стратегії; реалізація обраної стратегії, виконання дій щодо досягнення поставлених цілей; покращення створення цінностей (продукції, послуг) [42].

Ефективній діяльності компанії повинні сприяти такі елементи системи ERM: управління ризиками та культура; розробка стратегії і встановлення цілей; виконання; моніторинг і вдосконалення; інформація, комунікація та звітність. Ці елемент системи ERM функціонують згідно з двадцятьма принципами [42]:

1. Рада директорів наглядає за управлінням ризиками.

2. Визначено та створено операційні структури.

3. Визначена бажана корпоративна культура.

4. Демонструється прихильність базовим цінностям.

5. Залучення кваліфікованих працівників, реалізація програм щодо їх розвитку та утримання.

6. Аналіз бізнес-контексту.

7. Визначення ризик-апетиту.

8. Оцінка альтернативних стратегій.

9. Визначення та формулювання бізнес-цілей.

10. Ідентифікація ризиків.

11. Оцінка ризиків.

12. Ранжування (приоритезація) ризиків.

13. Реалізація відповідної реакції на ризики.

14. Формування і оцінка комплексного портфелю ризиків.

15. Оцінка істотних змін.

16. Моніторинг ефективності функціонування організації і пов'язаних з цим ризиків.

17. Поліпшення системи управління ризиками.

18. Використання інформаційної системи для функціонування системи управління ризиками.

19. Інформування про ризики.

20. Звіти про ризики, корпоративну культуру та ефективність діяльності і для різних організаційних рівнів.

У лютому 2018 був опублікований спільний документ COSO і Всесвітньої ділової ради зі сталого розвитку (World Business Council for Sustainable Development, WBCSD) «Система управління ризиками. Застосування управління ризиками до соціальних, екологічних та управлінських ризиків» (Enterprise Risk Management. Applying enterprise risk management to environmental, social and governance-related risks) [43], у якому COSO розглядає особливості управління ризиками, пов'язані з головними цілями стійкого розвитку організації. У документі ці ризики визнвчені як екологічні, соціальні та управлінські ризики (Environmental, Social and Governance Related Risks, ESG-related risks).

На відміну від інших стандартів, виконання вимог стандарту COSO організаціями, акції яких обертаються на Нью-Йоркській фондовій біржі, є обов'язковоим [40].

Поряд із перевагами даного стандарту, він має ряд недоліків:

стандарт є достатньо об'ємним, а також складним для практичного застосування;

COSO лише поверхнево розглядає підходи до візуалізації та кількісного

оцінювання ризиків;

недостатньо чітко визначено заємозв'язок процесів менеджменту ризиків та створення вартості.

Ці недоліки змушують підприємства та організації використовувати при впровадженні ризик-менеджменту комбінацію COSO з іншими стандартами, наприклад FERMA або ISO 31000:2018.

Стандарт з управління ризиками Федерації європейських асоціацій ризик-менеджерів (Federation of European Risk Management Association – FERMA) є спільною розробкою британського інституту ризик-менеджменту (The Institute of Risk Management, IRM), Асоціації ризик-менеджменту та страхування (The Association of Insurance and Risk Management, AIRMIC) і Національного форуму з ризик-менеджменту у громадському секторі (The National Forum for Risk Management in the Public Sector, ALARM), прийнятою у 2002 році [40, 44].

FERMA створена у 1974 році і на сьогодні налічує 21 члена-національну асоціацію з 20 країн Європи [44].

Стандарт FERMA містить основні визначення, пояснює внутрішні та зовнішні фактори ризику, основні етапи процесу РМ (рис. 2.3), методологію оцінювання та аналізування ризиків, обов'язки ризик менеджера.

Згідно з документом існують чотири групи ризиків компанії: стратегічні, операційні, фінансові, а також ризики небезпеки.

В рамках характеристики етапів процесу РМ, викладено докладний опис вимог до інформації в звітах про ризики залежно від споживача цієї інформації (споживачі внутрішніх звітів – рада директорів організації, її структурний підрозділ та конкретний співробітник; зовнішніх звітів – зовнішні зацікавлені сторони організації). Так, звіт про ризики організації для зовнішніх користувачів інформації повинен включати опис:

методів внутрішнього контролю (зони відповідальності менеджменту організації щодо управління ризиками);

способів ідентифікації ризиків, їх практичного застосування в існуючій СУР організації

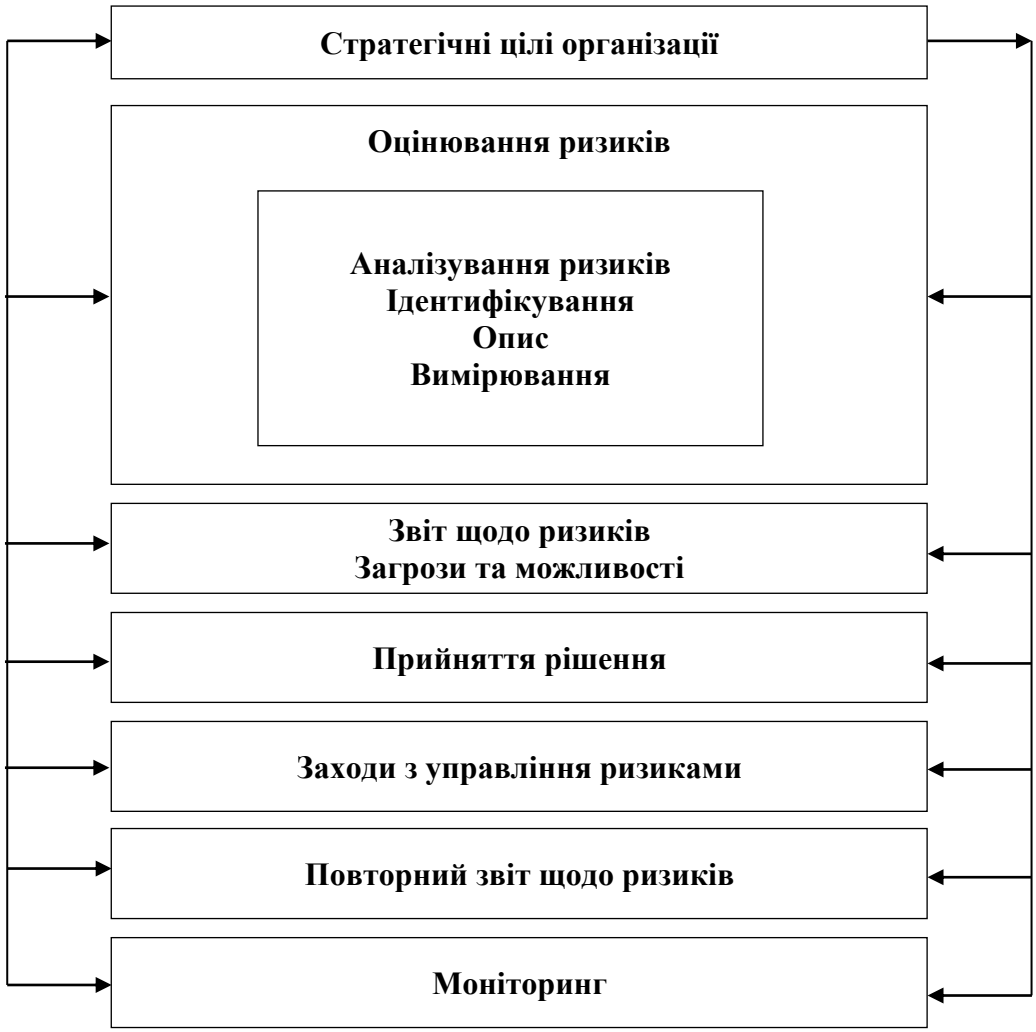

Рис. 2.3. Процес управління ризиками згідно з стандартом FERMA

інструментів системи внутрішнього контролю найнебезпечніших ризиків;

існуючих інструментів моніторингу ризиків.

Також стандарт визначає організаційну структуру управління ризиками (рада директорів – структурний підрозділ – РМ) та основні вимоги до нормативних документів щодо ризик-менеджменту на корпоративному рівні (Програма з управління ризиком організації).

Згідно з стандартом FERMA обов'язками ризик-менеджера компанії є розроблення програми управління ризиками, супровід її реалізації, координація співробітництва підрозділів організації, створення програм зі зменшення втрат і заходів з підтримки безперервності бізнес-процесів.

У додатку до стандарту наведено приклади використовуваних на практиці методів і технологій аналізу ризиків.

Стандарт FERMA призначений для штатних ризик-менеджерів (на відміну від COSO ERM, який спрямований на внутрішніх аудиторів). Виконання вимог стандарту не є обов'язковим, а використовувати його найбільш доцільно підприємствам та організаціям виробничої сфери [40].

Також існує ряд концепцій-стандартів різного рівня (національних, регіональних, міжнародних) з управління ризиками у певних сферах діяльності (галузях економіки).

Прикладом такого документу національного рівня щодо управління ризиками у сфері охорони навколишнього середовища є керівництво «Рамки для оцінки кумулятивних ризиків» (Framework for Cumulative Risk Assessment) [45], розроблений Управлінням з охорони довкілля США (U.S. Environmental Protection Agency (EPA або USEPA)). Він пропонує перехід на концепцію кумулятивного ризику (сукупного ризику від комбінації декількох часткових) та описує три основні фази оцінювання такого ризику: планування, визначення обсягу та постановка проблем; аналіз та характеристика ризиків.

Одним із приоритетних завдань EPA на 2018-2019 р.р. проголошено забезпечення виконання вимог Закону про контроль токсичних речовин щодо менеджменту ризику для 100 відсотків існуючих хімічних речовин, які використовуються на виробництві та у торгівлі [46].

Прикладом стандарту регіонального рівня у страхуванні був стандарт Solvency I, введений Директивами Європейського Союзу [40]. Він використовувався страховими компаніями країн ЄС до 2012 року та базувався на обліку страхового ризику при визначенні вимог до капіталу страхувальника, не враховуючи при цьому операційний, ринковий, кредитний ризики та їхню диверсифікаці. У 2012 році було видано стандарт платоспроможності операторів страхових ринків Solvency II [47], який підтримали Європейський комітет страхувальників (CEA) та Форум виконавчих ризик-менеджерів (CRO) [40]. Цей стандартI призначений для

мінімізації ризику невиконання вимог пенсійними фондами, а також страховими компаніями.

Прикладом стандартів з менеджменту ризику у банківській сфері є стандарти BASEL I, BASEL II та BASEL III, прийняті у 1998, 2004 та 2010 роках відповідно [40]. Документи, розроблені Базельським комітетом з банківського нагляду, визначають три види ризиків (кредитний, ринковий та операційний), критерії для регулювання діяльності фінансових установ. Основною метою стандартів Basel є підвищення стабільності та надійності світової банківської системи шляхом впровадження в процеси управління нею передових практик РМ стосовно побудови ефективної СУР банківської діяльності.

Велика кількість стандартів різного рівня існує щодо РМ в сфері інформаційної безпеки: ДСТУ ISO/IEC 27001:2015 [49], ДСТУ ISO/IEC 27005:2015 [50], BSI Standard 200-3: Risk Analysis based on IT Grundschutz Version 1.0 – британський стандарт від 2017 року, заснований на методиці базового захисту IT(IT-Grundschutz) від Федерального відомства з інформаційної безпеки Німеччини. [51], NIST 800-30 Guide for conducting risk assesments [52] – керівництво з оцінювання ризиків для IT-сфери, розроблене Лабораторією інформаційної технології (ITL) Національного інституту стандартів і технології (NIST) США.

Однак найбільш визнаними та широко вживаними у світі наразі є стандарти з ризик-менеджменту, розроблені міжнародною організацією стандартизації ISO одноосібно та у співпраці їз міжнародною електротехнічною комісією IEC.

Одним з них є стандарт ISO Guide 73:2009 [37], який узагальнив багаторічні теоретичні та практичні напрацювання фахівців у термінологічній сфері РМ.

Наступним етапом розвитку стандартизованих концепцій управління ризиками стало видання міжнародного стандарту ISO 31000, остання версія якого вийшла у 2018 р. є прийнята в Україні як ДСТУ ISO 31000:2018 [17]. У стандарті, який не є вузькоспеціалізованим або галузевим, викладені загальні рекомендації щодо управління будь-якими ризиками, з якими стикаються протягом усього життєвого циклу будь-які організації. Коротко розглянемо основні положення запропонованої стандартом концепції РМ.

Згідно із стандартом, РМ:

є частиною корпоративного управління і лідерства, значно впливає на управління організацією на всіх рівнях, сприяючи поліпшенню систем управління;

застосовується до всіх видів діяльності організації, включно із її взаємодією з стейкхолдерами;

розглядає фактори як зовнішнього, так і внутрішнього середовища організації, включно із поведінковими та культурними чинниками.

заснований на принципах, структурі та процесі (рис. 2.4), причому кожній організації ці компоненти необхідно адаптувати та постійно поліпшувати для підвищення результативності та ефективності РМ.

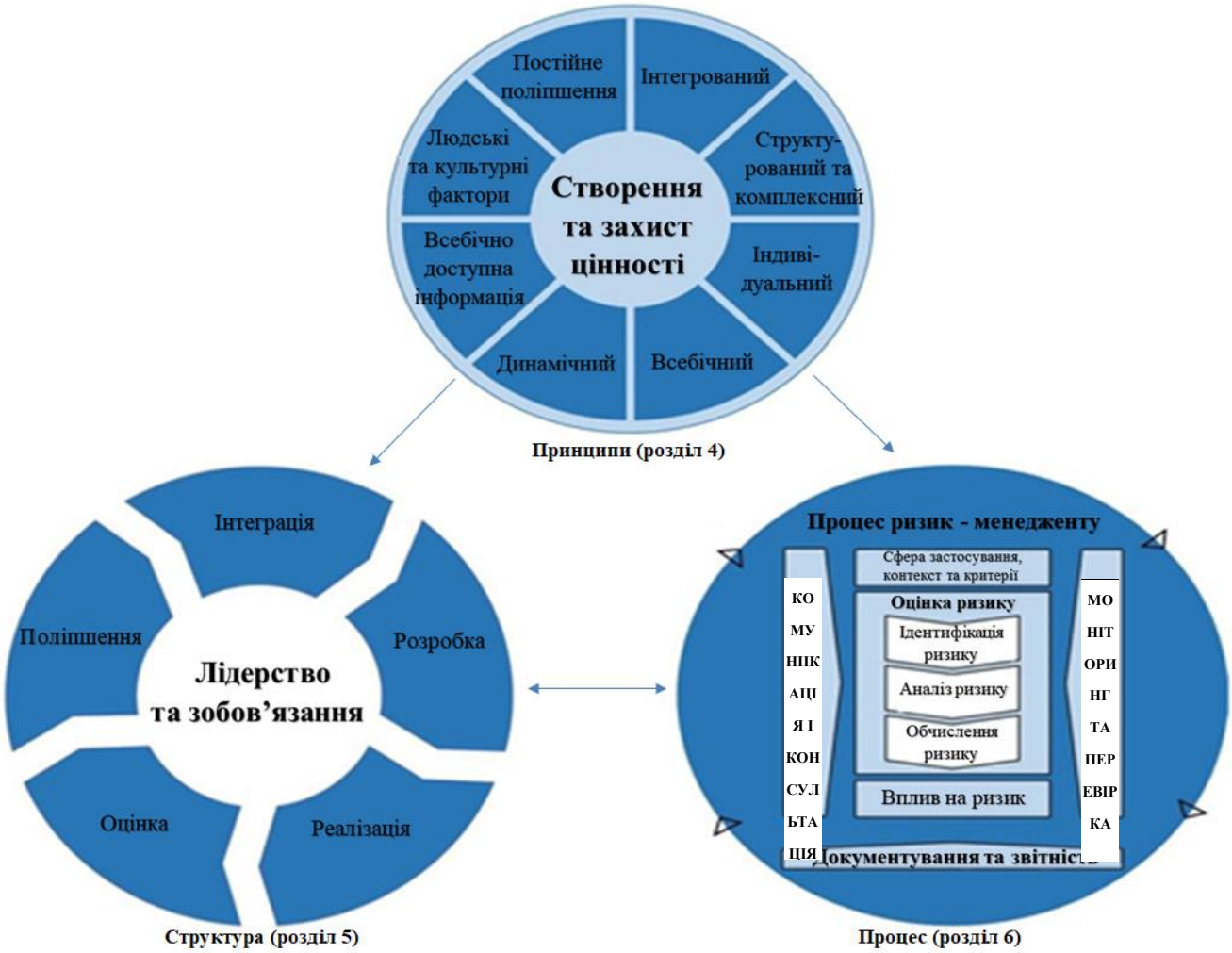

Рис. 2.4. Тріада «Принципи, структура та процес РМ» згідно із стандартом ISO 31000:2018

Принципи РМ (рис. 2.4), визначені у стандарті, встановлюють характеристики ефективного і результативного РМ і повинні враховуватися при формуванні структури і процесів РМ організації.

Принцип інтегрованого РМ означає, що він повинний бути нероздільною частиною діяльності організації.

Принцип структурованого та комплексного РМ сприяє отриманню узгоджених і придатних до порівняння результатів.

Принцип адаптованого РМ означає, що його структура і процес співвідносяться і корегуються відповідно до зовнішнього та внутрішнього середовищ підприємства, які пов'язані з його завданнями.

Принцип всебічного РМ означає, що своєчасне та розумне залучення стейкхолдерів дозволяє враховувати їх знання та думки, що призводить до підвищення обізнаності та обґрунтованості РМ.

Принцип динамічного РМ означає, що він відповідним чином і вчасно передбачає, виявляє, оцінює і реагує на ризики, які постійно виникають через зміни зовнішнього і внутрішнього середовища (зовнішнього і внутрішнього) організації.

Принцип всебічно доступної інформації означає, що РМ повинний враховувати будь-які обмеження і невизначеності щодо наявних даних (історичних та фактичних) та прогнозних очікувань, а вся інформація СУР має бути актуальною, чіткою, зрозумілою та доступною для всіх зацікавлених сторін

Принцип людських та культурних факторів зосереджує увагу на значному впливі людської поведінки та культури на всі аспекти та процеси кожного рівня й етапу РМ.

Принцип постійного поліпшення означає, що РМ повинен постійно вдосконалюватися шляхом навчанню та накопичення досвіду.

Структура РМ (рис. 2.4) повинна забезпечити його інтегрування в систему управління організацією (її підсистеми, наприклад, СУЯ), в усі функції та сфери її діяльності.

Формування структури полягає у, розробленні, впровадженні (інтегруванні), реалізації, оціннюванні та постійному поліпшуванні РМ в організації.

Компоненти структури і їх взаємодія повинні підпорядковуватися потребам організації.

Структура РМ базується на *лідерстві та зобов'язаннях* вищого керівництва і наглядових органів щодо інтегрування РМ у діяльність організації шляхом:

адаптації і впровадження всіх компонентів структури;

затвердження політики ризик-менеджменту;

виділенням необхідних для РМ ресурсів;

встановлення повноважень, відповідальності, підзвітності на різних рівнях організації.

Це допоможе узгодити РМ з цілями, стратегією та культурою організації; встановити тип і величину ризиків, розробити критерії ризику; інформувати всіх стейкхолдерів щодо цінностей РМ; стимулювати постійний моніторинг ризиків та привести структуру РМ у відповідність до контексту організації.

Компонент структури РМ *інтеграція* базується на правильному тлумаченні оргструктур і контексту. РМ повинен здійснюватися у всіх елементах структури організації та кожним її членом, стати органічною частиною цілей, стратегії, завдань організації, корпоративного управління, лідерства та відповідальності.

Компонент структури РМ *розробка* містить такі складові частини:

розуміння організації та її середовища (контексту);

демонстрація прихильності до управління ризиками;

визначення організаційних функцій, повноважень, відповідальності та підзвітності;

розподіл ресурсів;

встановлення механізмів обміну інформацією та консультування.

Компонент структури РМ *реалізація* передбачає:

розроблення плану РМ із зазначенням термінів і необхідних ресурсів;

визначення осіб, часу, місць, і способів прийняття рішень в організації;

визначення рамок (меж) корегування процесів прийняття рішень;

розуміння особливостей та коректного застосування механізмів РМ організації.

Компонент структури РМ *оцінка* визначає, необхідність періодичного оцінювання ефективності структури РМ з огляду на її мету, показники, плани реалізації, прогнозовані стани тощо, а також встановлення її спроможності продовжувати сприяти досягненню організацією споставлених цілей.

Компонент структури РМ *поліпшення* акцентує увагу на необхідності неперервного моніторингу та адаптації структури РМ для адекватного реагування на зовнішні і внутрішні зміни в середовищі організації, поліпшуючи таким чином показники її вартості. Наголошено, що організація має регулярно поліпшувати адекватність та ефективність структури РМ, удосконалювати методичні прийоми інтегрування РМ у свою діяльність. При виявленні будь-яких недоліків чи можливостей для поліпшення своєї діяльності, організація має розробляти відповідні плани з її корегування та контролювати їх виконання відповідальними посадовими особами.

Нарешті, **процес РМ** (рис. 2.4) передбачає постійне, цілеспрямоване та інтегроване застосування адекватних політик, процесів, процедур і практичних дій щодо управління ризиками з метою систематичного обміну інформацією та проведення консультування, визначення середовища (контексту) організації, а також оцінювання ризиків, впливу на них, моніторингу, аналізування, документування та ведення звітності щодо ризиків.

Обмін інформацією та консультування, які повинні відбуватися на всіх етапах процесу РМ, сприяють розумінню стейкхолдерами природі того чи іншого ризику, передумов прийняття відповідних рішень, причин необхідності певних дій. Якщо обмін інформацією підвищує обізнаність і розуміння ризику, то консультування забезпечує зворотній зв’язок та інформацію для прийняття обгрунтованих рішень.

Сфера застосування, контекст і критерії розуміють під собою визначення сфери охоплення процесу РМ, розуміння зовнішнього і внутрішнього середовища (контексту) організації з метою оптимізації процесу управління ризиками для ефективного оцінювання ризику та оперативного й адекватного впливу на нього.

Організація повинна визначити узгоджені зі структурою РМ та адаптовані

до відповідних цілей, своїх зобов'язань, поглядів стейкхолдерів та сфери охоплення певної діяльності критерії оцінки ризику для обгрунтування процесів прийняття того чи іншого рішення.

Внаслідок своєї динамічності критерії ризику повинні регулярно переглядатися та коригуватися.

Формуючи критерії ризику, необхідно враховувати характер і тип невизначеностей, які потенційно можуть вплинути на результати і цілі; метод визначання, вимірювання та імовірності появи позитивних і негативних наслідків; часовий фактор; ступінь узгодженості у застосуванні певних вимірювань; послідовність встановлення рівня ризику; потенціал організації.

Оцінювання ризику являє собою ітеративний комплексний процес, підпроцесами якого є ідентифікація, аналізування та обчислення (визначання) ризику.

Ідентифікація ризиків полягає в пошуку, визначенні та описі ризиків щодо досягнення цілей організації з використанням будь-якої придатної, відповідної й актуальної інформації. При ідентифікації ризиків потрібно враховувати джерела ризику (матеріальні та нематеріальні); загрози та можливості; причини та події; уразливість та спроможність; зміни зовнішнього і внутрішнього середовища; характер і цінність ресурсів тв активів; індикатори для ризиків, які виникають; вплив можливих наслідків на цілі; неповноту знань, в також достовірності наявної інформації; часові фактори; вплив людського фактору з боку залучених осіб.

Аналіз ризиків, необхідний для встановлення характеру та особливостей ризику, полягає у детальному розгляді невизначеностей, джерел ризику, наслідків, ймовірностей подій, можливих сценаріїв. Аналіз ризику виконується з різними ступенями складності та деталізації, а його методи можуть бути якісними, кількісними або комбінованими. При аналізі ризику потрібно враховувати імовірність подій та їх наслідків; характер і масштаб наслідків; складність і взаємообумовленість компонентів; часові фактори та волатильність; ефективність наявних засобів контролю; чутливість і достовірність обраних методів.

Обчислення ризику сприяє прийняттю рішень щодо визначення необхідності

прийняття додаткових дій та полягає у порівнянні результатів його аналізу із встановленими критеріями. За результатами аналізу ризику можуть прийматися такі варіанти рішень: додатково нічого не робити; розглянути можливі варіанти впливу на ризик; провести глибший аналіз для кращого зрозуміння ризику; переглянути існуючі цілі тощо.

Результати обчислення ризику обов'язково повинні задокументовуватися та доводитися до стейкхолдерів з наступним перевірянням на відповідних рівнях управління організації.

Вплив на ризик означає вибір та подальше застосування певного варіанту реагування на ризик. Цей ітеративний процес включає вибір одного або декількох із визначеної множини варіантів впливу на ризик; планування та безпосередній вплив на ризик; оцінку ефективності цього впливу; прийняття рішення щодо прийнятності рівня залишкового ризику; подальший вплив за умови неприйнятності останнього.

Можливі такі варіанти (або їх комбінації) впливу на ризик:

уникнення ризику шляхом ухвалення рішення щодо розпочинання або не продовження діяльності, яка і причиною цього ризик;

прийняття (збільшення) ризику для користання сприятливою можливістю;

усунення джерела ризику;

зміна наслідків реалізації ризику;

зміна імовірності настанні ризику;

поділ ризику з іншою стороною (сторонами), наприклад, через договори, страхування;

свідоме утримання ризику.

Обов'язковими елементами реалізації впливу на ризик повинні бути моніторинг та перевірка, адже неадекватний вплив на ризик може спричинити нові ризики.

Підготовка і реалізація планів впливу на ризик

Мета планів впливу на ризик полягає в тому, щоб визначити порядок реалізації обраних варіантів впливу, так, щоб заходи були зрозумілі учасниками цього процесу і була можливість контролювати прогрес по виконанню плану.

План впливу повинен чітко визначати порядок, відповідно до якого слід здійснювати вплив на ризик.

Плани впливу на ризик повинні бути інтегрованими до планів та процесів управління організації з урахуванням думок відповідних стейкхолдерів. План впливу повинний містити таку інформацію: обґрунтування варіантів впливу, із визначенням очікуваних вигод; визначення підзвітних і відповідальних за реалізацію плану осіб; власне дії, які пропонуються; необхідні ресурси; запропоновані показники ефективності; обмеження впливів; вимоги до моніторингу та звітності; терміни виконання запланованих дій.

Моніторинг та перевірка процесу РМ мають проводитися на всіх етапах процесу, бути його чітко спланованою частиною та містити такі елементи, як планування, збір, аналіз наявної інформації, документування отриманих результатів і організацію зворотного зв'язку.

Документування та звітність процесу РМ призначені для обміну інформацією про його заходи і результати; отримання інформації для прийняття обґрунтованих рішень; поліпшення діяльності з РМ; полегшення взаємодії із стейкхолдерами.

Створювати, зберігати та обробляти документовану інформацію з РМ потрібно з урахуванням її прогнозованого використання, ступеню конфіденційності інформації, контексту.

При звітуванні потрібно враховувати своєчасність, методи та цінність звітності; специфіку стейкхолдерів, особливості їх потреб в та вимог до інформації; її релевантність цілям організації та прийняттю своєчасних адекватних рішень.

Для більш детального роз'яснення базових концепцій ISO 31000 з рекомендаціями та прикладами, адаптованими до індивідуальних потреб користувачів у 2013 році ISO видала технічний звіт ISO/TR 31004:2013, прийнятий в Україні як ДСТУ ISO/TR 31004:2018 Менеджмент ризиків. Настанова з впровадження ISO 31000 [19].

Стосовно ж методів оцінювання ризиків які можуть застосовуватися у процесі РМ, ISO спільно з IEC видала стандарт IEC/ISO 31010, остання версія

якого – IEC/ISO 31010:2019 Керування ризиком. Методи загального оцінювання ризику [18] – вийшла у цьому році. Більш детально основні положення стандарту розглянемо нижче.

2.3 Методи оцінювання ризику

Оцінювання ризику як комплексний процес полягає в ідентифікації, аналізуванні та визначенні ризику. Оцінювання ризику включає порівняння рівня ризику, виявленого під час процесу аналізування із встановленими критеріями ризику під час розгляду ситуації (контексту), та є невід'ємною частиною оцінювання всієї діяльності організації та якості роботи підрозділів і окремих працівників.

З огляду на відсутність грунтовних досліджень щодо практичного застосування великої кількісті існуючих методів оцінювання ризику на різних етапах швидко набуваючого популярності РМ, у світі виникла нагальна потреба у створенні стандарту, у якому були б надані систематизований перелік таких методів з визначенням їхніх переваг та недоліків, а також рекомендації щодо їх вибору та застосуванню у різних ситуаціях.

У відповідь на цей виклик спільними зусиллями ISO та IEC був розроблений міжнародний стандарт ISO/IEC 31010, перша редакція якого вийшла в 2009 році як доповннення до стандарту ISO 31000.

Відповідно нової версії стандарту ISO 31000: 2018, у 2019 році вийшла більш сучасна версію ISO/IEC 31010:2019 [18], ключовми відмінностями якої від попередньої є:

кількість методів оцінювання ризику збільшено до 41. Зокрема, додані VaR, CVaR, S-Curve та ін.;

стандарт повністю узгоджений з ISO 31000: 2018;

на відміну від ISO/IEC 31010:2009, у якому методи були розділені на дві великі групи «Аналіз сценаріїв» і «Аналіз функціональності» та на ряд невеликих і допоміжних, в ISO/IEC 31010:2019 методи згруповані в 10 груп, пов’язаних з елементами процесу РМ;

у ISO/IEC 31010: 2019 зроблена нова спроба порівняння методів оцінки ризику

з використанням метрики з 8 характеристик.

Наглядне уявлення щодо розподілу в ISO/IEC 31010: 2019 методів оцінювання ризику за 10 групами відповідно до елементів процесу оцінювання ризику, визначеними в ISO 31000: 2018, можна отримати з рис. 2.5.

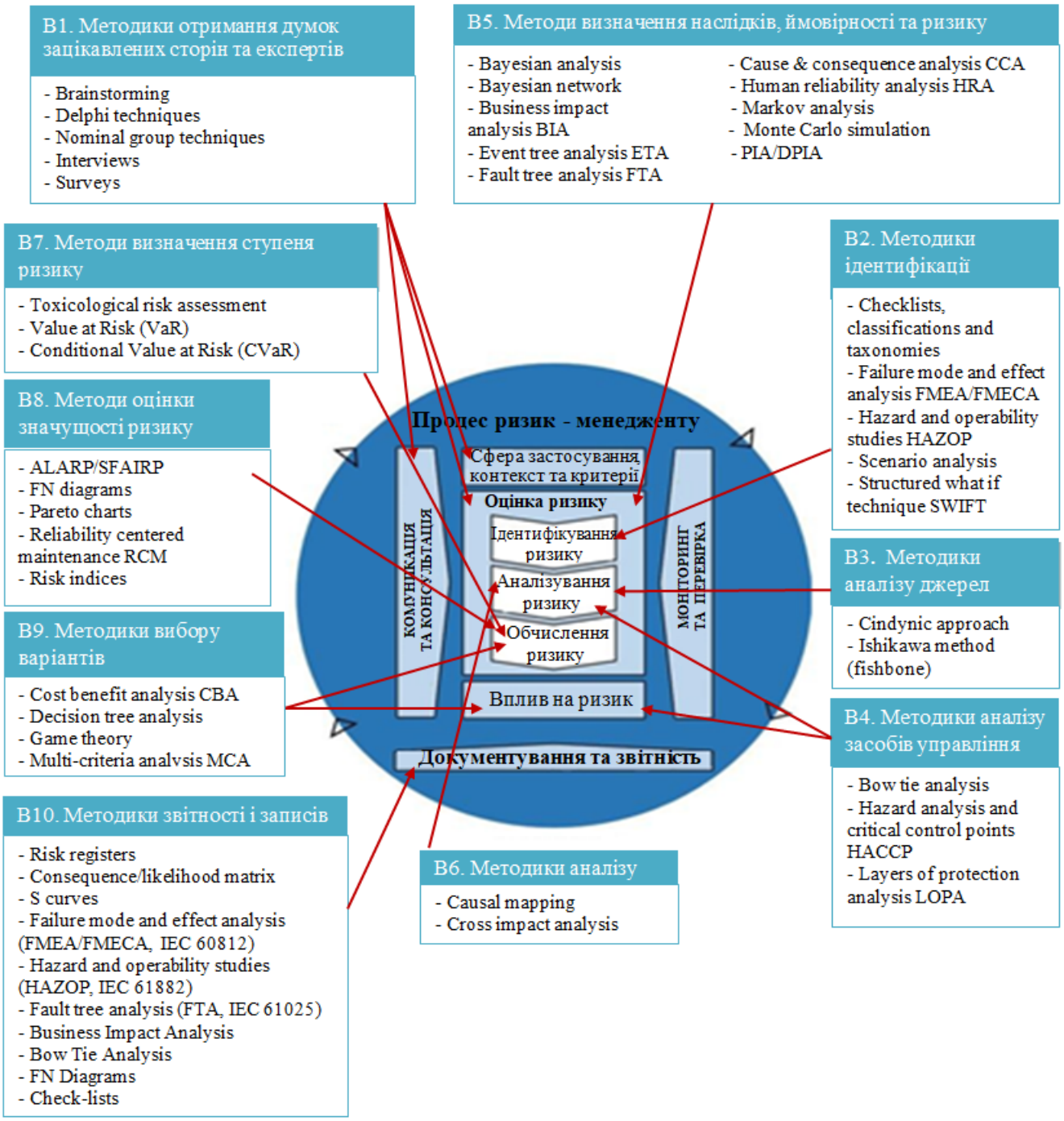

Рис. 2.5. Розподіл методів оцінювання ризику за 10 групами згідно з ISO/IEC 31010:2019 відповідно до елементів процесу оцінювання ризику, визначеними в ISO 31000: 2018

Згідно з ISO/IEC 31010:2019 методи оцінювання ризику розподіляються на групи:

отримання думок зацікавлених сторін та експертів;

ідентифікації;

аналізу джерел ризику;

аналізу засобів управління;

аналізу залежностей;

визначення ступеня ризику;

оцінки значущості ризику;

вибору варіантів;

звітності і записів;

визначення наслідків, ймовірності та ризику.

Для прикладу розгдянемо *метод Дельфі (метод експертних оцінок)*, етапами реалізації якого є:

формування команди з реалізації методу;

формування групи (груп) експертів (які на знають один одного);

разроблення анкети;

тестування анкети;

надсилання анонімних анкет кожному члену групи;

аналізування та узагальнення інформації за першим етапом та розсилання її членам групи для обговорення;

отримання відповідей членів групи, повторення процесу (за необхідності) до досягнення консенсусу.

Переваги методу:

зважаючи на анонімність суджень, більш імовірним є висловлювання непопулярних думок; усі думки є рівнозначними, що дає змогу уникати проблеми переважання думок окремих особистостей;

є право власності на результати;

немає потреби збирати учасників одночасно в одному місці.

Недоліки методу:

потреба у значних витратах часу та праці, а також; спроможності респондентів у чіткому письмовому викладаанні влвсних думок.

Аналогічно в ISO/IEC 31010:2019 розглянуті решта методів управління ризиками.

2.4 Висновки до другого розділу

У розділі проведено аналіз концепцій та методів управління ризиками.

Визначено сутність поняття ризику та проведено класифікацію його видів. Установлено, що існує багато трактувань поняття ризику, однак найбільш уживаним натепер є його визначення згідно із стандартом ISO/IEC 3100:2018, який визначає ризик як вплив невизначеності на цілі. При цьому ризик визначається в термінах джерел ризику потенційних подій, наслідків цих подій та їх ймовірності

Проведено огляд основних сучасних концепцій ризик-менеджменту, викладених у найбільш відомих та розповсюджених стандартах з управління ризиком: COSO ERM, FERMA, Solvency, BASEL, ISO 31000, ISO/IEC 31010. Визначено, що усі стандарти мають рамковий характер та не подають визначеного механізму побудови системи ризик-менеджменту на підприємстві, однак найбільш загальне уявлення про сутність ризик-менеджменту незалежно від цілей його використання, виду діяльності та організаційної форми господарювання надає стандарт ISO 31000, який визначає ризик-менеджмент як частину корпоративного управління і лідерства, яка значно впливає на управління організацією на всіх рівнях, а також встановлює та описує основні елементи основоположної тріади ризик-менеджменту – «принципи-структура-процеси».

Установлено, що найбільш грунтовною класифікацією методів оцінювання ризику є класифікація, викладена у стандарті ISO/IEC 31010:2019, у якому вони згруповані у 10 груп, пов’язаних з елементами процесу ризик-менеджменту та порівнюються з використанням метрики з 8 характеристик.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ РИЗИКАМИ В СИСТЕМАХ УПРАВЛІННЯ ЯКІСТЮ

3.1 Розроблення задокументованої процедури СУЯ «Управління ризиками»

На виконання вимоги ДСТУ ISO 9001:2015 [13] стосовно застосування в організації ризик-орієнтованого мислення та з урахуванням результатів проведеного аналізу підходів до управління ризиками, у роботі запропоновано проект задокументованої процедури (ЗП) СУЯ «Управління ризиками» для вищого навчального закладу (ВНЗ).

Документ складається з наступних розділів:

1 ПРИЗНАЧЕННЯ І ОБЛАСТЬ ЗАСТОСУВАННЯ

2 НОРМАТИВНІ ПОСИЛАННЯ

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ, ПОЗНАЧЕННЯ І СКОРОЧЕННЯ

4 ЗАГАЛЬНІ ПОЛОЖЕННЯ

5 ОПИС ПРОЦЕДУРИ

5.1 Опис процедури

5.1.1 Встановлення контексту

5.1.2 Ідентифікація ризиків і можливостей

5.1.3 Аналіз ризиків і можливостей

5.1.4 Оцінювання ризиків та можливостей

5.1.5 Обробка ризиків і можливостей

5.1.6 Моніторинг та перегляд

5.2 Схема послідовності виконання робіт

5.3 Повноваження і відповідальність

6 ЗАПИСИ

ДОДАТКИ

Нижче наведені найбільш важливі елементи документованої процедури.

4 ЗАГАЛЬНІ ПОЛОЖЕННЯ

4.1. Задокументована процедура (ЗП) призначена для інтегрування управління ризиками (УР) у СУЯ та загальну систему управління ВНЗ.

4.2. Для результативного УР ВНЗ на всіх рівнях слід відповідати наступним *принципам*:

УР створює і захищає цінність (сприяє наочному досягненню цілей і поліпшенню діяльності);

УР є невід'ємною частиною всіх процесів організації (не є відокремленою діяльністю від основної діяльності тапроцесів організації);

УР є частиною процесу прийняття рішень (допомагає особам, які приймають рішення, робити обґрунтований вибір, пріоритезувати дії та вибирати між альтернативними напрямами дії);

УР безпосередньо розглядає невизначеність;

УР є систематичним, структурованим і своєчасним;

УР грунтується на оптимально доступній інформації;

УР є адаптивним;

УР враховує людські та культурні чинники;

УР є прозорим;

УР є динамічним;

УР сприяє постійному поліпшенню закладу освіти.

4.3. ЗП «Управління ризиками» включає наступні *види діяльності*: встановлення контексту; ідентифікування ризиків і можливостей; аналізування ризиків і можливостей; оцінювання ризиків і можливостей; обробка ризиків і можливостей; моніторинг і перегляд.

4.4. *Об'єкти* процедури УР: політика, цілі ВНЗ; функціонування процесів СУЯ; діяльність структурних підрозділів (СП), відокремлених СП (ВСП) ВНЗ; документація СМЯ.

4.5. Для здійснення УР необхідні такі *ресурси*: персонал, його навички, досвід і компетенція; процеси, методи і інструменти, які будуть використовуватися для здійснення УР; документовані процеси та процедури; системи менеджменту

інформації та знань; програми навчання.

4.6. Процедура «Управління ризиками» представлена графічною блок- схемою в підрозділі 5.2 цієї ЗП.

4.7. Відповідальним за розробку і введення в дію даної ЗП є ректор ВНЗ.

5 ОПИС ПРОЦЕДУРИ

5.1 Опис процедури

5.1.1 Встановлення контексту

5.1.1.1. Метою встановлення контексту є визначення основних параметрів, урамках яких має відбуватися УР.

5.1.1.2. ВНЗ встановлює контекст, контекст процесу УР, а також визначає критерії ризику.

5.1.1.3. Контекст включає наступні *фактори зовнішнього середовища*: соціальне, культурне, політичне, юридичне, законодавче, фінансове, технологічне, економічне, природне і конкурентне середовище на різних рівнях; ключові рушійні фактори, тренди, що впливають на цілі ВНЗ; взаємини із зовнішніми зацікавленими сторонами, їх сприйняття та цінності.

5.1.1.4. Контекст включає наступні *фактори внутрішнього середовища*: керівництво, організаційне середовище, ролі та відповідальність; політики, цілі та стратегії; можливості, які сприймаються у вигляді ресурсів і знань; взаємини з внутрішніми зацікавленими сторонами, їх сприйняття і цінності; культуру ВНЗ; інформаційні системи та потоки; стандарти, керівні вказівки й моделі; форму та рамки контрактних взаємин.

5.1.1.5. *Контекст процесу* УР включає: визначення цілей УР; визначення відповідальності за УР; визначення області застосування УР; визначення діяльності, процесу тощо; визначення взаємозв'язків; визначення методології оцінювання ризиків; визначення способу оцінювання діяльності та результативності.

5.1.1.6. Встановлення контексту ВНЗ представлено на рис. 3.1.

5.1.1.7. Для оцінювання значущості ризику повинні бути встановлені критерії.

Рис. 3.1. Встановлення контексту ВНЗ

При цьому необхідно враховувати такі фактори: характер і типи причин і наслідків ризику, способи їх вимірювання; способи визначення імовірності виникнення; тимчасові рамки імовірності виникнення та наслідків; способи визначення рівня ризику; точки зору зацікавлених сторін; рівень, на якому ризик стає прийнятним або допустимим; чи слід враховувати комбінації ризиків.

5.1.2 Ідентифікація ризиків і можливостей

5.1.2.1. Метою ідентифікації є складання повного переліку ризиків і можливостей, які можуть вплинути на досягнення цілей ВНЗі його СП (ВСП).

5.1.2.2. Даний етап включає ідентифікацію джерела ризику, області дії, події, його причин і потенційних наслідків (якщо можливо, ідентифікація ризику може також розглянути можливість управління ризиком). При цьому необхідно отримати відповіді на питання: що може трапитися, коли, де, як і чому? Необхідно виявити вичерпний список джерел ризиків і можливостей, подій, які можуть мати вплив на досягнення кожної з цілей, ідентифікованих в контексті.

5.1.2.3. Відповідальність за ідентифікацію ризиків і можливостей на рівні СП (ВСП) несуть керівники відповідних СП (ВСП), на рівні процесів – власники відповідних процесів.

5.1.2.4. На етапі ідентифікації ризиків і можливостей здійснюють таке:

формують експертної групи з оцінки ризиків / можливостей в СП (ВСП) або на рівні процесу (заи необхідності);

складають переліку ризиків / можливостей в СП (ВСП) або на рівні процесу.

5.1.2.5. За необхідності формування експертної групи з оцінки ризиків / можливостей в СП (ВСП) (на рівні процесу) керівник відповідного СП (ВСП) (власник відповідного процесу) визначає загальну чисельність експертів в групі, вимоги до спеціалізації, кваліфікації і досвіду експертів, а також структуру експертної групи.

5.1.2.6. З метою проведення комплексного, всебічного експертного аналізу ризиків і можливостей, пов'язаних з функціонуванням СУЯ, при формуванні складу експертної групи щодо кожного експерта необхідно враховувати: професійний рівень; досвід наукової / практичної діяльності; наявність необхідних знань в області функціонування процесу; доступ до інформації про функціонування СУЯ; авторитет у колективі.

5.1.2.7. Для уникннення зниження точності та надійності експертних оцінок, до групи експертів слід включати не менше трьох осіб.

5.1.2.8. При роботі експертної групи можуть бути використані різні методи. Рекомендованим є один з наступних методів: опитування експертів; мозковий штурм; метод Делфі.

5.1.2.9. Мета опитування експертів – ідентифікація та оцінка ризиків шляхом інтерв'ю відповідних кваліфікованих фахівців, які висловлюють свою думку про ризики і дають їм оцінку, виходячи зі своїх знань, досвіду і наявної інформації. Даний метод допомагає уникнути повторення однієї і тієї ж помилки.

5.1.2.10. До участі у мозковому штурмі залучаються кваліфіковані фахівці, які заздалегідь готують свої судження по певній категорії ризиків. Спори і зауваження не допускаються, всі ризики записуються, групуються за типами і характеристиками, кожному ризику дається визначення. Мета – складання первинного переліку можливих ризиків для подальшого відбору і аналізу.

5.1.2.11. При застосуванні методу Делфі експерти беруть участь в опитуванні анонімно. Тому результат характеризується меншою суб'єктивністю, меншою

упередженістю і меншим впливом окремих експертів. Опитування експертів проводиться в кілька етапів. На кожному етапі модератор (провідний спеціаліст) розсилає анкети, збирає і обробляє відповіді (по аналогії з методом мозкового штурму). Результати опитування розсилаються експертам знову для уточнення їх думок і оцінок. Такий підхід дозволяє досягти якогось спільної думки фахівців про ризики.

5.1.2.12. Керівником СП (ВСП) або експертною групою складається перелік ризиків / можливостей процесів СУЯ в СП (ВСП) (табл. 3.1).

Таблиця 3.1

Перелік ризиків / можливостей процесів СУЯ в СП (ВСП)

Найменування ризику (негативний вплив на досягнення цілей СУЯ)	Найменування ризику (позитивний вплив на досягнення цілей СУЯ)
Найменування процесу СУЯ	

5.1.3 Аналізування ризиків і можливостей

5.1.3.1. Аналізування ризиків передбачає розгляд причин і джерел ризиків і можливостей, їх позитивних і негативних наслідків та імовірності того, що ці наслідки можуть виникнути.

5.1.3.2. Результатом етапу є достатньо детальне розуміння рівня ризику та його характеру для подальшого обробляння.

5.1.3.3. Аналізування ризиків надає вхідні дані для оцінювання ризиків і прийняття рішень щодо необхідності подальшого обробляння, а також для вибору найбільш доцільних стратегій і методів оообробляннн ризиків.

5.1.3.4. На етапі аналізування ризиків і можливостей керівником СП (ВСП) (власником процесу) або кожним експертом (при формуванні та залученні експертної групи до оцінки ризиків / можливостей) відповідно до розробленого переліку оцінюється імовірність виникнення кожного ризику / можливості, наслідки реалізації події та його рівень (як добуток імовірності та наслідків).

5.1.3.5. Оцінка імовірності ризиків / можливостей та їх наслідків здійснюється

з урахуванням класифікацій, наведених в таблицях 3.2 та 3.3.

Таблиця 3.2

Класифікація ризиків / можливостей за імовірністю виникнення

Імовірність виникнення ризика	Значеннння імовірності (*P*), бали	Опис
Мінімальна	1	Подія відбувається у виняткових випадках, практично неможливо припустити, що подібний фактор виникне
Помірна	2	Рідкісна подія, яка мала місце раніше, виникає в окремих випадках
Суттєва	3	Наявність свідчень, достатніх для припущення можливості події
Значна	4	Подія може відбутися. Умови для цього виникають досить регулярно і / або протягом певного інтервалу часу
Дуже висока	5	Подія, як очікується, відбудеться. Умови для цього обов'язково виникають протягом досить тривалого проміжку часу

Таблиця 3.3

Класифікація ризиків / можливостей за наслідками

Наслідки впливу ризика	Величина втрат (*U*), бали	Опис
Мінімальні	1	Відсутні будь-які значущі наслідки при реалізації ризику / можливості
Помірні	2	Наслідки від реалізації ризику / можливості незначні
Суттєві	3	Наслідки від реалізації ризику значні, але можуть бути повністю виправлені / Реалізація можливості матиме позитивний вплив на функціонування окремих напрямків діяльності ВНЗ
Значні	4	Наслідки від реалізації ризику значні, але можуть бути виправлені лише до певної міри / Реалізація можливості матиме позитивний вплив на функціонування ВНЗ в цілому
Дуже високі	5	Важко відновитися від наслідків, пов'язаних з даним ризиком / У разі реалізації ВНЗ зможе вийти на лідируючі позиції на ринку освітніх послуг

5.1.3.6. Рівень ризику / можливості визначається за формулою:

$$R = P \cdot U, \qquad (3.1)$$

де R – рівень ризику / можливості;

P – значення імовірності виникнення ризику / можливості, бал;

U – величина втрат (наслідки впливу) ризику / можливості, бал.

5.1.3.7. Думки експертів узагальнюються, оцінка рівня ризиків / можливостей в СП (ВСП) або на рівні процесу представляється у вигляді табл. 3.4.

Таблиця 3.4

Класифікація ризиків / можливостей за рівнем

Найменування ризика/можливості	Імовірнвсть, P	Наслідки, U	Рівень, R
Найменування процесу СУЯ			
Ризики			
Можливості			

5.1.4 Оцінювання ризиків та можливостей

5.1.4.1. Метою оцінювання ризиків і можливостей є сприяння прийняттю рішень, заснованих на вихідних даних аналізу ризиків і можливостей, щодо необхідності їх обробляння та встановлення пріоритету для обробляння.

5.1.4.2. Оцінювання ризиків та можливостей включає порівняння рівня, виявленого в процесі аналізу, до критеріїв, встановлених при розгляді контексту. На підставі цього приймається до уваги необхідність обробляння ризику і можливості.

5.1.4.3. На етапі оцінювання ризиків і можливостей здійснюють такі дії:

оцінювання рівня ризиків / можливостей і складання паспорта ризиків СП (ВСП);

складання паспорта ризиків процесу СУЯ;

складання паспорта ризиків СУЯ.

5.1.4.4. Керівник СП (ВСП) або експертна група оцінює прийнятність рівня ризиків в СП (ВСП). Оцінювання прийнятності проводиться з урахуванням ризикової стратегії ВНЗ, що відбиває його готовність йти на ризик.

5.1.4.5. У разі якщо рівень ризику перевищує встановлений рівень прийнятності, то в його відношенні повинні бути реалізовані заходи, спрямовані на зниження ризиків до прийнятного рівня. Необхідно максимально знизити можливість настання негативного результату і звести до мінімуму можливі втрати, пов’язані з його реалізацією.

5.1.4.6. Відносно прийнятних ризиків заходи з управлінського впливу не розпочинаються (табл. 3.5).

Таблиця 3.5

Управлінські впливи залежно від виду ризику

Вид ризику	Рівень ризику	Необхідність обробляння ризику
Низький	R_i<6	Прийнятний рівень ризику. Заходи з впливу на ризик не виконують
Помірний	6≤ R_i ≥10	Неприйнятний рівень ризику. За необхідності розробляють заходи з УР, спрямовані на зниження рівня ризику до прийнятного. Рішення про доцільність розроблення відповідних заходів залежно від рівня управління даним ризиком приймає ректор, проректор, власник процесу, керівник СП (ВСП). УР зводиться до загального спостереження та контролю за ризиком. Зниження впливу наслідків проводиться шляхом прийняття оперативних управлінських рішень з урахуванням наявних матеріально-технічних і кадрових ресурсів
Суттєвий	R_i >10	Неприйнятний рівень ризику. Розробляють заходи з УР, спрямовані на зниження рівня ризику до прийнятного. Ризик вимагає постійного моніторингу, аналізу та оцінки з боку керівництва

5.1.4.7. Якщо рівень можливості досить високий, повинні бути реалізовані заходи, спрямовані на реалізацію даної можливості. Відносно можливостей з низьким рівнем заходи з управлінського впливу не розпочинаються (табл. 3.6).

Таблиця 3.6

Управлінські впливи залежно від виду можливості

Вид можливості	Рівень можливості	Необхідність обробляння
Низька	R_i<6	Недостатній рівень можливості. Заходи з впливу на можливість не роблять
Помірна	6≤ R_i ≥10	Значний рівень можливості. За необхідності розробляють заходи щодо поліпшення для реалізації наданої можливості. Рішення про доцільність розроблення відповідних заходів залежно від рівня управління даною можливістю приймає ректор, проректор, власник процесу, керівник СП (ВСП). Реалізація можливостей даного рівня здійснюється шляхом прийняття оперативних управлінських рішень з урахуванням наявних матеріально-технічних і кадрових ресурсів
Суттєва	R_i >10	Значний рівень можливості. Розробляють заходи щодо поліпшення для реалізації наданої можливості. Реалізація можливості знаходиться під контролем керівництва

5.1.4.8. Найбільш значущі ризики і можливості (помірні та суттєві) розглядають детально, відомості про ці ризики і можливості документують у

паспорті ризиків СП (ВСП) (додаток А). Паспорт ризиків розглядають на засіданнях (нарадах) СП (ВСП) і затверджують керівники відповідних СП (ВСП). Інформація про ризики / можливості СП (ВСП) передається власникам процесів для подальшого аналізування.

5.1.4.9. Власники процесів аналізують і узагальнюють інформацію про ризики / можливості СП (ВСП) в рамках своїх підшефних процесів. За результатами аналізу розробляється паспорт ризиків процесу СУЯ (додаток Б). Інформація про ризики / можливості процесів СУЯ передається до сектору управління якістю і моніторингу освіти навчально-методичного відділу (СУЯіМО) для узагальнення.

5.1.4.10. СУЯіМ спільно з проректором з навчальної роботи узагальнюють дані про ризики / можливості процесів СУЯ і розробляють паспорт ризиків СУЯ (додаток В).

5.1.5 Обробляння ризиків і можливостей

5.1.5.1. Обробляння передбачає вибір одного або декількох варіантів зміни ризиків і можливостей і впровадження цих варіантів.

5.1.5.2. Після впровадження варіантів зміни ризиків і можливостей обробляння забезпечує або модифікує засоби управління.

5.1.5.3. Обробляння передбачає циклічний процес, що складається з: проведення оцінки обробляння; прийняття рішення про те, чи є залишкові рівні допустимими; ініціалізація нового обробляння, якщо залишкові рівні неприпустимі; проведення оцінки результативності обробляння.

5.1.5.4. На етапі обробляння ризиків і можливостей здійснюються такі дії: постановка цілей в області якості; розробка планів заходів щодо управління ризиками; розробка планів заходів щодо поліпшення.

5.1.5.5. На основі виявлених ризиків і можливостей здійснюється постановка цілей в області якості СП (ВСП) (додаток Г), цілей в області якості процесів і СУЯ ВНЗ (додаток Д).

5.1.5.6. Заходи з управління ризиками розробляються з метою зниження ступеня впливу ризику або зниження його ймовірності.

5.1.5.7. Заходи з управління ризиками можуть бути спрямовані: на усунення

джерел ризику; на ослаблення впливу джерел ризику; мінімізацію (зміна) наслідків ризику; локалізацію (обмеження) наслідків ризику; комбінацію вище викладеного.

5.1.5.8. Заходи з управління ризиками розробляють на рівні СП (ВСП) (додаток Е), процесів СУЯ, СУЯ ВНЗ в цілому (додаток Є).

5.1.5.9. У графі «Найменування заходу з управління ризиком» (додатки Е, Є, Ж) формулювання заходу повинно чітко і ясно відображати спосіб впливу на ризик. Не допускається загальних формулювань, які нечітко відображають суть дій з управління ризиком. Захід може носити як регулярний, так і разовий характер.

5.1.5.10. У графі «Відповідальний виконавець» (додатки Е, Є, Ж) вказується особа і СП, відповідальні за виконання заходу. У разі, якщо в заході бере участь кілька СП, першим вказується СП, відповідальний за виконання. Вона повинна бути визначеною в обов'язковому порядку, інші вказуються як учасники. За неможливості чіткого визначення одного відповідального, захід має бути розбитий на кілька залежно від кількості зон відповідальності при виконанні заходу.

5.1.5.11. Термін виконання заходу встановлюється виходячи з можливостей і завантаженості СП, які беруть у ньому участь, а також ступеня терміновості питання, що вирішується.

5.1.5.12. Відповідають за розроблення і виконання заходів з управління ризиками та подальший їх моніторинг на рівні СП (ВСП) керівники відповідних СП (ВСП), на рівні процесів – власники відповідних процесів. За необхідності виконання заходів з мінімізації даного ризику СП (ВСП), які не перебувають в зоні відповідальності власника процесу, такий захід узгоджується з СП (ВСП), потенційно відповідального за виконання даного заходу.

5.1.5.13. Для кожного ризику необхідно вибрати стратегію або комбінацію з різних стратегій, яка видається найбільш ефективною для роботи з ним. Існують три типових стратегії реагування на появу загроз, здатних вплинути на досягнення цілей СУЯ: ухилення; передавання; зниження.

5.1.5.14. Ухилення від ризику передбачає зміну плану діяльності таким чином, щоби виключити загрозу, викликану негативним ризиком, захистити цілі СУЯ від наслідків ризику або послабити цілі, які знаходяться під загрозою.

5.1.5.15. Передавання ризику має на увазі перекладення негативних наслідків загрози з відповідальністю за реагування на ризик на третю сторону. Передавання ризику просто переносить відповідальність за його управління іншій стороні; ризик при цьому не усувається. Передавання відповідальності за ризик є найбільш ефективною у відношенні фінансових ризиків.

5.1.5.16. Зниження ризиків передбачає зниження імовірності та / або наслідків негативної ризикованої події до прийнятних меж.

5.1.5.17. Відносно позитивних ризиків розробляються план заходів щодо поліпшення СП (ВСП) (додаток З); план заходів щодо поліпшення процесу СУЯ (додаток И); план заходів щодо поліпшення СУЯ (додаток І).

5.1.5.18. Для кожного позитивного ризику необхідно вибрати стратегію або комбінацію з різних стратегій, яка видається найбільш ефективною для роботи з ним. Існують три типових стратегії реагування на позитивні ризики: використання; спільне використання; посилення.

5.1.5.19. Стратегія використання може бути обрана для реагування на ризиків з позитивним впливом, якщо необхідно, щоби дана сприятлива можливість гарантовано була б реалізована. Дана стратегія призначена для усунення всіх невизначеностей, пов'язаних з ризиком за допомогою засобів, що забезпечують появу даної слушної нагоди в різних формах. Заходами прямого реагування на дану можливість є залучення до участі в роботі більш талановитого персоналу з тим, щоб скоротити час, необхідний для його завершення, або забезпечення більш високої якості, ніж було передбачено початковим планом.

5.1.5.20. Спільне використання позитивні ризиків передбачає передавання відповідальності третьій стороні, здатній щонайкраще скористатися наданою сприятливою можливістю, а також організація спільної діяльності з третьою стороною.

5.1.5.21. При застосуванні стратегії посилення змінюється рівень слушної нагоди шляхом підвищення імовірності виникнення та / або позитивного впливу, а також шляхом виявлення і максимізації основних джерел цих позитивних ризиків. Для цього можна спробувати полегшити або зміцнити причину, що викликає

сприятливу можливість, і цілеспрямовано підсилити умови її появи.

5.1.6 Моніторинг та перегляд

5.1.6.1. Після затвердження заходів з управління ризиками і планів поліпшень керівники СП (ВСП) і власники процесів здійснюють контроль за виконанням заходів відповідно до термінів виконання кожного заходу.

5.1.6.2. У графі «Відмітка про виконання, документи, що підтверджують» планів заходів вказують дату фактичного виконання заходу. У коментарях наводять посилання на документи, підтверджуючі факт виконання заходів, розкриття причин, за якими захід не виконується, виконується в повному обсязі або терміни виконання заходу перенесені. В якості документів можуть бути вказані акти про виконані роботи та здачі до експлуатації, положення, посадові інструкції та інші внутрішні нормативні документи, висновки експертизи.

5.1.6.3. Моніторинг ризиків / можливостей здійснюється:

в ході операційної діяльності СП (ВСП) (за необхідності відбивається в протоколах засідань СП (ВСП), протоколах засідань колегіальних органів в іншій документації);

при проведенні внутрішніх аудитів (відбивається в планах і звітах по внутрішнім аудитів); при проведенні аналізу функціонування процесів в СП (ВСП)

при проведенні аналізу СУЯ з боку керівництва.

5.1.6.4. Регулярно, не рідше одного разу на рік, здійснюється актуалізація інформації про ризики та можливості та їх оцінки шляхом внесення відповідних змін до паспорта ризику. Власники процесів організують збір, аналіз, уточнення, систематизацію та ранжування інформації про ризики / можливості з обов’язковим моніторингом виконання заходів з управління найбільш важливими ризиками / можливостями.

5.1.6.5. Оцінювання результативності виконання заходів з управління ризиками та заходів щодо реалізації можливостей здійснюється власниками процесів і керівниками СП (ВСП) шляхом підтвердження факту виконання заходів і факту зниження ризику. Показники результативності процесу «Управління ризиками» для окремого підрозділу і університету в цілому наведені у табл. 3.7.

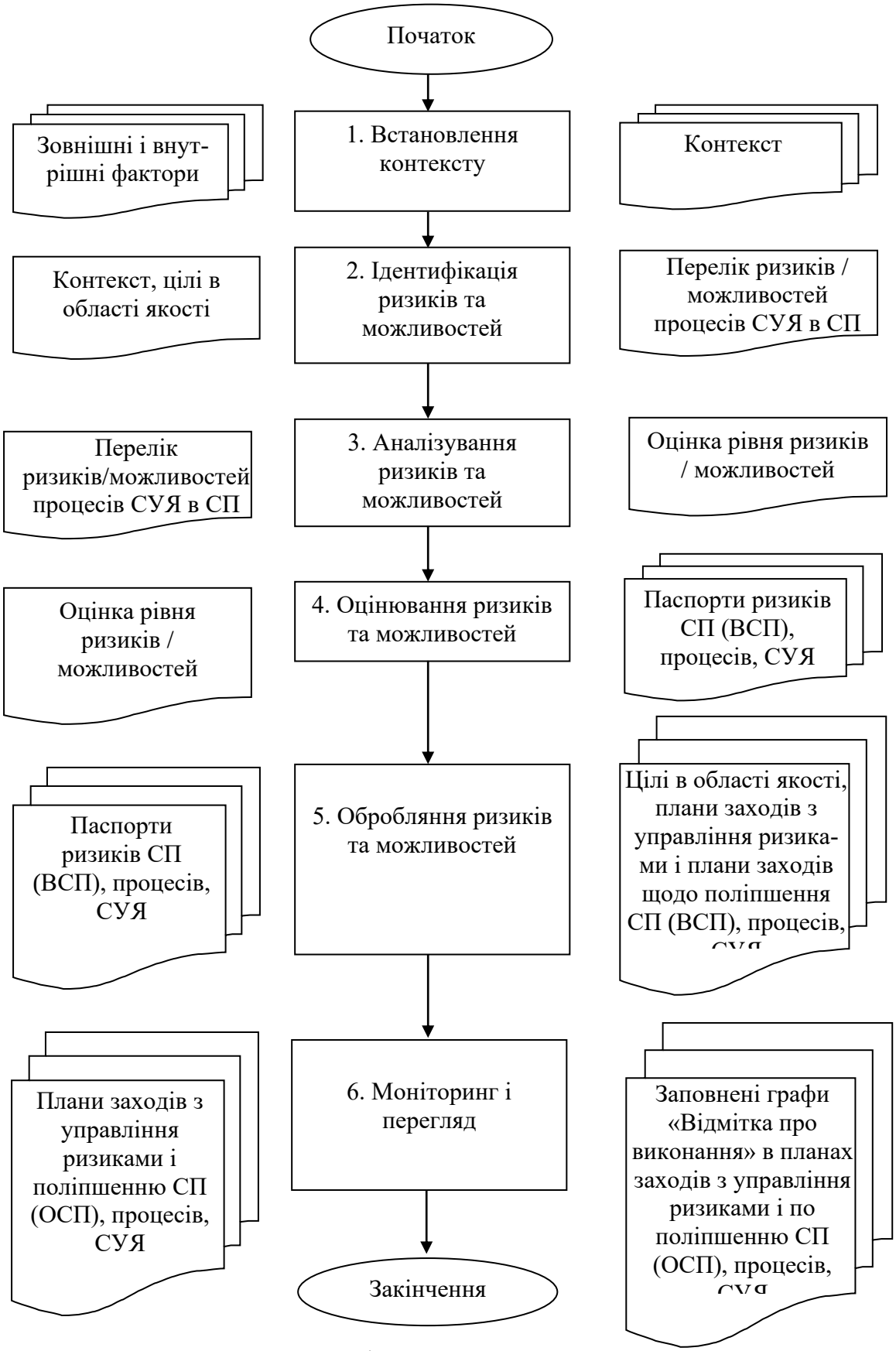

Рис. 3.2. Алгоритм управління ризиками

Таблиця 3.7

Показники результативності процесу «Управління ризиками»

Керівники підрозділів/ процесів	Показники результативності процесу	Одиниця вимірю-вання	Критерії результативності	Значення показника	
				Мину-лий рік	Звітний рвк
Керівники підрозділів	Реалізація плану заходів щодо усунення ризиків	%	Не менше 80%		
Вчена рада	Рішення Вченої ради про результативність процесу	Рішення	Процес результативний / нерезультативний		
Вчена рада	Рішення Вченої ради щодо стратегічних змін у діяльності Університету, що містять вимоги до подальших заходів з усунення ризиків	Рішення	Рішення принято / не прйнято		

5.3 Повноваження і відповідальність

5.3.1 Власником даної процедури є ректор.

5.3.2 Відповідальність у рамках даної процедури і розподіл повноважень представлені в табл. 3.8.

Таблиця 3.8

Матриця розподілу відповідальності і повноважень

Вид діяльності	Посадова особа				
	Ректор	Власник процесу	Керівник СП (ВСП)	Експертна група (за потреби)	СУЯіМО
Встановлення контексту	К	О, В	О		
Ідентифікація ризиків і можливостей	К	О	О, В	В	
Аналізування ризиків і можливостей	К	О	О, В	В	
Оцінювання ризиків та можливостей	К	О	О, В	В	
Обробляння ризиків і можливостей	К	О	О, В	В	В
Моніторинг та перегляд	К	О, В	В		В

К – контролює, О – організовує, В – виконує

6 ЗАПИСИ

6.1 Переліки записів, що реєструються в підрозділах, їх форми, відповідальність за реєстрацію, місце і терміни зберігання наведені у відповідних документах СУЯ.

3.2 Урахування людського фактора в управлінні ризиком

Людський фактор (ЛФ) є одним із головних чинників виникнення або уникнення інцидентів, а також джерелом зростання невизначеності у процесі прийняття управлінських рішень. Саме тому результати аналізування ЛФ мають систематично переглядатися у рамках процесу управління ризиком та у прямому зв'язку з виникненням інцидентів за одночасного виявлення їх причин та формування впливів на них.

Обов'язкове врахування ЛФ в оцінці ризиків надаватиме адекватне розуміння ролі людини у виконанні виробничих завдань, імовірності виникнення небажаних подій тощо. При цьому потрібно використовувати технології, які включають аспект ЛФ, наприклад анкети; спостереження; співбесіди (опитування); оцінювання людської надійності (HRA) моделювання; когнітивний наскрізний аналіз (CWT); когнітивний аналіз завдання (CTA); експертне оцінювання тощо.

Без застосування технологій, що ґрунтуються на ЛФ, а також без врахування аспектів ЛФ, на будь-якому кроці процесу управління ризиком існує велика імовірність неналежної реалізації найважливіших елементів. За умови неврахування елементу ЛФ, потенційно можна отримати невірний результат при оцінюванні ризику через незрозумілість першопричин.

Для кращого розуміння загальної концепції ЛФ та її складових у соціально-технологічній системі можна застосувати модель Septigon [53] (рис. 3.3), яка може використовуватися як контрольна форма для визначення небезпек і описує сім головних аспектів, які мають бути розглянуті, а також взаємодію між будь-якими з елементів. Septigon означає поєднання перших літер слів, використаних у моделі: Суспільство і Культура (Society and Culture), Фізичне Середовище (Physical Environment), Практика (Practice), Технологія (Technology), Окремі особи (Individual), Група (Group) та Мережа організаційного середовища (Organizational Environment Network). Слово «Septigon» (в перекладі з англійської – «семикутник») відображає форму самої моделі.

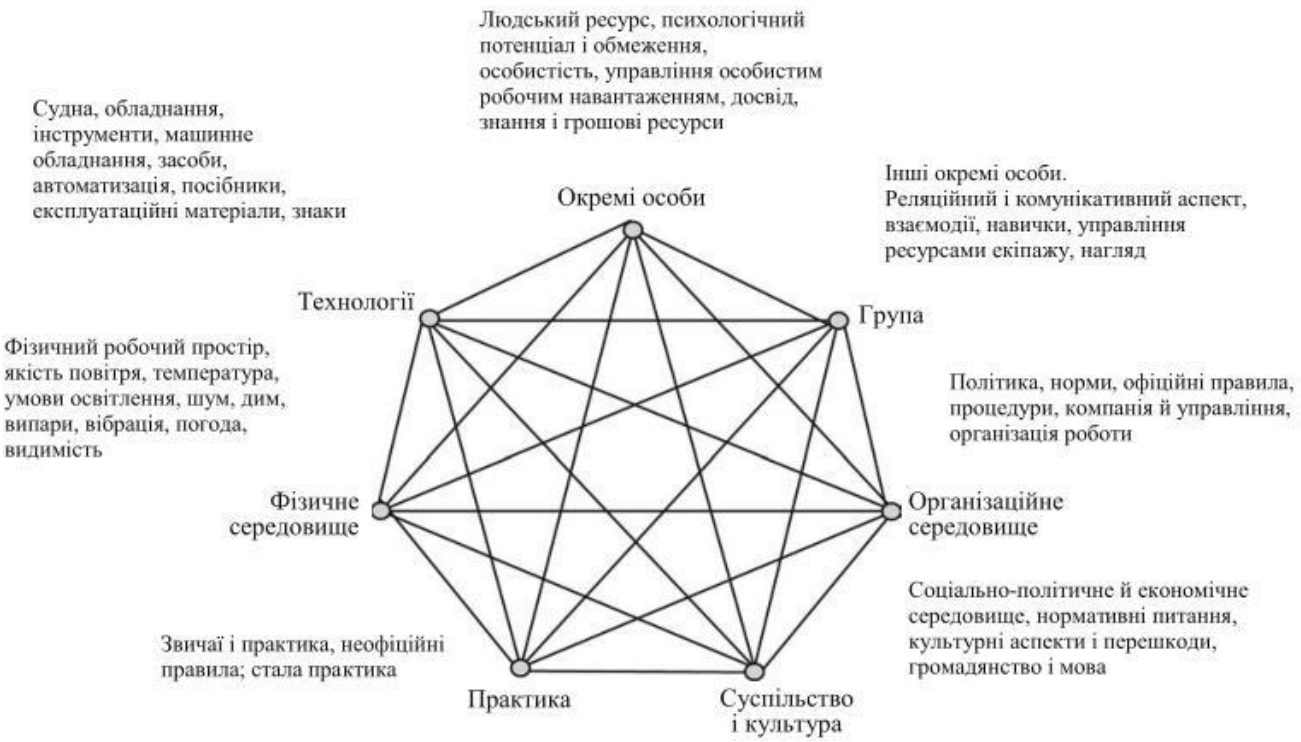

Рис. 3.3. Модель Septigon

Основними елементами ЛФ у теорії управління ризиками вважають (рис. 3.4) [54]:

ставлення до ризику – індивідуальне та колективне відношення до ризику та ступінь ефективності прийнятих рішень з управління ризиком;

Рис. 3.4. Основні елементи людського фактора в управлінні ризиками [54]

сприйняття ризику – здатність адекватно сприймати або чітко усвідомлювати всі небезпеки та ризики;

аналіз ризику – здатність адекватно оцінювати ризик, зважуючи ймовірність виникнення інциденту та можливі наслідки;

компетентність з ризику – здатність грамотно дотримуватися прийнятої практики управління ризиками та адекватно реагувати на ризики.

За даними [54] через помилки людини кількість аварій у небезпечних сферах діяльності за останні тридцять років зросла з 20 до 80%, що спричинено із діяльністю людини не лише при експлуатації, а й при проектуванні, виготовленні та обслуговуванні техніки.

Через недоврахування психологічних, антропометричних, психофізіологічних тощо властивостей людини-оператора в конструкції систем управління відбувається близько 30-40 % усіх помилок внаслідок ЛФ в авіації, більше 60 % транспортних пригод із важкими наслідками, більше 50 % аварій в енергосистемах [55].

Очевидно, що при дослідженні ЛФ потрібно аналізувати взаємодію індивідуальних, робочих та організаційних факторів, які мають значний вплив на продуктивність людини, на її здатність безпомилково виконувати завдання професійної діяльності.

Для проактивного управління потенційно небезпечною помилкою людини-оператора, цей процес потрібно розглядати як частину процесу оцінки ризику, де необхідно виявляти [55,56]:

значні потенційні помилки людини;

чинники, які впливають на імовірність їх виникнення (недоліки у організації робочого місця з погляду ергономіки, відволікання уваги, надмірне робоче навантаження, брак компетентності, робоче середовище, моральний стан у колективі тощо).

чинники, що впливають на продуктивність праці;

заходи з контролю, які дозволяють своєчасно виявити помилку людини-оператора.

Розуміння першопричин виникнення помилок та різних чинників, які

збільшують імовірність їх виникнення або знижують можливість їх виявлення, допомагають розробці більш ефективних засобів контролю.

Розрізняють два типи проявів ЛФ у процесі прийняття рішень чи виконанні дій: помилки і порушення [57].

Помилка – це ненавмисна дія (бездіяльність) або рішення, що є відхиленням від правильного алгоритму.

Порушення – це навмисне відхилення від правила або процедури.

Помилки або промахи є незапланованими, тобто ненавмисними діями, які виникають при виконанні звичних завдань. Цей тип помилок, як правило, виникає у технологічних процесах із високим рівнем автоматизації, коли людині-оператору не потрібно постійно концентруватися на виконанні управлінських дій. Помилки такого роду зазвичай не можуть усуватися шляхом проведення навчання персоналу, проте ергономічно удосконалений дизайн може частково зменшити їх імовірність і забезпечити більшу стійкість людини до помилок.

Інший тип помилок – помилки судження або прийняття рішення, коли людина-оператор неправильно діє, вважаючи, що це правильно. Це, як правило, притаманно ситуаціям, коли людина або не знає, як правильно виконати певне завдання, або воно є новим чи несподіваним, або людині просто бракує необхідних знань чи компетентності. У таких випадках людина-оператор часто намагається пригадати аналогічну ситуацію та відповідний алгоритм дій, що може не відповідати обставинам ситуації, що склалася. Навчання, засноване на правильних процедурах, є основним шляхом уникннення таких помилок.

Порушення відрізняються від помилок тим, що вони є навмисними.

Існують різні класифікації порушень. Наприклад, згідно з класифікацією [56], існують:

рутинні порушення, які є незначними та звичними для працівників;

ситуаційні порушення, які допускають працівники під впливом певної виробничої ситуації, яка склалася;

виняткові порушення, викликані необхідністю діяти у виняткових, як правило, екстремальних обставинах;

порушення під час намагання оптимізувати робочий процес;

саботаж або навмисні злочинні порушення.

Автори [3] поділяють причини помилкових дій на безпосередні та віддалені.

До безпосередніх причин відносять [55]:

невідповідності психологічним можливостям перероблення інформації (неоптимальний потік інформації, порушення в розрізненні сигналів, мала тощо);

недоліки умінь або навичок (їх невідповідність ситуації, помилки перемикання тощо);

недоліки уваги (надмірна або недостатня концентрація, неправильна структура і послідовність перемикання, порушення стійкості тощо).

Віддалені причини помилок пов'язують з [55]:

недоліками системи управління і робочого місця (розподіл і узгодження функцій між фахівцем і технічним пристроєм; способи роботи; компонування робочого місця, чисельності працівників у робочому приміщенні, психологічного клімату в групі);

недостатньою підготовкою до виконання завдання;

станом організму;

психологічною установкою оператора;

організацією праці та відпочинку;

психічним станом оператора (емоційна напруженість тощо).

Незалежно від причини та виду помилок та порушень, вони здатні призвести до аварії чи травмування працівників, а тому потребують своєчасної ідентифікації та впровадження відповідних управлінських рішень.

За узагальненими даними матеріалів щодо розслідувань виробничих нещасних випадків і аварій [58], можна сформувати чотири групи причин проявів ЛФ:

не вміє – працівник не має необхідних для конкретної роботи знаннь, не опанував потрібних навичок, методів, способів, прийомів;

не хоче – працівник уміє якісно виконувати певну роботу, протеу нього немає бажання дотримуватися вимог безпеки, інакше кажучи, немає внутрішньої мотивації, не розвинена психологічна установка на дотримання цих вимог;

не може – працівник перебуває в такому фізичному або психологічному стані, що, незважаючи на уміння, навички та бажання, допускає небезпечні дії;

не забезпечений – працівник не виконує запропоновану дію через незабезпечення його необхідними умовами та ресурсами (інструментом, приладами, матеріалами, інформацією тощо).

Перші три групи причин зумовлені індивідуальними особистісними характеристиками робітника.

Четверта група є зовнішнім по відношенню до працівника чинником, що формується завдяки параметрам виробничого середовища, де відбуваєтьсядіяльність працівника.

Безпечні умови праці – умови, за яких вплив на робітників з боку шкідливих та/або небезпечних виробничих факторів виключено, або рівні їх впливу не перевищують встановлених нормативів. Це визначення не виключає наявності на робочому місці потенційно небезпечних факторів і не містить будь-яких додаткових вимог до робітника.

Проте подібних умов, щоб попередити нещасний випадок (аварію), недостатньо. По-перше, через ряд причин сам працівник може виконати небезпечну дію, в результаті якої відбудеться нещасний випадок або аварія. По-друге, потенційна небезпека виробництва за певних умов може трансформуватися в реальну, коли створюється небезпечна або аварійна ситуація, яка потребує від працівника адекватних дій (поведінки). По-третє, можливі ситуації, коли тяжкі наслідки настають не через вплив небезпечного фактора, не через необачну поведінку працівника, а через його стан, наприклад, на ідеальному з огляду на безпеку робочому місці у працівника через сильні переживання (які мали місце до початку або протягом робочого дня) стався серцевий напад, він втратив свідомість, впав і отримав черепно-мозкову травму.

Очевидно, що безпечні умови праці є необхідними, але недостатніми для безпечної праці, адже багато залежить від поведінки, кваліфікації, фізичного і психологічного тощо стану самого працівника.

Отже, безпечну працю можна визначити як діяльність, за якої дотримуються

безпечні умови праці, працівник як при виконанні звичайних робочих операцій, так і при виникненні небезпечних ситуацій діє адекватно і безпечно, а його фізичний і психолгічний стан відповідає нормі.

За такого підходу сукупність необхідних і достатніх умов для забезпечення безпеки конкретного працівника можна представити у вигляді суми інтегральних показників:

Вміє = Володіє професійними знаннями + Володіє відповідною професією (посадою, виконуваної роботи) навичками, методами, прийомами, способами.

Хоче = Вироблена психологічна установка на виконання вимог безпеки + Сформована позитивна мотивація.

Може = Здатний фізично + Перебуває у нормальному психологічному стані.

Забезпечений = Існують відповідні санітарно-гігієнічні та матеріально-технічні умови праці.

Зазначені вище засади ризикорієнтованого підходу формують підґрунтя для розроблення та реалізація заходів менеджменту охорони праці.

Розуміння різних типів людських помилок стає у нагоді при визначенні заходів щодо підвищення рівня безпеки, за допомогою яких можна своєчасно виявити помилку та мінімізувати її наслідки.

Для визначення впливу ЛФ на безпеку застосовується один з методів оцінювання ризику − метод загального оцінювання надійності людини Human Reliability Assessment (HRA) [18].

Цей метод можна застосовувати для якісного та кількісного аналізування ризику. Якісна оцінка дій людини-оператора може використовуватися для ідентифікації його можливих помилок та їх причин, що, у свою чергу, дозволяє знизити імовірність цих помилок. Також метод HRA придатний для отримання кількісних даних щодо відмов, пов’язаних з помилками оператора, на додаток до застосування іншого методу оцінки ризику, наприклад FTA або інших методів.

Вхідні дані методу HRA [18]:

інформація для визначення завдань, які виконуються операторами;

дані щодо типових помилок, які зустрічаються на практиці, та їх причин;

експертні оцінки помилок людини-оператора та їх кількісна оцінка.

Процес HRA відбувається за такими етапами (рис. 3.5) [18]:

1. Постановка завдання. Визначення типів дій людини-оператора, які повинні бути досліджені і оцінені.

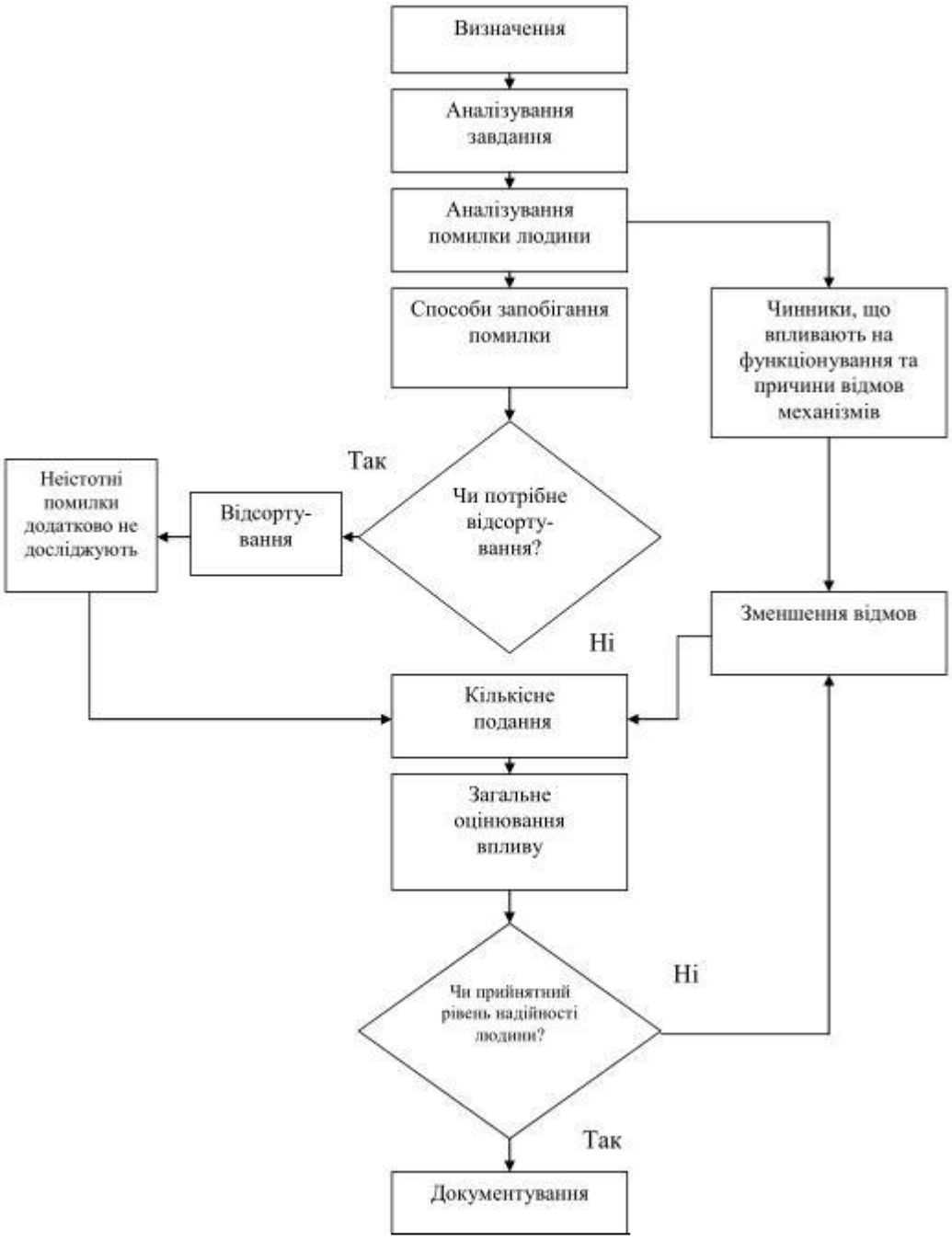

Рис. 3.5. Алгоритм аналізу впливу людського фактора за допомогою методу HRA

2. Аналізування завдання. Визначення способів виконання завдання та допоміжних засобів, необхідних для його виконання.

3. Аналізування помилки оператора. Визначення відмов, що виникають в процесі виконання завдання, можливих помилок оператора і способів їх усунення.

4. Подання. Визначення того, як ці помилки при виконанні завдання в поєднанні з іншими подіями, пов’язаними з устаткуванням, програмним забезпеченням та іншими факторами, можуть бути використані для розрахунку імовірності відмови системи в цілому.

5. Попереднє перевіряння. Визначення помилок або завдань, які вимагають детальної кількісної оцінки.

6. Кількісне оцінювання. Визначення імовірності помилок оператора та відмов при виконанні завдання.

7. Оцінювання впливу. Визначення значущості помилок або завдань, тобто помилок і завдань, які більшою мірою впливають на забезпечення надійності або прийнятного рівня ризику.

8. Скорочення помилок. Визначення способів скорочення кількісних помилок оператора.

9. Документування. Визначення інформації та деталей аналізу HRA, які повинні бути задокументовані.

На практиці процес HRA найчастіше виконують поетапно, хоча іноді деякі його етапи (наприклад, аналізування завдань та ідентифікацію помилок) проводять паралельно.

Вихідні дані процесу HRA [18]:

перелік помилок, які можуть статися, та методи їх виключення;

види помилок, причини та наслідки типових помилок;

якісна або кількісна оцінка ризику розглянутих помилок.

Переваги методу HRA [18]:

метод забезпечує формалізований підхід до вивчення помилок людини-оператора при оцінюванні ризику для систем, у яких персонал відіграє важливу роль;

формалізоване дослідження видів і помилок оператора та способів дозволяє зменшити імовірність відмов, викликаних цими помилками.

Недоліки методу HRA [18]:

значна складність і різноманіття способів поведінки операторів створює значні труднощі при визначенні простих видів відмови та оцінюванні їх імовірності;

неможливо описати багато дій операторів за допомогою понять «працездатний» та «непрацездатний» стан;

метод важко застосувати в ситуації із частковими відмовами чи відмовами через прийняття невідповідних рішень.

Для прикладу проведемо аналіз ризиків впливу ЛФ на безпеку виконання вантажопідіймальних робіт в умовах транспортного підприємства із використанням методу HRA.

Вихідною інформацією у даному випадку буде:

сукупність інформаційних характеристик працівника;

сукупність норм з охорони праці щодо технічного стану вантажопідіймального обладнання;

сукупність норм з охорони праці щодо технологічного процесу проведення вантажопідіймальних робіт;

сукупність норм з охорони праці щодо стану виробничого середовища.

Для аналізування ризику скористаємося бальною експертною шкалою:

для шкали імовірності виникнення помилки *(P)*: 10 балів – імовірність виникнення P=0,999; 1 бал – імовірність виникнення P=0,001;

для шкали оцінювання тяжкості наслідків (H): 10 балів – тяжкість наслідків є максимальною; 1 бал – тяжкість наслідків є несуттєвою, наслідками можна знехтувати.

Ризик R будемо визначати за формулою:

$$R=P\cdot H$$

де P – імовірність виникнення помилки з боку правцівника;

H – тяжкість наслідків.

Результати проведених розрахунків представлені у табл. 3.9.

Таблиця 3.9

Аналіз ризику впливу людського фактора на безпеку виконання вантажопідіймальних робіт (методом HRA)

№ з/п	Опис можливої помилки працівника	Причина виникнення помилки	*P*	*H*	*R*
1	Перевищення вантажопідйомності вантажопідіймального механізму	Хворобливий стан працівника	6	10	60
		Недоліки у проведенні навчання з охорони праці	5	10	50
		Знаходження у стані алкогольного, наркотичного сп’яніння	7	10	70
2	Виконання робіт на несправному вантажопідіймально му пристрої	Незадовільний рівень контролю за станом вантажопідіймального обладнання	7	9	63
		Недоліки у проведенні навчання з охорони праці	8	9	72
3	Використання вантажопідіймально-	Знаходження у стані алкогольного, наркотичного сп’яніння	7	9	63
		Незадовільний рівень контролю за охороною праці з боку безпосереднього керівника робіт та особи, відповідальної за експлуатацію вантажопідіймального устаткування	7	9	63
4	Невикористання засобів індивідуального захисту	Недоліки у проведенні навчання з охорони праці	6	8	48
		Незадовільний рівень контролю за охороною праці з боку безпосереднього керівника робіт та особи, відповідальної за експлуатацію вантажопідіймального устаткування	7	8	56

Деталізація аналізу залежить від складності аналізованого процесу та завдань, які висувають експертам з безпеки.

За результатами проведеного аналізу ризику визначено, що для досліджуваного прикладу найбільш значущими є помилки, пов’язані із виконанням робіт на несправному вантажопідіймальному пристрої. Тому, задля забезпечення безпеки праці при проведенні вантажно- розвантажувальних робіт першочерговим

завданням є саме вдосконалення системи контролю за технічним станом вантажопідіймального обладнання.

Розглянемо основні шляхи підвищення рівня надійності персоналу. Професійна надійність працівника полягає в працездатності і функціональній готовності його психіки працювати в нормальних і екстремальних умовах на заданому рівні якості. Далеко не кожна людина є спроможною до застосування своїх професійних знань у скрутних непередбачених ситуаціях або за низької мотивації до виконання певних завдань. є його Саме особистісні психологічні та психофізіологічні якості персоналу є визначальними в забезпеченні його психологічної готовності до застосування власних професійних знаню.

Психологічна готовність персоналу до роботи в мінливих умовах завжди займала одну з провідних позицій у проблемі його надійності. На рівень психологічної готовності персоналу впливають такі чинники, як: професійна компетентність; функціональний стан; особистісні психологічні якості; соціально-психологічний клімат в колективах; соціальні умови роботи і життя персоналу.

Можна запропонувати такі методи підвищення надійності персоналу [59]:

підвищення відповідальності (духовний, правовий, організаційний та інші аспекти);

кваліфікаційний і психофізіологічний відбір, навчання і тренування кандидатів на тренажерах;

автоматизація рутинних операцій, що не вимагають інтелектуальних зусиль;

удосконалення робочого місця, інформаційного забезпечення та підтримки оператора, організації управління, взаємодії і розподілу відповідальності персоналу.

Як принципи забезпечення безпеки об’єктів за рахунок зниження ролі ЛФ можна запропонувати [59]:

пріоритет технічних заходів безпеки над організаційними. Чим більше прийнято технічних заходів і досконалішим є кожний з них, тим менший вплив на безпеку об’єкта чинить ЛФ. Однак навряд чи коли- небудь вдасться виключити цей вплив повністю. Виключення людини з процесу управління потенційно небезпечним об’єктом поки є несвоєчасним і неефективним, враховуючи унікальні властивості

людини знаходити оптимальні рішення в складних ситуаціях. Поки це доцільно лише на короткий час відразу після аварії, коли людина ще перебуває в умовах стресу і не має об'єктивної інформації про розвиток аварійного процесу;

створення умов для прийняття правильних рішень щодо запобігання аваріям;

удосконалення організаційних заходів забезпечення безпеки небезпечних об'єктів, які доповнюють технічні заходи та, за можливості, компенсують їхню недосконалість.

Організаційними заходами зниження передумов для здійснення персоналом помилкових і злочинних дій, що можуть призвести до негативних наслідків, є:

організація відбору персоналу за медичними і психофізіологічними характеристиками, морально-вольовими якостями, рівнем освіти і здібностями;

перевірка медичного і психофізіологічного стану персоналу безпосередньо перед проведенням небезпечних робіт;

вдосконалення норм і правил безпеки при проведенні небезпечних робіт;

навчання персоналу нормам і правилам безпеки і періодична перевірка знань;

дотримання «правила декількох осіб» при проведенні небезпечних операцій;

відпрацювання персоналом практичних навичок на макетах і тренажерах;

інструктаж перед виконанням небезпечних робіт тощо.

Нарешті, одним із найважливіших методів управління ризиками впливу людського фактору на безпеку та якість продукції, процесів, прийнятих рішень, послуг є постійний контроль персоналу під час виконання ним всіх видів діяльності.

3.3 Управління кібер-ризиками у діяльності підприємства

З огляду на широке використання сучасних інформаційних технологій у діяльності будь-якого сучасного підприємства взагалі та його СУЯ зокрема, необхідно враховувати вплив такої відносно нової форми ризиків, як кібер-ризики на всі аспекти його функціонування.

Останнім часом значно зросла кількість кібер-атак як на світові, так є на українські організації [60]. Метою хакерів стають не лише державні інституції та великі підприємства, а й приватний сектор, малий та середній бізнес. Згідно із звітом про ризики кібербезпеки Cybersecurity Venturesreport, у 2019 році бізнес буде стикатися з кібер-атаками кожні 14 секунд, а до 2021 року збитки від кібер-загроз сягнуть 6 трлн дол. [61].

Кібер-ризики є найбільш недооціненими ризиками в довгостроковій перспективі в Україні. Яскравим прикладом цього є те, що у 2017 році під час кібератаки вірусу Petya постраждали понад 1500 компаній, а 13 тис комп'ютерів були заражені. За рік український бізнес втратив від кібератак мільярди гривень [60]. Узагальнений аналіз даних щодо кибер-ризиків в 2017 році як в Україні, так і в світі наведено у табл. 3.10 [60].

Таблиця 3.10

Топ-10 кібер-ризиків у 2017 році

№ з\п	Назва	Суть ризику
1	Petya	програма-вимагач, яка шифрує дані
2.	Blueborne	вразливість - у протоколі Bluetooth
3	NotPetya	програма, яка знищує дані на ПК
4	Wannacry	програма-шифрувальник, що вимагає викуп за дешифрування
5	KRACK	критична уразливість мереж Wi-Fi
6	EternalBlue	програма для одержання віддаленого доступу до системи
7	Bad rabbit	вірус-шифрувальник, розроблений для ОС сімейства Windows
8	Loki / Locky	Android-шкідливий / шифрувальник Windows
9	Reaper	вірус, спрямований на IoT-пристрої
10	Критична вразливість у доступі під root користувачем в MacOS	

Основними потенційно небезпечними джерелами (чинниками) виникнення кібер-ризику можуть бути [60]:

1) втрата або крадіжка носіїв інформації та мобільних пристроїв;

2) доступ сторонніх осіб до конфіденційної інформації за допомогою вразливих хмарних сховищ;

3) ненавмисне розголошення співробітниками конфіденційної інформації;

4) навмисні дії співробітників (інсайдерів);

5) неконтрольоване копіювання даних співробітниками.

Узагальнена класифікація кібер-ризиків наведена на рис. 3.6 [60].

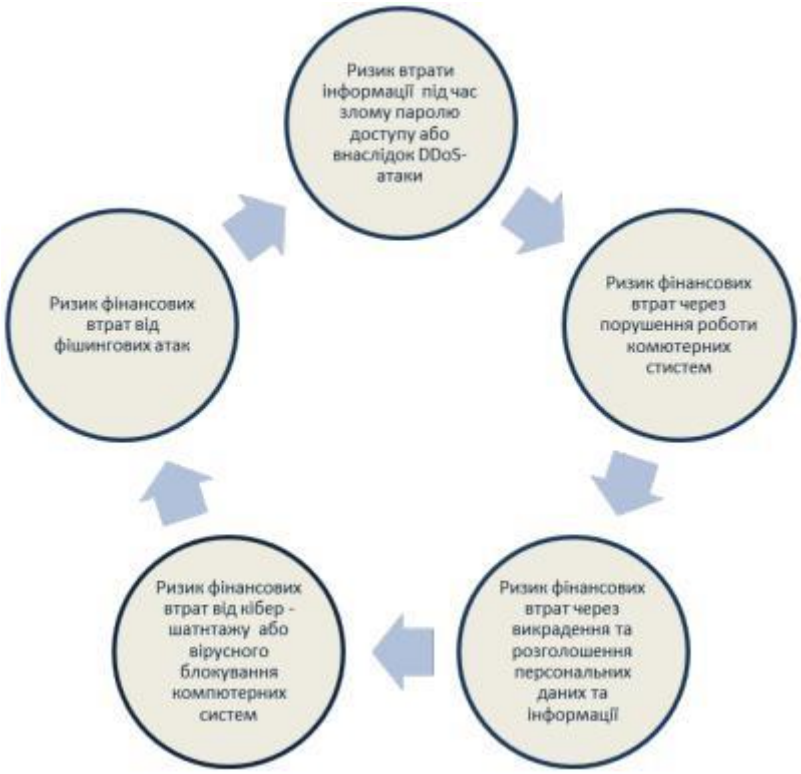

Рис. 3.6. Узагальнена класифікація кібер-ризиків

Негативний ефект від кібер-ризиків може включати втрату прибутку, пошкодження інформаційної системи, зниження продуктивності, втрату репутації у клієнтів. У цьому відношенні організації малого та середнього бізнесу більше втрачають, ніж великі підприємства, адже кібер-атака є надзвичайно коштовною справою.

Зважаючи на великі втрати від кібер-атак, з 25 травня 2018 року набрав чинності Загальноєвропейський регламент про захист персональних даних (англ. GDPR – General Data Protection Regulation) [63], який погоджує стандарти захисту даних в межах ЄС, а ті, хто не виконує його вимоги, може штрафуватися Радою зі стандартів безпеки даних індустрії платіжних карт (англ. PCI SSC - Payment Card Industry Security Standards Council) [60].

Регламент є загальнообов’язковим документом без необхідності імплементації його норм у національне законодавство кожної країни-учас ниці. Норми Регламенту є нормами прямої дії. Найбільше потрібно зосередитися на тих компаніях, які організовують свою діяльність у сфері інформаційних технологій та здійснюють її

через всесвітню мережу Інтернет, оскільки їхня діяльність більшою мірою пов'язана з персональними даними, ніж діяльність будь-яких інших компаній. Порушення норм регламенту передбачає штраф у розмірі до 20 млн євро або до 4% від річного обороту компанії [62].

При цьому більшість представників бізнесу як у Європі, так і в Україні почали усвідомлювати, що з розвитком технологій ризики від кібер-загроз будуть тільки підвищуватися [62].

Із світового досвіду боротьби з кібер-загрозами відомо, що ефективного захисту даних організації можуть досягти лише з використанням розподіленої інфраструктури та резервного копіювання, адже будь-які дані, які зберігаються в одному місці, колись можуть бути втрачені – це лише питання часу. Резервне копіювання значно скорочує простоювання системи при втраті даних, кібератак або технічних неполадок, а розподілена інфраструктура ефективно усуває ризик недоступності. Також для організацій важливо чітко розуміти, яку інформацію необхідно захищати. На думку фахівців компанії «Ернст енд Янг» захисту від кібер-загроз потребує така інформація:

1) економічна (інформація щодо видів продукції чи послуг; статистика обсягів продажів; фінансові транзакції; звітність до її офіційної публікації; прогнози виробництва; інформація щодо заробітної платні);

2) персональна (номери кредитних карток; паспортні дані; ідентифікаційні номери; інформація для доступу в системи - логіни, паролі, ключі, налаштування);

3) ділова (постанови, які видані регулюючими органами щодо роботи бізнесу; інтелектуальна власність; проектна документація);

4) інформація про споживачів і клієнтів (реєстри клієнтів; реквізити партнерів; реєстри потенційних клієнтів) [63].

Отже, у сучасних умовах будь-яким організаціям потрібно постійно підвищувати свою здатність оперативного реагування на неминучі кібер-атаки та якомога швидшого повернення до штатних умов функціонування. Цього можна досягнути за допомогою менеджменту кібер-ризиків організацій, який повинен включати комплекс таких дій:

1) навчання і підготовка користувачів з метою підвищення їх інформованості;

2) розроблення процедур управління IT-інцидентами, в тому числі процедур реагування та ліквідації наслідків їх виникнення;

3) розроблення керівництва з кібербезпеки (воно повинно містити найкращі практики кібер-безпеки. Доцільно включити процедури забезпечення безпеки працівників, постачальників та клієнтів. Політика в галузі кібербезпеки повинна містити також протоколи, яких працівники повинні дотримуватися у разі виявлення порушень);

4) використання процедур захисту від шкідливих програм; контроль використання змінних носіїв інформації;

5) страхування кібер-ризиків [63].

Управління кібер-ризиком, яке повинно полягати в оцінюванні загроз і ризиків, розробленні заходів щодо впливу на них та постійному моніторингу залишкових ризиків, не повинно бути одноразовим рішенням. Управління кібер-ризиком стає стратегічним імперативом, який має глибокий характер та наслідки для загальної продуктивності організацій, воно нерозривно пов’язане зі здатністю організацій вести свій бізнес ефективно.

3.4 Висновки до третього розділу

У розділі розроблено пропозиції щодо удосконалення процесів управління ризиками в системах управління якістю, зокрема:

розроблено проект задокументованої процедури СУЯ «Управління ризиками» для вищого навчального закладу (ВНЗ). У рамках проекту описані дії щодо встановлення контексту організації, розроблені алгоритм управління ризиками, порядок ідентифікації, оцінювання та обробляння ризиків і можливостей, запропонована класифікація ризиків / можливостей за імовірністю виникнення та за наслідками, визначені управлінські впливи залежно від виду ризику, сформовані

показники результативності процесу «Управління ризиками» та визначені повноваження і відповідальність за реалізацію етапів процедури;

для врахування впливу людського фактора на процеси управління ризиком запропонований алгоритм, заснований на методі оцінки ризику Human Reliability Assessment (HRA), який дозволяє провести як якісний, так і кількісний аналіз ризику. Застосування алгоритму дозволить визначити роль людського фактора у реалізації певної небезпеки та запобігти виникненню аварії чи нещасного випадку на робочих місцях, а також забезпечить розуміння причин виникнення помилок і різних факторів, які збільшують вірогідність їх виникнення та погіршують можливість їх виявлення, що, у кінцевому рахунку, допоможе розробити більш ефективні засоби контролю;

з огляду на широке використання сучасних інформаційних технологій у діяльності будь-якого сучасного підприємства взагалі та його СУЯ зокрема, та значне зростання кількості кібер-атак, запропоновано комплекс заходів щодо управління кібер-ризиками у діяльності підприємства, зокрема навчання і підготовка користувачів з метою підвищення їх інформованості; розроблення процедур управління ІТ-інцидентами, в тому числі процедур реагування та ліквідації наслідків їх виникнення; розроблення керівництва з кібербезпеки; використання процедур захисту від шкідливих програм; контроль використання змінних носіїв інформації; страхування кібер-ризиків.

Розроблені у роботі пропозиції призначені для використання у практичній діяльності підприємств бідь якого розміру, сфери діяльності та форм власності.

РОЗДІЛ 4
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

У Законі України «Про Основні засади (стратегію) державної екологічної політики України на період до 2030 року» [64] зазначено: «Процеси глобалізації та суспільних трансформацій підвищили пріоритетність збереження довкілля, а отже, потребують від України вжиття термінових заходів. Протягом тривалого часу економічний розвиток держави супроводжувався незбалансованою експлуатацією природних ресурсів, низькою пріоритетністю питань захисту довкілля, що унеможливлювало досягнення збалансованого (сталого) розвитку» [64]. Звідси стає очевидним визнання на найвищому державному рівні важливості та актуальності негайного розроблення комплексу заходів щодо охорони навколишнього природного середовища в Україні на всіх рівнях управління.

Одними з основних завдань державної екологічної політики України на період до 2030 року є «запровадження міжнародних стандартів систем екологічного управління(СЕУ) на підприємствах і в компаніях, яке сприятиме розвитку системи управління навколишнім природним середовищем та реалізації в Україні міжнародних природоохоронних ініціатив» та «впровадження системи управління екологічними ризиками в усіх сферах національної економіки, яке сприятиме запобіганню катастроф техногенного та екологічного характеру» [64].

З огляду на вищенаведене, у розділі розглянуті міжнародні стандарти СЕУ та питання управління екологічними ризиками.

4.1 Огляд основних міжнародних стандартів на системи екологічного управління

Одним з перших у світі стандартів з упровадження СЕУ став британський стандарт BS 7750 (British Specification for Environmental Management Systems) [65],

розроблений у 1992 р. Британським інститутом стандартизації.

Він не встановлює вимог до природоохоронної діяльності підприємства, однак містить рекомендації, корисні для створення ефективної СЕУ, визначаючи етапи розроблення і впровадження СЕУ [66].

Положення цього британського стандарту були враховані Міжнародною організацією стандартизації (ISO) при розробці стандарту ISO 14001.

Схема екологічного менеджменту і аудиту EMAS (Eco-Management and Audit Scheme) [67] була розроблена для держав-членів Європейського Союзу у першій половині 1990-х рр. з метою оцінки й покращення екологічних характеристик діяльності організацій, а також створення належних умов для отримання екологічної інформації зацікавленими сторонами. Систему було створено виключно для промислових підприємств. Реєстрація (сертифікація) організацій відповідно до вимог EMAS є добровільною. Система EMAS складається з декількох етапів, які залежать один від одного. Вважається, що основою для розроблення EMAS був британський стандарт BS 7750, тому основні пункти загальноєвропейської системи екологічного управління й аудиту та британського стандарту є досить схожими.

Натепер система EMAS діє лише в межах Європейського Союзу. Вона може бути цікавою для виробників, які орієнтовані на експорт до країн ЄС або країн, які претендують на членство в ЄС. Проте вона не може замінити загальновизнані міжнародні стандарти ISO серії 14000.

Основні підходи щодо розроблення та удосконалення СЕУ розглядають на базі стандартів ISO серії 14000, які визначають системний підхід до аналізування та покращення показників екологічної дієвості організації.

Стандарти серії ISO 14000 орієнтовані на поліпшення екологічних характеристик діяльності підприємства, мають рекомендаційний характер і містять практичні інструменти для створення ефективної СЕУ та розвитку ініціативного екологічного аудиту.

Стандарти серії ISO 14000 включають групи стандартів з таких питань: принципи розроблення та впровадження СЕУ; оцінювання життєвого циклу та управління ним; інструменти екологічного контролю та оцінки; комунікації, екологічні декларації та маркування; стандарти, що орієнтовані на продукцію;

управління парниковими газами.

Сучасна серія стандартів ISO 14000 вважається найбільш перспективною та пристосованою для впровадження СЕУ в усьому світі.

Серія ISO 14000 виникла внаслідок рішень, прийнятих на двох визначних самітах: Всесвітньому саміті ООН зі сталого розвитку, що відбувся в Ріо-де-Жанейро у 1992 р., та протягом Уругвайського раунду переговорів щодо Генеральної угоди з тарифів і торгівлі (сучасна Світова організація з торгівлі) у 1994 році.

Головною метою впровадження стандартів серії ISO 14000 стало забезпечення єдиних рекомендацій для всіх країн світу, які враховують найкращий досвід уже наявних регіональних або національних СЕУ. Міжнародні стандарти ISO серії 14000 та відповідні національні стандарти є базою для побудови СЕУ в організації.

Ключовим поняттям стандартів серії ISO 14000 є поняття СЕУ. Тому головним стандартом у цій серії вважається ISO 14001. У 2015 році Міжнародною організацією зі стандартизації було прийнято редакцію ISO 14001:2015 [68]. ISO 14001 установлює вимоги до системи екологічного управління, що їх організація може використовувати для підвищення своєї екологічної дієвості.

Стандарт побудований на основі циклу Шухарта-Демінга або PDCA (плануй-виконуй-контролюй-дій) і має структуру високого рівня (рис. 4.1) [66].

Призначення цього стандарту – надати організаціям загальну схему діяльності задля охорони довкілля та реагування на зміни умов довкілля в рівноважному поєднанні із соціально-економічними потребами. Дії стосовно ризиків і можливостей – вимога, які належить до ризиків і можливостей, пов’язаних із СЕУ. У попередній версії стандарту подібна вимога була наявна як вимога до прогнозування й попередження помилок. Станадарт очікує, що організації будуть виявляти й аналізувати свої ризики та можливості (пов’язані з унікальним контекстом організації, її заінтересованими сторонами, зобов’язаннями та екологічними аспектами), які можуть вплинути (позитивно чи негативно) на здатність їх системи екологічного управління досягати запланованих результатів. Стандарт також очікує, що організації будуть вживати відповідних заходів для подолання всіх ризиків та використання можливостей.

Рис. 4.1. Цикл Шухарта-Демінга в системі екологічного управління та структура стандарту ISO 14001:2015

Організації також повинні визначити, яким чином ці заходи будуть упроваджені до процесів системи екологічного управління і яким чином буде здійснюватися контроль, оцінка та аналіз ефективності цих заходів та процесів. Ця вимога дозволяє організації визначити фактори, які можуть викликати відхилення результатів її процесів та системи екологічного управління від запланованих. Організації повинні розробити попереджувальні засоби і методи для мінімізації негативного впливу й максимально використовувати можливості, які виникають.

Призначення цього стандарту – надати організаціям загальну схему діяльності задля охорони довкілля та реагування на зміни умов довкілля в рівноважному поєднанні із соціально-економічними потребами. Дії стосовно ризиків і можливостей – вимога, які належить до ризиків і можливостей, пов’язаних із СЕУ. У попередній версії стандарту подібна вимога була наявна як вимога до прогнозування й попередження помилок. Станадарт очікує, що організації будуть виявляти й аналізувати свої ризики та можливості (пов’язані з унікальним контекстом організації, її заінтересованими сторонами, зобов’язаннями та екологічними аспектами), які можуть вплинути (позитивно чи негативно) на

здатність їх СЕУ досягати запланованих результатів. Стандарт також очікує, що організації будуть вживати відповідних заходів для подолання всіх ризиків та використання можливостей. Організації також повинні визначити, яким чином ці заходи будуть упроваджені до процесів СЕУ і яким чином буде здійснюватися контроль, оцінка та аналіз ефективності цих заходів та процесів. Ця вимога дозволяє організації визначити фактори, які можуть викликати відхилення результатів її процесів та СЕУ від запланованих. Організації повинні розробити попереджувальні засоби і методи для мінімізації негативного впливу й максимально використовувати можливості, які виникають.

Доповнює ISO 14001 та надає додаткові вказівки та корисні пояснення щодо впровадження СЕУ стандарт ISO 14004 [69]. Стандарт покликаний допомогти організаціям отримати максимальну віддачу від своїх систем управління впливом на довкілля, незалежно від розміру або типу таких організацій.

У стандарті ISO 14005 [70] подано настанови для всіх організацій, але особливо для малих та серед - ніх підприємств, щодо поетапного розробляння, запроваджування, підтримування та поліпшування СЕУ. Стандарт також містить рекомендації щодо інтеграції й використання екологічних методів оцінки продуктивності. Стандарт застосовний до будь-якої організації, незалежно від рівня її розвитку, характеру діяльності чи місця її провадження. СЕУ не стосується виключно екологічних аспектів процесів виробництва. Вони пов’язані із зв’язками з постачальниками, підрядниками, продукцією чи послугами, виконанням робіт, споживачами та іншими зацікавленими сторонами. Тому комітет ISO/TC 207 розробив додаткові інструменти для вирішення таких аспектів.

Оцінка життєвого циклу (ОЖЦ) є інструментом для визначення та оцінки екологічних аспектів товарів та послуг від «колиски до могили»: від отримання природних ресурсів до можливостей утилізації продукту або його відходів.

Стандарти серії ISO 14040 дають рекомендації щодо принципів та методів досліджень життєвого циклу, які надають організації інформацію про те, як зменшити загальний вплив своїх продуктів та послуг на стан довкілля.

Зокрема, стандарт ISO 14040 установлює принципи та структуру ОЖЦ.

ISO 14044 визначає вимоги та містить рекомендації щодо ОЖЦ, у тому числі:

визначення мети і сфери застосування ОЖЦ, стадії інвентаризаційного аналізу життєвого циклу, стадії оцінки впливу життєвого циклу, стадії інтерпретації життєвого циклу, підготовки звітів і критичного аналізу ОЖЦ, обмежень ОЖЦ, взаємозалежності стадій ОЖЦ, умов використання кількісних значень і додаткових елементів. Деякі приклади, які пояснюють положення ISO 14044, містить стандарт ISO/TR 14047.

Стандарт ISO/TR 14049 містить приклади виконання методів інвентаризаційного аналізування життєвого циклу (ІАЖЦ) як засобу задоволення відповідних положень стандарту ISO 14044.

Серія стандартів ISO 14020 стосується різноманітних підходів до застосування екологічних декларацій та маркувань, що вказують на екологічні характеристики та переваги продукції.

ISO 14026 [71] містить принципи, вимоги та настанови щодо повідомлення про екологічні аспекти та потенційний вплив на довкілля продукту, пов'язаний з конкретною проблемою.

ISO/TS 14027 [72] містить принципи, вимоги та настанови щодо розроблення, перегляду, реєстрації та оновлення правил категорії продукції в рамках екологічної декларації типу III або програм вуглецевого сліду, які базуються на основі ОЖЦ відповідно до ISO 14040 та ISO 14044, а також ISO 14025, ISO 14046 і ISO/TS 14067. Стандарт також надає інструкції щодо способів інтеграції додаткової екологічної інформації, незалежно від того, чи вона ґрунтується на ОЖЦ, на основі узгодженого та науково обґрунтованого способу відповідно до стандарту ISO 14025.

Ефективно впроваджена СЕУ дозволить ідентифікувати ті сфери в організації, у яких можливе зменшення витрат, та ті сфери, які потребують удосконалення. Це також повний контроль за «правовою відповідністю» організації, зокрема, законодавству у сфері охорони навколишнього природного середовища. Завдяки чіткому визначенню відповідальності покращується організація праці, а отже, відбувається зменшення питомих витрат і зростання конкурентоспроможності організації.

4.2 Підходи до управління екологічними ризиками

Поняття екологічного ризику розглядається різними дослідниками і науковцями по різному. Ряд авторів до проблемами екологічного ризику вважають не лише ризик для здоров'я населення, а ряд інших його видів. Наприклад, виділяють такі види екологічного ризику: 1) ризик руйнування природних систем; 2) ризик для здоров'я населення; 3) ризик техногенних систем для конкретного промислового підприємства; 4) ризик у керуванні природними ресурсами; 5) ризик природних катастроф; 6) ризик впливу регіональних військових конфліктів; 7) ризик екологічного тероризму [73].

Наприкінці 80-х років XX ст. Агентством з охорони навколишнього середовища США (EPA) були систематизовані методи аналізу ризику окремих факторів навколишнього середовища, зокрема ті, що не мають порогового характеру дії (радіонуклідів, хімічних канцерогенів) [73]. Далі були розроблені методики оцінювання ризику на популяційному рівні.

У медико-екологічних дослідженнях використовують такі види ризику: відносний, атрибутивний, атрибутивний популяційний і популяційна фракція атрибутивного ризику [73].

Основні джерела ризику в галузі екології наведені у табл. 4.1 [73].

Таблиця 4.1

Основні джерела ризику в галузі екології

№ з/п	Назви
1	Спонтанність природних процесів і явищ, стихійні лиха
2	Випадковість соціально-економічних процесів, багатоваріантність взаємозв'язків між суб'єктами
3	Наявність антагоністичних тенденцій, що протидіють, зіткнень суперечливих інтересів
4	Невизначеність і ризик зумовлюються імовірнісним характером НТП
5	Існування невизначеності внаслідок неповної і недостатньої інформації про об'єкт, процес, явище, якого стосується прийняття рішення. Обмеженість щодо збору та обробки інформації, яку потрібно постійно оновлювати
6	Обмеженість та недостатність усіх необхідних ресурсів (матеріальних, фінансових, трудових тощо) для прийняття та реалізації рішень
7	Неможливість однозначного пізнання об'єкта за наявних рівнів і методів наукового пізнання
8	Відносна обмеженість свідомої діяльності людей, неминучі відмінності в соціально-психологічних установках, ідеалах, намірах, оцінках, стереотипах поведінки
9	Незбалансованість основних компонентів господарського механізму: планування ціноутворення, МТП, фінансово-кредитні відносини

Очікувана частота несприятливих ефектів, яка виникає від негативного впливу факторів навколишнього середовища, визначається за формулою

$$R=F\cdot C,$$

де F – частота, C – наслідки [1].

Ризик для здоров’я людини через забрудненням навколишнього природного середовища виникає за умов:

існування самого джерела ризику (токсичної речовини в об'єктах навколишнього середовища, продуктах харчування тощо);

наявності цього джерела ризику в шкідливій для людини дозі;

схильності населення до дії заданої дози токсичної речовини.

Оцінка ризику для здоров’я – це кількісна та/або якісна характеристика шкідливих ефектів, здатних розвинутися в результаті впливу факторів навколишнього середовища на конкретну групу людей за специфічних умов експозиції.

У науковому аспекті оцінювання ризику (ОР) – це поступовий, системний розгляд усіх аспектів впливу факторів, що аналізується, для здоров’я людини, який передбачає обґрунтування допустимих рівнів впливу.

Основне завдання оцінки ризику полягає в отриманні та узагальненні інформації щодо можливого впливу факторів середовища існування людини на стан її здоров’я, необхідної та достатньої для обґрунтування найоптимальніших управлінських рішень щодо усунення та зниження рівнів ризику, оптимізації контролю (регулювання та моніторингу) рівнів експозицій та ризиків.

Процес Human Health Risk Assessment складається з наступних етапів [73]:

Оцінювання ризику: ідентифікація небезпеки; оцінка “доза-відповідь”; оцінка експозиції; характеристика ризику.

Керування ризиком: порівняння ризиків; оцінка впливів; реалізації рішень; моніторинг і оцінка ефективності.

Інформування про ризик: обмін інформацією і думками.

Етап ідентифікації небезпеки. Визначення речовин, рівнів, середовищ та шляхів надходження, які можуть викликати несприятливі наслідки для здоров’я людини, доведеність зв’язку між фактором та захворюванням небезпечних

чинників, оцінка вагомості доказів, їхньої здатності викликати певні шкідливі ефекти у людини за передбачуваних умов дії, а також відбирання пріоритетних чинників, що підлягають поглибленому дослідженню в процесі ОР [73].

Етап оцінки залежності "доза-відповідь". Кількісна характеристика зв'язків між концентрацією, експозицією чи дозою впливу, що вивчається, і що викликає шкідливі ефекти. Метою етапу є узагальнення всіх наявних даних щодо гігієнічних нормативів, безпечних рівнів дії (референтних доз та концентрацій), критичних органів/систем та шкідливих ефектів, а також оцінка застосування цих даних для розв'язання задач, поставлених у проекті щодо оцінки ризику [73].

Етап оцінки експозиції. Характеристика джерел забруднення, маршрутів руху забруднювачів від джерела до людини, шляхи та точки впливу, рівні експозиції тощо. На цьому етапі аналізують і визначають:

джерела надходження забруднення в навколишнє середовище;

маршрути дії і потенційні шляхи поширення, транспортні та впливні середовища;

остаточний сценарій дії зі встановленням місць потенційного контакту певних груп населення зі шкідливими чинниками (точок дії) і шляхів надходження їх в організм людини (під час дихання, споживання води, випадкового заковтування ґрунту тощо);

кількісна характеристика експозиції, що передбачає встановлення і оцінку величини, частоти і тривалості дії для кожного аналізованого шляху надходження забруднювачів, ідентифікованого на попередньому етапі;

надходження в організм (впливні дози) [73].

Визначення експозиції. Використання моделей дає змогу ідентифікувати шляхи впливу від джерел викидів до місць проживання населення для конкретних метеоумов та зобразити результати в просторовому та у часовому аспектах визначення середньорічних, середньодобових та максимальних концентрацій.

Етап характеристики ризику. Аналіз усіх отриманих даних, розрахунок ризиків для популяції та її окремих підгруп, порівняння ризиків з допустимими (прийнятними) характеристиками, порівняльна оцінка і ранжування різних ризиків за ступенем їхньої статичної, медико-біологічної та соціальної значущості. Цей етап

ОР інтегрує інформацію, отриману на попередніх етапах, з метою її подальшого використання на стадії управління ризиком.

Розрахунок неканцерогенних ризиків виконують за такими формулами [73]:

$$HQ = AD/RfD,$$

$$HQ = AC/RfC,$$

де HQ – коефіцієнт небезпеки; AD – середня доза, мг/кг; A_C – середня концентрація, мг/м^3; RfD – референтна (небезпечна) доза мг/кг; Rf_C – референтна (небезпечна) концентрація, мг/м^3.

Розрахунок індивідуального (ICR) канцерогенного ризику:

$$ICR = LADD \cdot SF,$$

де LADD – середньодобова доза протягом життя, мг/(кг*день); SF – фактор нахилу ((мг/кг* день)).

Розрахунок популяційного (PCR) канцерогенного ризику:

$$PCR = ICR \cdot POP,$$

де POP – чисельність досліджуваної популяції, людина; ICR – індивідуальний канцерогенний ризик.

Розрахунок кількості додаткових випадків смерті (AM):

$$AM = C \text{ x } MR \cdot N \cdot 365 \cdot 70,$$

де AM – кількість додаткових випадків смерті; C – концентрація, мг/м^3; MR – прогнозований рівень добової смертності.

Керування ризиком є логічним продовженням оцінки ризику і спрямоване на обґрунтування найкращих у певній ситуації рішень з його вилучення та мінімізації, а також динамічного моніторингу експозицій ризиків, оцінювання ефективності та коригування оздоровчих заходів.

У сучасних умовах перехідної економіки оцінювання ризику повинно стати підґрунтям для економічного аналізу екологічної політики держави та проектів.

Інтерналізація зовнішніх факторів дала б змогу визначати сукупну суспільну вартість проектів і політики на місцевому, регіональному та національному рівнях. До найважливіших категорій екологічних товарів і послуг належить охорона здоров’я населення та краса живої природи.

Оцінювання ризику може застосовуватися для: кількісної оцінки впливу довкілля на здоров'я населення; установлення стандартів; визначення пріоритетних напрямів проектного фінансування з державного бюджету, екологічних фондів; поточного та запобіжного санітарного контролю; визначення пріоритетів економічного розвитку на державному та локальному рівнях; оцінки завданої шкоди в судових справах щодо виплати компенсацій тощо.

Збитки оцінюють на підставі витрат та збитків індивідуума (котрий захворів або помер) та його сім'ї в зв'язку із втратою здоров'я або життя. Це також витрати та втрати, яких зазнає суспільство через порушення здоров'я населення.

Завершальним етап оцінювання ризику – *передавання та поширення інформації про ризик* зацікавленій частині населення.

Оцінювання екологічного ризику надає змогу:

охарактеризувати реальний або прогнозований збиток здоров'ю з урахуванням різного ступеня ефекту та обґрунтувати безпечні умов проживання населення;

визначити внески джерел різних груп у рівень ризику для здоров'я населення;

оцінити ступінь загрози для здоров'я на майбутню перспективу;

врахувати витрати на різні варіанти превентивних заходів та їхнє здійснення на практиці, оцінити адекватність скарг населення;

визначити основи перегляду санітарно захищеної зони (СЗЗ) та здійснити функціональне зонування територій;

встановити диференційовану плату за наднормативні викиди;

здійснювати квотування та визначати плату за будівельні об' єкти тощо [73].

Отже, широке використання методів управління екологічними ризиками на підприємствах усіх галузей вітчизняної економіки сприятиме запобіганню катастроф техногенного та екологічного характеру та екологічній безпеці населення нашої держави.

4.4 Висновки до четвертого розділу

У розділі визначено проведено огляд міжнародних стандартів на системи екологічного управління досліджено підходи до управління екологічними ризиками

Визначено, що найбільш перспективною та пристосованою для впровадження СЕУ в усьому світі вважається сучасна серія стандартів ISO 14000.

Установлено, що стандарти серії ISO 14000 включають групи стандартів з таких питань: принципи розроблення та впровадження систем екологічного управління; оцінювання життєвого циклу та управління ним; інструменти екологічного контролю та оцінки; комунікації, екологічні декларації та маркування; стандарти, що орієнтовані на продукцію; управління парниковими газами.

Зазначено, що широке використання методів управління екологічними ризиками на підприємствах усіх галузей вітчизняної економіки сприятиме запобіганню катастроф техногенного та екологічного характеру та екологічній безпеці населення нашої держави.

ВИСНОВКИ

У кваліфікаційній магістерській роботі вирішена актуальна задача, яка полягала в удосконаленні організації управління ризиками в системах управління якістю на основі дослідження теоретичних основ управління якістю та сучасних концепцій і методів управління ризиками.

Для досягнення мети дипломної роботи досліджено:

теоретичні основи управління якістю. Встановлено, що натепер найбільш розповсюдженими є дієвими у цій сфері є підходи, запропоновані у п'ятій версії стандартів ISO серії 9000, які багато у чому співпадають з концепцією TQM. Аналіз вимог стандарту ISO 9001:2015 до СУЯ організації показав, що однією з основних вимог, поруч із потребою у застосуванні процесного підходу, є необхідність упровадження ризик-орієнтованого підходу, імплементація якого потребує приймати рішення лише на основі результатів оцінювання ризиків;

сучасні концепції та методи ризик-менеджменту, викладені у найбільш відомих та розповсюджених стандартах з управління ризиком: COSO ERM, FERMA, Solvency, BASEL, ISO 31000, ISO/IEC 31010. Визначено, що усі стандарти мають рамковий характер та не подають визначеного механізму побудови системи ризик-менеджменту на підприємстві, однак найбільш загальне уявлення про сутність ризик-менеджменту незалежно від цілей його використання, виду діяльності та організаційної форми господарювання надає стандарт ISO 31000, а найбільш грунтовною класифікацією методів оцінювання ризику є класифікація, викладена у стандарті ISO/IEC 31010, у якому вони згруповані у 10 груп, пов'язаних з елементами процесу ризик-менеджменту та порівнюються з використанням метрики з 8 характеристик.

На підставі узагальнення результатів досліджень розроблено пропозиції щодо удосконалення процесів управління ризиками в системах управління якістю,

зокрема:

розроблено проект задокументованої процедури СУЯ «Управління ризиками» для вищого навчального закладу (ВНЗ). У рамках проекту описані дії щодо встановлення контексту організації, розроблені алгоритм управління ризиками, порядок ідентифікації, оцінювання та обробляння ризиків і можливостей, запропонована класифікація ризиків / можливостей за імовірністю виникнення та за наслідками, визначені управлінські впливи залежно від виду ризику, сформовані показники результативності процесу «Управління ризиками» та визначені повноваження і відповідальність за реалізацію етапів процедури;

для врахування впливу людського фактора на процеси управління ризиком запропонований алгоритм, заснований на методі оцінки ризику Human Reliability Assessment (HRA), який дозволяє провести як якісний, так і кількісний аналіз ризику. Застосування алгоритму дозволить визначити роль людського фактора у реалізації певної небезпеки та запобігти виникненню аварії чи нещасного випадку на робочих місцях, а також забезпечить розуміння причин виникнення помилок і різних факторів, які збільшують вірогідність їх виникнення та погіршують можливість їх виявлення, що, у кінцевому рахунку, допоможе розробити більш ефективні засоби контролю;

з огляду на широке використання сучасних інформаційних технологій у діяльності будь-якого сучасного підприємства взагалі та його СУЯ зокрема, та значне зростання кількості кібер-атак, запропоновано комплекс заходів щодо управління кібер-ризиками у діяльності підприємства, зокрема навчання і підготовка користувачів з метою підвищення їх інформованості; розроблення процедур управління ІТ-інцидентами, в тому числі процедур реагування та ліквідації наслідків їх виникнення; розроблення керівництва з кібербезпеки; використання процедур захисту від шкідливих програм; контроль використання змінних носіїв інформації; страхування кібер-ризиків.

Розроблені у роботі пропозиції призначені для використання у практичній діяльності підприємств бідь якого розміру, сфери діяльності та форм власності.

Також у роботі розглянуті питання охорони навколишнього середовища.

Розроблені у роботі пропозиції можуть бути використаними всіма організаціями, які бажають досягти конкурентної переваги на ринку, які прагнуть до досягнення стійкого успіху, зведення до мінімуму впливу невизначеності на їх діяльність, а також отримання вигоди від ризиків в організації.

Застосування розроблених заходів на практиці дозволить організаціям визначати фактори, які можуть спричиняти відхилення її процесів та її системи управління якістю від запланованих результатів, щоб установлювати запобіжні заходи контролю для зменшення негативних впливів та якнайбільшого використання можливостей у міру їх виникнення. Окрім того, буде мінімізовано вплив людського фактора на процеси управління та виробничої діяльності організації, що, у кінцевому рахунку, призведе до зменшення її матеріальних збитків від виробництва продукції (надання послуг) невідповідної якості, підвищить довіру споживачів і сприятиме зростанню її конкурентоздатності та стійкому прибутковому функціонуванню.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Минько Э. В., Минько А. Э., Смирнов В. П. Качество и конкурентоспособность продукции и процессов: Учеб. Пособие / СПбГУАП. − СПб., 2005. − 240 с.

2. Гиссин В. И. Управление качеством. – [2-е издание] Гиссин В. И. – М.: ИКЦ «МарТ», 2003. – 400 с.

3. Управління якістю : [підр.] / П. П. Вороб'єнко, І. В. Станкевич, Є. М. Стрельчук, О. І. Глухова. – Одеса: ОНАЗ, 2014. – 376 с.

4. Стандартизація і сертифікація продукції та послуг: навч. посіб. / Н. А. Мєдвєдєва, О. В. Радько, О. Д. Близнюк, М. М. Регульський. – К.: НАУ, 2013. – 400 с.

5. Вознюк Т. К. Управління якістю продукції на підприємствах легкої промисловості [Текст]: автореферат дис. ...канд. екон. Наук / Т. К. Вознюк; 08.00.04 – економіка та упр. підприємствами (за видами екон. діяльн.). – Хмельницький: ХНУ, 2015. – 21 с.

6. Траченко Л. А. Системи управління якістю підприємств сфери інжинірингу: монографія / Л. А. Траченко – Одеса : ОНЕУ, 2019. – 378 с.

7. Управління якістю: навчальний посібник / Г. І. Капінос, І. В. Грабовська. – К. : Кондор-Видавництво, 2016. – 278 с.

8. Офіційний сайт Європейської організації з контролю якості (European Organization for Quality) / [Електронний ресурс]. – Режим доступу: http://www.eoq.org/home.html.

9. ДСТУ ISO 9000:2015 Системи управління якістю. Основні положення та словник термінів.

10. Адлер Ю. П., Шпер В. Л. Истоки статистического мышления // Методы менеджмента качества – 2003. – № 1. – С.34–40.

11. Уилер Д., Чамберс Д. Статистическое управление процессами. Оптимизация бизнеса с использованием контрольных карт Шухарта / Пер. с англ.. М.: Альпина Бизнес Букс, 2009. – 272 с.

12. Кане М. М., Иванов Б. В., Корешков В. Н., Схиртладзе А. Г. Системы, методы и инструменты менеджмента качества: Учебное пособие. − СПб.: Питер, 2008. − 560 с.

13. ДСТУ ISO 9001:2015 Системи управління якістю. Вимоги.

14. ДСТУ ISO 9004:2018 Управління якістю. Якість організації. Настанови щодо досягнення сталого успіху.

15. ISO 19011:2018 Настанови щодо здійснення аудитів систем управління.

16. Офіційний веб-сайт Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») / [Електронний ресурс]. – Режим доступу: http://uas.org.ua.

17. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови.

18. IEC/ISO 31010:2019 Керування ризиком. Методи загального оцінювання ризику.

19. ДСТУ ISO/TR 31004:2018 (ISO/TR 31004:2013, IDT) Менеджмент ризиків. Настанова з впровадження ISO 31000.

20. Донець Л.І. Економічні ризики та методи їх вимірювання : навчальний посібник /Л.І. Донець. – К. : Центр навчальної літератури, 2006. – 312 с.

21. Томас Л. Бартон Риск-менеджмент. Практика ведущих компаний / Томас Л. Бартон, Уильям Г. Шенкир, Пол Л. Уокер; пер.с англ. Т. Клекота, В. Кравченко, М. Нежура, К. Сафонова – М.: Издательский дом Вильямс, 2008. – 208 с.

22. Дядюк М. А. Управління ризиками: консп. лекц. Харків: Форт, 2017. С. 165 URL: http://elib.hduht.edu.ua/jspui/handle/123456789/1893 (дата звернення: 17.11.2019).

23. Мамаева Л.Н. Управление рисками / Л.Н. Мамаева. – М. : Дашков и Ко, 2013. – 256 с.

24. Холмс Э. Риск-менеджмент: пер.с англ. – М.: Эксмо, 2007. – 304 с.

25. Боровик М. В. Ризик-менеджмент : конспект лекцій для студентів магістратури усіх форм навчання спеціальності 073 – Менеджмент / М. В. Боровик ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2018. – 65 с.

26. Peter L. Bernstein Against the Gods. The Remarkable Story of Risk . Бернстайн П. Против богов. Укрощение риска. М.: «Олимп-Бизнес», 2008. – 1008 с.

27. Kindinger J. P. Risk Factor Analysis – A New Qualitative Risk Management Tool [E-resource] / J. P. Kindinger, J. L. Darby // Proceedings of the Project Management Institute Annual Seminars & Symposium September 7–16, 2000, Houston,Texas, USA. – [Електронний ресурс]. – Режим доступу: https://www.lanl.gov/orgs/d/d5/documents/risk-fact.pdf.

28. Kaplan R. S., Mikes A. Managing Risks: A New Framework // HBR [Електронний ресурс]. – Режим доступу: https://hbr.org/2012/06/managing-risks-a-new-framework.

29. Солоникова Т.Г. Управление рисками в системе менеджмента качества организации: теоретические аспекты интеграции и внедрение на основе международных стандартов [Електронний ресурс]. – Режим доступу: http: http://sisupr.mrsu.ru/2013-3/PDF/solonikova_t_g_statya.pdf.

30. Филина Ф. Н. Риск-менеджмент / Ф.Н. Филина. – М. : ГроссМедиа, РОСБУХ, 2008. – 232 с.

31. Сосновська О.О. Ризик-менеджмент як інструмент забезпечення стійкого функціонування підприємства в умовах невизначеності / О.О. Сосновська, Л. В. Деденко // European scientific journal of Economic and Financial innovation. – 2019. – № 1 (3). – С. 71 – 79.

32. Knight F. H. Risk, Uncertainty and Profit. New York, 1965. pp.156.

33. Webster's Dictionary of English Usage. – 1989 by Merriam-Webster Inc, US. pp. 978.

34. Березуцький В.В. Небезпечні виробничі ризики та надійність: навчальний посібник для студентів за напрямком підготовки 6.170202 «Цивільна безпека» / В.В. Березуцький, М.І. Адаменко – Харків. : ФОП Панов А. М., 2016. – 385 с.

35. AS / NZS 4360: 2004 «Ризик-менеджмент», 2004 Об’єднаний стандарт з управління ризиками Австралії і Нової Зеландії.

36. A Risk Management Standard // FERMA. Federation of European Risk Management Associations. [Електронний ресурс]. – Режим доступу: http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-russian-

version.pdf.

37. ДСТУ ISO Guide 73:2013 (ISO Guide 73:2009, IDT) Керування ризиком. Словник термінів.

38. Dembo Ron S. Andrew Freeman Seeing Tomorrow: Rewriting the Rules of Risk / Dembo Ron S. – John Wiley & Sons, Apr 16, 1998. – 270 p.

39. Баранов А. Международные стандарты управления рисками: не Базелем единым / А. Баранов // Рынок ценных бумаг. – 2015. – № 5. – С. 23-33.

40. Герасименко О. Аналітичний огляд міжнародних стандартів з ризик-енеджменту, орієнтованих на підприємства різних галузей господарства / О. Герасименко // European Journal of Economics And Management. – 2018. –Vol. 4, Issue 4. – С. 10-29.

41. Управление рисками организаций. Интегрированная модель, сентябрь 2004 COSO ERM The Committee of Sponsoring Organizations of the Treadway Commission // [Електронний ресурс]. – Режим доступу: http://www.valtars.ru/files/upload/Actual_info/coso_upravlenie_riskami_organizacii_integrirovannaya_model.pdf.

42. Enterprise Risk Managament - Integrating with Strategy and Perfomance (2018). The Committee of Sponsoring Organizations of the Treadway Commission (COSO). [Електронний ресурс]. – Режим доступу: < https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.

43. Enterprise Risk Management. Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks. COSO. WBCSD. February 2018. [Електронний ресурс]. – Режим доступу: https://goo.gl/Etpcww.

44. About FERMA (2019). Federation of European Risk Management Associations. [Електронний ресурс]. – Режим доступу: https://www.ferma.eu/about/ about-ferma.

45. Framework for Cumulative Risk Assessment. EPA/630/P-02/001F May 2003 [Електронний ресурс]. – Режим доступу: URL: https://www.epa.gov/sites/production/files/2014-11/documents/frmwrk_um_risk_assmnt.pdf.

46. Working Together. FY 2018-2022 U.S. EPA Strategic Plan. Washington: U.S. EPA, 2018. 56 p. [Електронний ресурс]. – Режим доступу: URL: https://www.epa.gov/sites/production/files/2018-08/documents/fy-2018-2022-epa-strategic

plan-print.pdf.

47. Directive 2009/138/EU of the European Parliament and of the Council of 25 Nov. 2009 on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II), 335 p.

48. From Basel I to Basel II to Basel III / Pushpkant Shakdwipee, Masuma Mehta // International Journal of New Technology and Research. – 2017. –Vol. 3, Issue 1. – P. 66-70.

49. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги».

50. ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки.

51. BSI Standard 200-1 Information Security Management Systems (ISMS) Version 1.0, October 2017. [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2001_en_pdf.pdf?__blob=publicationFile&v=3

52. NIST 800-30 Guide for conducting risk assesments (Керівництво з інформаційними ризиками - керівництво з аналізу та управління ризиками був розроблений Лабораторією інформаційної технології (ITL) Національного інституту стандартів і технології (NIST) США і представлені рекомендації в керівництві з аналізу та управління ризиками.

53. Michelle Grech Tim Horberry, Thomas Koester Human Factors in the Maritime Domain. CBC Press, 2008.

54. Heather Ikin Overcoming Human Limitations in Managing Risk -[Електронний ресурс].- Режим доступу: .http://www.qldminingsafety.org.au/wp-content/uploads/2015/08/Ikin-overcoming- human-limitations-in-managing-risk.pdf.

55. Бодров В.А., Орлов В.Я. Психология и надежность: человек в системах управления техникой. – М.: Изд-во «Институт психологии РАН», 1998. – 288 с.

56. Health And Safety Executive (Офіційний сайт Управління охорони праці у Великобританії) – [Електронний ресурс]. – Режим доступу:

http://www.hse.gov.uk/index.htm

57. Understanding Human Factors a guide for the railway industry / Understanding Human Factors/June 08 [Електронний ресурс]. – Режим доступу: https://www.rssb.co.uk/Library/improving-industry-performance/2008-guide-understanding-human-factors-a-guide-for-the-railwav-industrv.pdf

58. Человеческий фактор безопасного труда / Правовая база по охране труда [Електронний ресурс]. – Режим доступу: https://websot.jimdo.com/

59. Вишняков Я.Д., Радаев Н.Н. Общая теория рисков : учеб. пособие для студ. высш. учеб. заведений. – 2-е изд., испр. – М. : Издательский центр «Академия», 2008. – 368 с.

60. Віннікова І.І. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними / І.І. Віннікова, С.В. Марчук // Східна Європа: економіка, бізнес та управління – 2018. – № 5 (16). – с. 110-114.

61. Global Cyber Security Industry 2018-2022. [Електронний ресурс]. – Режим доступу: https://www.reportlinker.com/market-report/Cybersecurity/517851/Cyber-Security? utm_source=adwords1&utm_medium=cpc&utm_campaign= Transportation & utm_adgroup=Cybersecurity_Reports&gclid= EAIaIQobChMIrqvcm5nq3AIVx44YCh 39Ww5e EAAY ASAAEgKx6vD_BwE.

62. GDPR. [Електронний ресурс]. – Режим доступу: https://www. olans.com.ua/novij-reglament-yes-pro-personalni.

63. Посилення цифрового середовища проти кібер-загроз. [Електронний ресурс]. – Режим доступу: https://www.pwc.com/ua/uk/survey/2018/ pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks-ukr.pdf.

64. Закон України від 28 лютого 2019 року № 2697-VIII «Про Основні засади (стратегію) державної екологічної політики України на період до 2030 року».

65. BS 7750:1992 Specification for Environmental Management Systems (Специфікації для систем екологічного менеджменту).

66. Системи екологічного управління: сучасні тенденції та міжнародні стандарти. Посібник / С.В. Берзіна, І.І. Яреськовська та ін. – К: Інститут екологічного управління та збалансованого природокористування, 2017. – 134 с.

67. EMAS (Eco-Management and Audit Scheme) [Електронний ресурс] / Режим доступу: http: // www.ec.europa.eu/environment/emas/index_en.htm. – Назва з екрану.

68. ДСТУ ISO 14001:2015 Системи екологічного управління. Вимоги та настанови щодо застосування.

69. ДСТУ ISO 14004:2016 Системи екологічного управління. Загальні настанови щодо запроваджування.

70. ДСТУ ISO 14005:2015 Системи екологічного управління. Настанови щодо поетапного запровадження системи екологічного управління, використовуючи оцінювання екологічних характеристик.

71. ISO 14026:2017 Environmental labels and declarations – Principles, requirements and guidelines for communication of footprint information (Екологічні маркування та декларації – Принципи, вимоги та керівні принципи для передавання інформації про сліди).

72. ISO/TS 14027:2017 Environmental labels and declarations – Development of product category rules (Екологічні маркування та декларації – Розробка правил категорії товарів).

73. Верес О.М. Дослідження множини ризиків прийняття рішень в галузі екології / О.М.Верес, В.М. Голиш // Вісник національного університету «Львівська політехніка». – 2010. – № 689. – С. 67-80.

ДОДАТКИ

Додаток А

Форма паспорта ризиків структурного підрозділу (відокремленого структурного підрозділу)

ПАСПОРТ РИЗИКІВ

_____

найменування структурного підрозділу (відокремленого структурного підрозділу)

	Найменування ризику / можливості	Оцінка (рівень)	Причини	Наслідки	Методи обробки
	2	3	4	5	6
	Найменування процесу				
	Ризики процесу				
	Можливості процесу				

Розглянутий на _____
засіданні / раді / нараді найменування структурного підрозділу

від _____ протокол № _____ .
дата засідання / ради / наради № протоколу

Керівник структурного підрозділу _____ ініціали, прізвище
підпис

_____
дата

Додаток Б

Форма паспорта ризиків процесу

ПАСПОРТ РИЗИКІВ

_____

процесу

	Найменування ризику / можливості	Оцінка (рівень)	Причини	Наслідки	Методи обробки
	2	3	4	5	6
	Найменування процесу				
	Ризики процесу				
	Можливості процесу				

Власник процесу _____ ініціали, прізвище
підпис

_____
дата

Додаток В
Форма паспорта ризиків СУЯ

ПАСПОРТ РИЗИКІВ
системи управління якістю
ВНЗ

	Найменування ризику / можливості	Оцінка (рівень)	Причини	Наслідки	Методи обробки
	2	3	4	5	6
	Найменування процесу				
	Ризики процесу				
	Можливості процесу				

Ректор _____ ініціали, прізвище
підпис

_____
дата

Додаток Г
Форма цілей в області якості структурного підрозділу (відокремленого структурного підрозділу)

Затверджую
_____
назва посади
_____
підпис **і**ніціали, прізвище
_____
дата

ЦІЛІ В ОБЛАСТІ ЯКОСТІ НА 20___РІК

_____
найменування структурного підрозділу (відокремленого структурного підрозділу)

Найменування цільового показника	Значення цільового показника	Ризики та можливості	Потрібні ресурси	Заходи з досягнення цілей	Відповідальні виконавці
1	3	4	5	6	7
Найменування процесу					

Розглянутий на _____
засіданні / раді / нараді найменування структурного підрозділу
від _____ протокол № _____ .
дата засідання / ради / наради № протоколу

Керівник структурного підрозділу _____ ініціали, прізвище
підпис

_____
дата

Додаток Д
Форма цілей в області ВНЗ

Затверджую
_____
назва посади
_____
підпис **і**ніціали, прізвище
_____
дата

ЦІЛІ В ОБЛАСТІ ЯКОСТІ НА 20____РІК
ВНЗ

Найменування цільового показника	Значення цільового показника	Ризики та можливості	Потрібні ресурси	Заходи з досягнення цілей	Відповідальні виконавці
1	3	4	5	6	7
Найменування процесу					

Розглянутий на _____
засіданні / раді / нараді ВНЗ
від _____ протокол № _____ .
дата засідання / ради / наради № протоколу

Ректор _____ ініціали, прізвище
підпис

_____
дата

Додаток Е

Форма плану заходів з управління ризиками структурного підрозділу (відокремленого структурного підрозділу)

ПЛАН ЗАХОДІВ З УПРАВЛІННЯ РИЗИКАМИ

_____
найменування структурного підрозділу (відокремленого структурного підрозділу)

№ п/п	Найменування ризика	Найменування заходу з управління ризиком	Термін виконання	Відповідальні виконавці	Відмітка про виконання
1	2	3	4	5	6
	Найменування процесу				

Розглянутий на _____
засіданні / раді / нараді найменування структурного підрозділу
від _____ протокол № _____ .
дата засідання / ради / наради № протоколу

Керівник структурного підрозділу _____ ініціали, прізвище
підпис

_____
дата

Додаток Є

Форма плану заходів з управління ризиками процесу

ПЛАН ЗАХОДІВ З УПРАВЛІННЯ РИЗИКАМИ

_____

найменування процесу

№ п/п	Найменування ризика	Найменування заходу з управління ризиком	Термін виконання	Відповідальні виконавці	Відмітка про виконання
1	2	3	4	5	6
	Найменування процесу				

Власник процесу _____ ініціали, прізвище

підпис

_____

дата

Додаток Ж

Форма плану заходів з управління СУЯ

ПЛАН ЗАХОДІВ З УПРАВЛІННЯ РИЗИКАМИ
системи управління якістю
ВНЗ

№ п/п	Найменування ризика	Найменування заходу з управління ризиком	Термін виконання	Відповідальні виконавці	Відмітка про виконання
1	2	3	4	5	6
	Найменування процесу				

Ректор _____ ініціали, прізвище

підпис

_____

дата

Додаток З

Форма плану заходів щодо поліпшення структурного підрозділу

(відокремленого структурного підрозділу)

ПЛАН ЗАХОДІВ З ПОЛІПШЕННЯ

_____

найменування структурного підрозділу (відокремленого структурного підрозділу)

№ п/п	Найменування можливості	Найменування заходу з реалізації можливості	Термін виконання	Відповідальні виконавці	Відмітка про виконання
1	2	3	4	5	6
	Найменування процесу				

Розглянутий на _____

засіданні / раді / нараді найменування структурного підрозділу

від _____ протокол № _____ .

дата засідання / ради / наради № протоколу

Керівник структурного підрозділу _____ ініціали, прізвище

підпис

_____

дата

Додаток И

Форма плану заходів щодо поліпшення процесу

ПЛАН ЗАХОДІВ З ПОЛІПШЕННЯ

_____

найменування процесу

№ п/п	Найменування можливості	Найменування заходу з реалізації можливості	Термін виконання	Відповідальні виконавці	Відмітка про виконання
1	2	3	4	5	6
	Найменування процесу				

Власник процесу _____ ініціали, прізвище

підпис

_____

дата

Додаток І

Форма плану заходів щодо поліпшення СУЯ

ПЛАН ЗАХОДІВ З ПОЛІПШЕННЯ
системи управління якістю
ВНЗ

№ п/п	Найменування можливості	Найменування заходу з реалізації можливості	Термін виконання	Відповідальні виконавці	Відмітка про виконання
1	2	3	4	5	6
	Найменування процесу				

Ректор _____ ініціали, прізвище
підпис

_____
дата

Додаток К

ЗНАННЯ

Найменування знання	Місце зберігання	Відповідальний за поповнення і зберігання	Кому надається доступ до знання	Порядок актуалізації
Паспорт ризиків СП (ВСП)	СП (ВСП)	Керівник СП (ВСП)	Керівники СП (ВСП), співробітники університету (ОСП)	У міру необхідності, 1 раз на рік
Паспорт ризиків процесу СУЯ	Власник процесу	Власник процесу	Керівники СП (ВСП), співробітники університету (ВСП)	У міру необхідності, 1 раз на рік
Паспорт ризиків СУЯ	СУЯиМО	СУЯиМО	Керівники СП (ВСП), співробітники університету (ВСП)	114 У міру необхідності,