

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
КАФЕДРА ЕКОНОМІКИ ТА МЕНЕДЖМЕНТУ

Ольга СЛОБОДЯНЮК
Ольга КІБІК
Вячеслав КОТЛУБАЙ

РИЗИКОЛОГІЯ

Навчально-методичний посібник
для здобувачів третього (освітньо-наукового) рівня вищої освіти
зі спеціальності «Менеджмент»

Одеса
Фенікс
2025

УДК 005.334 (075.8)
С 48

*Рекомендовано навчально-методичною радою
Національного університету «Одеська юридична академія»
(протокол № 7 від 24.06.2025 р.)*

Автори:

Слободянюк Ольга – докторка економічних наук, професорка, професорка кафедри економіки та менеджменту НУ «Одеська юридична академія» (ORCID ID 0000-0003-2678-4707);

Кібік Ольга – докторка економічних наук, професорка, завідувачка кафедри економіки та менеджменту НУ «Одеська юридична академія» (ORCID ID 0000-0001-9587-578X);

Котлубай Вячеслав – кандидат економічних наук, доцент, доцент кафедри економіки та менеджменту Національного університету «Одеська юридична академія» (ORCID ID 0000-0002-4560-7063).

Рецензенти:

Князєва Олена – доктор економічних наук, професорка, в.о. завідувачки кафедри економічної теорії і економіки підприємства Одеського державного аграрного університету;

Слатвінська Марина – доктор економічних наук, професорка, керівниця центру забезпечення якості освіти, завідувачка кафедри фінансів Одеського національного економічного університету.

Слободянюк О., Кібік О., Котлубай В.

С 48 **Ризикологія** : навч.-метод. посіб. для здобувачів третього (освіт.-наук.) рівня вищої освіти зі спец. «Менеджмент» [Електронне видання] / О. Слободянюк, О. Кібік, В. Котлубай ; Нац. ун-т «Одеська юрид. Академія». – Одеса : Фенікс, 2025. – 78 с. URL: <https://hdl.handle.net/11300/30599> ; DOI: 10.32837/11300.30599

ISBN 978-617-8430-84-9

Навчально-методичний посібник відповідає програмі навчальної дисципліни «Ризикологія».

У посібнику викладено зміст навчальної дисципліни за темами лекцій і практичних занять, питання до практичних завдань з курсу, завдання для самостійної роботи, питання для перевірки знань з навчальної дисципліни, теми презентацій і повідомлень, список рекомендованих джерел.

Навчально-методичний посібник призначений для здобувачів вищої освіти, що отримують освіту на третьому (освітньо-науковому) рівні зі спеціальності «Менеджмент».

УДК 005.334 (075.8)

ISBN 978-617-8430-84-9

© О. В. Слободянюк, О. М. Кібік, В. О. Котлубай, 2025

ЗМІСТ:

ВСТУП	4
ТЕМА 1. ТЕОРЕТИЧНІ ОСНОВИ РИЗИКУ ТА НЕВИЗНАЧЕНОСТІ	7
ТЕМА 2. МЕТОДИ ОЦІНКИ ТА ВИМІРЮВАННЯ РИЗИКІВ	14
ТЕМА 3. МОДЕЛІ ТА СТРАТЕГІЇ УПРАВЛІННЯ РИЗИКАМИ	27
ТЕМА 4. РИЗИКИ В ЕКОНОМІЧНИХ СИСТЕМАХ.....	38
ТЕМА 5. КІБЕРРИЗИКИ ТА РИЗИКИ В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ	44
ТЕМА 6. РИЗИКИ СТАЛОГО РОЗВИТКУ	53
ТЕМА 7. РИЗИКИ В УМОВАХ ГЛОБАЛІЗАЦІЇ ТА МІЖНАРОДНОЇ ДІЯЛЬНОСТІ.....	60
ПИТАННЯ ДЛЯ ПІДГОТОВКИ ДО ЕКЗАМЕНУ	68
РЕКОМЕНДОВАНИЙ ПЕРЕЛІК ДЖЕРЕЛ.....	71

ВСТУП

Дисципліна «Ризикологія» вивчається здобувачами вищої освіти третього (освітньо-наукового) рівня за освітньо-науковою програмою «Менеджмент». Дана дисципліна є невід'ємною частиною професійної підготовки майбутніх фахівців у сфері управління, оскільки забезпечує формування комплексних знань про природу ризиків та методи управління ними в сучасних умовах невизначеності та динамічних змін.

Метою викладання навчальної дисципліни «Ризикологія» є формування у здобувачів вищої освіти системних знань про теоретичні основи ризику та невизначеності, практичних навичок ідентифікації, оцінки та управління ризиками в різних сферах діяльності, а також розвиток компетентностей щодо прийняття обґрунтованих управлінських рішень в умовах ризику та невизначеності.

Коротким описом предметної сфери є вивчення теоретичних засад ризикології як науки, методологічних підходів до ідентифікації та оцінки ризиків, сучасних моделей та стратегій ризик-менеджменту, специфіки ризиків у різних економічних системах, кіберризиків та ризиків інформаційних технологій, ризиків сталого розвитку, а також особливостей управління ризиками в умовах глобалізації та міжнародної діяльності.

Оволодіння курсом «Ризикологія» передбачає читання лекцій, проведення практичних занять, виконання самостійної роботи та складання екзамену. Особлива увага приділяється розвитку навичок критичного мислення при аналізі ризикових ситуацій, розвитку здатності до системного підходу в управлінні ризиками, формуванню практичних компетентностей використання сучасних інструментів ризик-менеджменту та вмінню адаптувати стратегії управління ризиками до специфіки різних сфер діяльності.

Згідно з вимогами освітньо-професійної програми після вивчення дисципліни «Ризикологія» здобувачі повинні:

- знати специфіку теоретичних основ ризику та невизначеності, класифікацію ризиків, методологічні підходи до їх ідентифікації та оцінки, сучасні моделі та стратегії управління ризиками, особливості ризиків у різних економічних системах та сферах діяльності;
- володіти основними методами якісного та кількісного аналізу ризиків, інструментами моделювання та прогнозування ризикових ситуацій, техніками розробки стратегій ризик-менеджменту, навичками використання спеціалізованого програмного забезпечення для управління ризиками;
- володіти навичками самостійної роботи з науковою літературою з питань ризикології, аналізу практичних кейсів управління ризиками, проведення досліджень ризикових факторів у різних галузях, підготовки аналітичних звітів та рекомендацій щодо мінімізації ризиків;
- застосовувати на практиці знання про методи ідентифікації, оцінки та управління ризиками для вирішення конкретних управлінських завдань,

розробки стратегій ризик-менеджменту для організацій різних типів та масштабів, прийняття обґрунтованих рішень в умовах невизначеності;

– використовувати спеціалізоване програмне забезпечення для моделювання ризиків, методи статистичного аналізу для оцінки ризикових факторів, сучасні інформаційні технології для моніторингу та контролю ризиків, міжнародні стандарти та найкращі практики у сфері управління ризиками.

Технологічною основою викладання є аудиторне навчання з інтеграцією дистанційних освітніх технологій. Використовуються методи лекцій, практичних занять (аналіз наукових публікацій, підготовка оглядових статей, презентації дослідницьких проєктів, аналіз кейсів, підготовка рефератів), консультацій та самостійної роботи. Практичні завдання спрямовані на формування дослідницьких і експертно-аналітичних компетентностей, розвиток наукового мислення та здатності проводити самостійні дослідження в умовах багатфакторної невизначеності. Самостійна робота здобувачів базується на індивідуальному науковому дослідженні та колективному обговоренні результатів.

Дисципліна формує поглиблені методологічні компетенції щодо підготовки до самостійної наукової діяльності.

Оцінювання результатів навчання здобувачів вищої освіти щодо опанування навчальної дисципліни здійснюється відповідно до Положення про організацію освітнього процесу в Національному університеті «Одеська юридична академія».

Критерії оцінювання знань здобувачів:

Оцінка виставляється за національною чотирибальною шкалою: «відмінно», «добре», «задовільно», «незадовільно». При оцінці за основу слід брати повноту і правильність виконання завдань.

1. Оцінка «5» (відмінно) ставиться в тому разі, коли відповідь здобувача правильна, повна, послідовна, логічна; здобувач впевнено володіє фактичним матеріалом з усього курсу, вміє застосовувати його щодо конкретно поставлених завдань.

2. Оцінка «4» (добре) ставиться в тому разі, коли відповідь правильна, послідовна, логічна, але здобувач допускає у викладі окремі незначні пропуски фактичного матеріалу вміє застосувати його щодо конкретно поставлених завдань.

3. Оцінка «3» (задовільно) ставиться у тому разі, коли здобувач володіє більшою частиною фактичного матеріалу, але викладає його не досить послідовно і логічно, допускає істотні пропуски у відповіді, невірно формулює основні теоретичні положення та причинно-наслідкові зв'язки.

4. Оцінка «2» (незадовільно) ставиться в тому разі, коли здобувач виявляє незнання більшої частини фактичного матеріалу або здобувач відмовляється відповідати на поставлені питання.

Шкала оцінювання: національна та ECTS

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		Екзамен	залік
90-100	A	Відмінно	зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
1-59	Fx	Незадовільно	не зараховано
1-34	F		

ТЕМА 1. ТЕОРЕТИЧНІ ОСНОВИ РИЗИКУ ТА НЕВИЗНАЧЕНОСТІ

Лекційні питання:

Мета вивчення/ роботи: ознайомлення з філософськими та методологічними засадами ризикології, формування системного розуміння природи ризику та невизначеності, засвоєння концептуальних підходів до дослідження ризикових явищ у сучасному науковому контексті

1. Філософські та методологічні основи ризикології як науки.
2. Концептуальні підходи до визначення ризику та невизначеності.
3. Еволюція наукових поглядів на природу ризику.
4. Системний підхід до дослідження ризикових явищ.

Зміст лекції

Ризикологія як наукова дисципліна виникла на стику філософії, економіки, соціології, математики, психології та інших галузей знань, що визначає її міждисциплінарний характер і високу актуальність для фахівців у сфері менеджменту, які мають опанувати комплексне розуміння сучасних управлінських викликів [1, 2, 3]. Філософські підвалини ризикології ґрунтуються на базових категоріях можливості та дійсності, необхідності та випадковості, детермінізму та індетермінізму, розроблених у працях класиків філософії, від Аристотеля (384–322 до н.е.) до Іммануїла Канта (1724–1804).

Онтологічний аспект ризику пов'язаний з об'єктивним існуванням невизначеності в природі та суспільстві. Дане питання аналізували філософи науки, зокрема Карл Поппер (1902–1994) у монографії «Логіка наукового відкриття» (1934), де він обґрунтував принцип фальсифікації та продемонстрував, що наукове знання завжди включає елемент невизначеності. Гносеологічний аспект стосується пізнання та інтерпретації ризикових феноменів [11].

Епістемологічні традиції вивчення ризику охоплюють позитивістську, інтерпретативну та критичну парадигми. Позитивістський підхід, ініційований Огюстом Контом (1798–1857), спрямований на об'єктивне вимірювання ризиків за допомогою статистичних методів. Інтерпретативна традиція, розроблена Максом Вебером (1864–1920), акцентує увагу на розумінні суб'єктивного значення ризикових дій. Критична традиція, представлена Франкфуртською школою, розглядає ризик у контексті соціальних відносин влади та нерівності.

Методологічні засади ризикології включають системний, структурно-функціональний, діалектичний та синергетичний підходи [1, 2]. Системний підхід трактує ризик як властивість складних систем, що має значення для управлінських досліджень, оскільки організації є складними соціально-технічними системами. Структурно-функціональний підхід, розроблений Талкоттом Парсонсом (1902–1979), аналізує взаємозв'язки елементів ризикових ситуацій та їхню функціональну роль у системі. Діалектичний

підхід вивчає суперечності та розвиток ризикових процесів крізь призму законів діалектики Георга Вільгельма Фрідріха Гегеля (1770–1831).

Синергетичний підхід, запропонований Германом Хакеном (1927–2024), фокусується на самоорганізації та нелінійності ризикових систем. Такий підхід є релевантним для розуміння емерджентних властивостей організаційних ризиків, коли поведінка системи не може бути передбачена на основі характеристик окремих елементів. Епістемологічна специфіка ризикології полягає в інтеграції раціональних та ірраціональних аспектів пізнання, а також у поєднанні кількісних і якісних методів дослідження, що відповідає вимогам сучасних міждисциплінарних студій у менеджменті [1, 3, 4].

Праксеологічний вимір ризикології стосується практичного застосування знань про ризик в управлінській діяльності. Людвіг фон Мізес (1881–1973) у фундаментальній праці «Людська діяльність» (1949) розвинув праксеологічну теорію, яка розглядає людську поведінку як цілеспрямовану в умовах невизначеності. Така концепція має значення для менеджерів, оскільки управлінські рішення приймаються в умовах неповної інформації та ризику.

Концептуалізація ризику та невизначеності є центральним завданням ризикології та має значення для формування наукового мислення майбутніх докторів філософії в галузі менеджменту. У науковій літературі представлено різноманітні підходи до дефініції цих понять, що відображає їхню складність та багатовимірність [1, 2, 3, 4].

Класичний підхід, викладений Френком Найтом (1885–1972) у праці «Ризик, невизначеність та прибуток» (1921), розрізняє ризик як вимірювану невизначеність і власне невизначеність як невимірювану категорію [5]. Найт аргументував, що ризик можна кількісно оцінити статистичними методами на основі історичних даних, тоді як справжня невизначеність не піддається такій оцінці. Розрізнення стало основою для розвитку теорії управління ризиками та є фундаментальним для розуміння меж застосовності аналітичних інструментів у менеджменті [5].

Джон Мейнард Кейнс (1883–1946) у «Загальній теорії зайнятості, відсотка та грошей» (1936) розвинув ідею фундаментальної невизначеності, яка не зводиться до об'єктивних ймовірностей. Кейнс підкреслив роль суб'єктивних очікувань та «animal spirits» у прийнятті економічних рішень, що стосується управлінської практики в турбулентному середовищі.

Сучасні концепції розширюють таке розуміння, інтегруючи суб'єктивні аспекти сприйняття ризику. Ульріх Бек (1944–2015) у монографії «Суспільство ризику» (1986) запропонував соціологічну концепцію ризику як продукту модернізації, що характеризується рефлексивністю та глобальністю [6]. Бек продемонстрував, що сучасні ризики мають нову природу порівняно з традиційними загрозами та вимагають нових форм управління.

Об'єктивістський підхід інтерпретує ризик як об'єктивну характеристику реальності, вимірювану статистичними методами. Такий підхід домінує в технічних науках та традиційному ризик-менеджменті. Його представник

Чарлз Перроу (1925–2019) у праці «Нормальні аварії» (1984) аналізував ризики складних технічних систем через призму теорії систем та організаційної теорії.

Суб'єктивістський підхід акцентує роль індивідуального сприйняття ризикових ситуацій. Даний напрям розвивали представники поведінкової економіки, зокрема Деніел Канеман (1934–2024) та Амос Тверські (1937–1996) у теорії перспектив (1979), яка виявила систематичні відхилення від раціональної поведінки в умовах ризику [7]. Дані дослідження є фундаментальними для розуміння психологічних аспектів управлінських рішень [7].

Конструктивістський підхід розглядає ризик як соціальний конструкт, сформований культурними, соціальними та інституційними процесами. Мері Дуглас (1921–2007) та Аарон Вільямс (1930–1993) у праці «Ризик та культура» (1982) продемонстрували, як культурні цінності та соціальні інститути впливають на сприйняття ризиків.

Інтегративний підхід поєднує об'єктивні та суб'єктивні аспекти ризику. Шейла Ясановф (нар. 1944) у своїх дослідженнях науки та технологічної політики розвинула концепцію «co-production» науки та суспільства, ілюструючи взаємозв'язок технічної експертизи та соціальних процесів у формуванні уявлень про ризик.

Невизначеність класифікується за різними критеріями: алеаторна (стохастична) пов'язана з випадковими процесами; епістемічна виникає через обмеженість знань; редукована може бути зменшена дослідженнями, тоді як нередукована є фундаментальною властивістю складних систем; кількісна піддається математичній формалізації, а якісна вимагає експертної оцінки.

Історичний розвиток уявлень про ризик ілюструє еволюцію від інтуїтивного розуміння до складних наукових теорій. Розуміння цієї еволюції сприяє кращому осмисленню сучасних дискусій у ризикології [2, 3].

У стародавніх цивілізаціях ризик асоціювався з долею чи божественною волею. Давньогрецькі філософи розрізняли «т्यूхе» (випадок) та «ананке» (необхідність). Аристотель (384–322 до н.е.) у «Нікомаховій етиці» розглядав прийняття рішень в умовах невизначеності через концепцію «фронезису» (практичної мудрості), що резонує з сучасними теоріями управлінського мислення.

Середньовічна думка пов'язувала ризик з моральними та релігійними категоріями. Тома Аквінський (1225–1274) у «Сумі теології» аналізував ризик у контексті справедливої ціни та етики торгівлі.

Епоха Відродження та розвиток торгівлі призвели до систематичних підходів до оцінки ризиків. Лука Пачолі (близько 1447–1517) у трактаті «Сума арифметики, геометрії, пропорцій та пропорційності» (1494) описав подвійну бухгалтерію для оцінки фінансових ризиків.

У XVII–XVIII століттях розвивалася теорія ймовірностей. Блез Паскаль (1623–1662) та П'єр де Ферма (1607–1665) у листуванні 1654 року заклали основи теорії ймовірностей. Якоб Бернуллі (1655–1705) у «Ars Conjectandi»

(1713) сформулював закон великих чисел. Абрагам де Муавр (1667–1754) у «Доктрині шансів» (1718) розвинув нормальний розподіл. Томас Байєс (близько 1701–1761) розробив байєсівську теорему. П'єр-Симон Лаплас (1749–1827) систематизував теорію у «Аналітичному есе про ймовірності» (1812).

XIX століття позначене формуванням статистичних методів. Карл Фрідріх Гаусс (1777–1855) розвинув методи статистичного аналізу. Адольф Кетле (1796–1874) застосував статистику до соціальних явищ. Френсіс Гальтон (1822–1911) розробив кореляційний аналіз.

XX століття принесло революційні зміни. Теорія корисності Джона фон Неймана (1903–1957) та Оскара Моргенштерна (1902–1977) у «Теорії ігор та економічної поведінки» (1944) створила математичні основи для аналізу рішень у ризику. Гаррі Марковіц (1927–2023) у «Виборі портфеля» (1952) розвинув теорію портфеля.

Поведінкова економіка, розроблена Деніелом Канеманом та Амосом Тверські, змінила підходи до ризику. Теорія перспектив (1979) виявила відхилення від раціональності [7].

Сучасний етап характеризується міждисциплінарністю та урахуванням психологічних факторів. Нассім Ніколас Талеб (нар. 1960) у «Одурений випадковістю» (2001) та «Чорний лебідь» (2007) акцентував рідкісні події з великими наслідками [8]. Деніел Канеман у «Мисленні швидкому та повільному» (2011) узагальнив досягнення поведінкової економіки.

Системний підхід у ризикології базується на розумінні ризику як властивості складних систем, що виникає від взаємодії елементів та зовнішнього середовища. Такий підхід є ключовим для менеджерів, оскільки організації є складними адаптивними системами в динамічному середовищі [10].

Теоретичні основи закладені Людвігом фон Берталанфі (1901–1972) у «Загальній теорії систем» (1968), де визначено систему як комплекс взаємодіючих елементів з принципами холізму, емерджентності, ієрархічності та цілеспрямованості [10]. Норберт Вінер (1894–1964) у «Кібернетиці» (1948) розвинув концепції зворотного зв'язку та самоорганізації. Джей Форрестер (1918–2016) розробив системну динаміку, з працями «Промислова динаміка» (1961) та «Динаміка міста» (1969).

Ризикова система характеризується цілісністю, структурованістю, ієрархічністю, динамічністю, адаптивністю та емерджентністю. Питер Сенге (нар. 1947) у «П'ятій дисципліні» (1990) розвинув концепцію організації, що навчається, та системні архетипи.

Системний аналіз ризиків включає ідентифікацію елементів, взаємозв'язків, зворотних зв'язків. Генетичний аспект вивчає еволюцію ризиків, телеологічний – стратегії в невизначеності.

Системна методологія виявляє синергетичні ефекти. Хайман Мінські (1919–1996) у гіпотезі фінансової нестабільності показав генерацію системних криз. Підхід включає аналіз адаптивних механізмів та резильєнтності,

розробленої Кроуфордом Холлінгом (1930–2019) в екології, з застосуванням в організаційних дослідженнях [9].

Складність ризиків вимагає інтеграції системної теорії, теорії складності та мережевого аналізу, що є essential для підготовки докторів філософії в менеджменті [4, 10].

Ризикологія як міждисциплінарна наука надає менеджерам концептуальний і методологічний інструментарій для ефективного управління в умовах невизначеності [1, 2, 3, 4]. Філософські основи, від категорій Аристотеля (384–322 до н.е.) до принципу фальсифікації Карла Поппера (1902–1994), розкривають онтологічну та гносеологічну природу ризику, підкреслюючи його невід’ємність у процесах прийняття рішень [11]. Концептуальні підходи, включаючи класичне розрізнення ризику та невизначеності Френка Найта (1921), соціологічну теорію суспільства ризику Ульріха Бека (1986) та поведінкові моделі Деніела Канемана і Амоса Тверські (1979), дозволяють аналізувати ризики з об’єктивної, суб’єктивної та соціокультурної перспектив [5, 6, 7]. Історичний розвиток уявлень про ризик, від теорії ймовірностей (Паскаль, Ферма, XVII ст.) до концепції "чорних лебедів" Нассім Ніколаса Талеба (2007), ілюструє еволюцію підходів до управління невизначеністю [8]. Системний підхід, заснований на працях Людвіга фон Берталанфі (1968) та Кроуфорда Холлінга (1973), трактує організації як складні адаптивні системи, де ризики виникають через взаємодію елементів і зовнішнього середовища [9, 10].

Для управлінської практики ці концепції мають безпосереднє застосування: розуміння фундаментальної невизначеності (Кейнс, 1936) сприяє розробці гнучких стратегій; поведінкові теорії допомагають уникати когнітивних упереджень [7]; концепція резильєнтності забезпечує стійкість організацій до криз [9].

Тому здобувачам освітньо-наукового рівня пропонується інтегрувати дані знання в дослідження, аналізуючи сучасні виклики, такі як кіберризики, кліматична нестабільність чи геополітичні загрози, через системний і синергетичний підходи [9]. Розробка інноваційних моделей ризик-менеджменту сприятиме підвищенню адаптивності організацій у турбулентному середовищі, що є ключовим завданням для майбутніх докторів філософії в менеджменті.

ПИТАННЯ ДО ПРАКТИЧНОГО ЗАНЯТТЯ

1. Філософські категорії в управлінні ризиками.
2. Ризик та невизначеність. Розгляд класичного підходу.
3. Суспільство ризику та сучасні виклики.
4. Поведінкові аспекти ризику.
5. Еволюція поглядів на ризик.
6. Системний підхід до управління ризиками.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ:

Обрати реальну організацію (наприклад, технологічний стартап, виробниче підприємство, фінансова установа чи міжнародна корпорація) та провести аналіз її ризиків, застосовуючи теоретичні концепції ризикології, розглянуті в лекції.

Етапи виконання:

1. Визначте щонайменше три ключові ризики, з якими стикається організація (наприклад, фінансові, операційні, репутаційні чи кіберризики). Розрізняйте вимірюваний ризик і невизначеність, спираючись на концепцію Френка Найта (1921).

2. Виберіть один із концептуальних підходів до ризику (об'єктивістський, суб'єктивістський, конструктивістський або інтегративний) для аналізу ідентифікованих ризиків. Обґрунтуйте вибір, посилаючись на відповідних авторів (наприклад, Найт, 1921; Канеман і Тверські, 1979; Бек, 1986; Ясанофф).

3. Оцініть, як еволюція уявлень про ризик (наприклад, від теорії ймовірностей Паскаля і Ферма до концепції «чорного лебедя» Талеба, 2007) може пояснити природу ідентифікованих ризиків.

4. Використовуючи принципи системного підходу (фон Берталанфі, 1968), опишіть організацію як складну систему, ідентифікуючи ключові елементи, зворотні зв'язки та емерджентні властивості, що впливають на ризики.

5. Запропонуйте три конкретні управлінські заходи для підвищення резильєнтності організації до ідентифікованих ризиків, спираючись на концепцію резильєнтності Кроуфорда Холлінга (1973).

Зробіть у формі письмового звіту або презентації із чітким викладом усіх етапів.

Питання для самоконтролю:

1. Які ключові філософські категорії (можливість/дійсність, необхідність/випадковість) лежать в основі ризикології, і як вони пов'язані з управлінськими рішеннями?

2. У чому полягає відмінність між ризиком і невизначеністю за Френком Найтом (1921), і як це розрізнення впливає на розробку управлінських стратегій?

3. Як еволюція уявлень про ризик від теорії ймовірностей (XVII ст.) до поведінкової економіки (XX ст.) змінила підходи до управління ризиками?

4. Що таке системний підхід до ризиків, і як принципи холізму та емерджентності (фон Берталанфі, 1968) застосовуються до аналізу організаційних ризиків?

5. У чому полягає відмінність між ризиком та невизначеністю в економічному аналізі?

6. Які методологічні підходи використовуються для дослідження ризикових явищ у сучасній економіці?

7. Як змінювалися наукові уявлення про природу ризику в різні історичні періоди?

8. У чому суть системного підходу до аналізу ризиків та які його переваги?

ТЕМИ ПРЕЗЕНТАЦІЙ ТА ПОВІДОМЛЕНЬ:

1. Філософські основи ризикології від Аристотеля до Поппера.
2. Концепція «суспільства ризику» Ульріха Бека та її значення для сучасного менеджменту.
3. Еволюція теорії ймовірностей від Паскаля і Ферма до сучасних моделей ризик-менеджменту.
4. Резильєнтність організацій у турбулентному середовищі та застосування концепції Кроуфорда Холлінга.

Література:

1. Вітлінський В. В., Великоіваненко Г. І. Ризикологія в економіці та підприємстві : монографія. Київ : КНЕУ, 2004. 480 с.
2. Степанов В. М. Ризикологія: основи, додатки, тезаурус. Одеса : ІПРЕІ НАН України, 2019. 292 с.
3. Бугріменко Р. М., Смірнова П. В. Ризикологія : навч. посіб. Харків : Форт, 2022. 148 с.
4. Герасименко О. М. Ризик-орієнтоване управління в системі економічної безпеки підприємства : дис. ... д-ра екон. наук : 21.04.02. Київ : Університет «КРОК», 2021. 667 с.
5. Knight, F. H. Risk, Uncertainty and Profit. Boston: Houghton Mifflin, 1921. 381 p. (Available via: <https://archive.org/details/riskuncertainty00knig>)
6. Beck, U. Risk Society: Towards a New Modernity. London: Sage Publications, 1992. 260 p. (Original: Risikogesellschaft, 1986) <http://www.riversimulator.org/Resources/Anthropology/RiskSociety/RiskSocietyTowardsAnewModernity1992Beck.pdf>
7. Kahneman, D., & Tversky, A. Prospect Theory: An Analysis of Decision under Risk. Econometrica, 1979, Vol. 47, No. 2, pp. 263–291. (DOI: 10.2307/1914185) <https://www.jstor.org/journal/econometrica>
8. Taleb, N. N. The Black Swan: The Impact of the Highly Improbable. New York: Random House, 2007. 400 p.
9. Holling, C. S. Resilience and Stability of Ecological Systems. Annual Review of Ecology and Systematics, 1973, Vol. 4, pp. 1–23. (DOI: 10.1146/annurev.es.04.110173.000245)
10. Von Bertalanffy, L. General System Theory: Foundations, Development, Applications. New York: George Braziller, 1968. 295 p.
11. Popper, K. The Logic of Scientific Discovery. London: Routledge, 2002 (Original: Logik der Forschung, 1934). 544 p.

ТЕМА 2. МЕТОДИ ОЦІНКИ ТА ВИМІРЮВАННЯ РИЗИКІВ

Лекційні питання:

Мета вивчення/ роботи: ознайомлення з сучасними методологічними підходами до кількісної та якісної оцінки ризиків, формування практичних навичок застосування різноманітних аналітичних інструментів для вимірювання та моделювання ризикових ситуацій у управлінській діяльності, розвиток компетентностей у використанні цифрових технологій для комплексного аналізу ризиків на рівні, необхідному для майбутніх докторів філософії в галузі менеджменту.

1. Кількісні методи оцінки ризику.
2. Якісні методи аналізу ризиків.
3. Інтегровані методи оцінки ризиків.
4. Сучасні цифрові технології в оцінці ризиків.

Зміст лекції

Кількісні методи оцінки ризику становлять основу сучасного ризик-менеджменту та базуються на математичному апараті теорії ймовірностей, математичної статистики, теорії ігор та оптимізації [1, 2, 3, 4, 5, 6].

Статистичні методи оцінки ризику базуються на аналізі історичних даних та екстраполяції трендів у майбутнє [4, 6, 7]. Основоположником статистичного підходу до аналізу ризиків вважається Карл Пірсон (1857-1936), який розробив хи-квадрат тест (тест χ^2) та заклав основи сучасної математичної статистики у роботі «Грамматика науки» (1892) [7]. Рональд Фішер (1890-1962) у працях «Статистичні методи для дослідників» (1925) та «Дизайн експериментів» (1935) розвинув основи статистичного висновку та аналізу варіансів, що стали фундаментальними для оцінки ризиків.

Дисперсія як міра ризику була введена Гаррі Марковіцем у його піонерській роботі з теорії портфеля:

$$Var(X) = E[(X - \mu)^2], \quad \sigma = \sqrt{Var(X)}$$

Стандартне відхилення σ стало основною мірою волатильності та ризику у фінансах.

Коефіцієнт варіації $CV = \sigma/\mu$ дозволяє порівнювати ризикованість різних активів з різними рівнями доходності, забезпечуючи нормалізовану міру ризику.

Показники асиметрії та ексцесу характеризують форму розподілу, де асиметрія вимірює симетричність розподілу та вірогідність односторонніх екстремальних подій, а ексцес визначає «товщину хвостів» розподілу та ймовірність екстремальних відхилень.

Асиметрія (Skewness) та ексцес (Kurtosis) характеризують форму розподілу та вірогідність екстремальних подій [6, 7].

$$\text{Асиметрія (Skewness)} = \frac{E[(X-\mu)^3]}{\sigma^3},$$

$$\text{Ексцес (Kurtosis)} = \frac{E[(X-\mu)^4]}{\sigma^4}$$

Value at Risk (VaR) - один із найпоширеніших методів оцінки ринкового ризику, розроблений у J.P.Morgan у 1990-х роках під керівництвом Тіла Гулдіамалі. VaR відповідає на питання: «Яку максимальну втрату може зазнати портфель з імовірністю α за період часу t ?»

Математично VaR визначається як квантиль розподілу прибутків:

$$P(\Delta P \leq -VaR_\alpha) = \alpha,$$

де α - рівень довіри (зазвичай 1%, 5% або 10% [4, 6, 8, 9]).

Філіп Жоріон (нар. 1955) у роботі "Value at Risk: Новий орієнтир для управління фінансовими ризиками" (2006) систематизував методи розрахунку VaR: параметричний метод, історичне моделювання та метод Монте-Карло [8]. Кожен метод має свої переваги та обмеження залежно від характеристик даних та горизонту планування. Параметричний метод припускає нормальність розподілу доходностей. Історичне моделювання використовує емпіричний розподіл історичних доходностей без припущень про теоретичний розподіл. Метод Монте-Карло генерує велику кількість випадкових сценаріїв на основі стохастичних моделей [4, 5, 6, 7, 8, 9].

Conditional Value at Risk (CVaR) або Expected Shortfall, запропонований Р. Тайроном Рокафеларом (нар. 1935), усуває деякі недоліки VaR та вимірює очікувану втрату за умови, що втрата перевищує VaR:

$$CVaR_\alpha = E[L|L \geq VaR_\alpha].$$

Імітаційне моделювання Монте-Карло, розроблене Станіславом Уламом (1909-1984) та Джоном фон Нейманом у 1940-х роках для потреб Манхеттенського проєкту, знайшло широке застосування в оцінці ризиків [4, 5, 6, 7]. Метод дозволяє моделювати складні стохастичні процеси через генерацію великої кількості випадкових сценаріїв. Для управлінських застосувань особливо важливими є методи зниження варіансу: стратифіковане семплування, антитетичні змінні, контрольні змінні.

Екстремальна теорія значень (Extreme Value Theory), розвинена Емільм Жюлем Гумбелем (1891-1966), фокусується на моделюванні рідкісних подій з великими наслідками. Теорема Фішера-Тіппетта-Гнеденка встановлює, що розподіл максимальних значень збігається до одного з трьох типів екстремальних розподілів: Гумбела, Фреше або Вейбулла і є критичним значенням для оцінки операційних ризиків та природних катастроф.

Копули-функції, вперше описані Абе Скларом (1916-1994) у 1959 році, дозволяють моделювати залежність між випадковими величинами незалежно від їх маргінальних розподілів. Теорема Склара стверджує, що будь-який багатовимірний розподіл може бути представлений через маргінальні

розподіли та копулу, що описує структуру залежності. Їх застосовують при визначенні портфельного ризику та кредитних деривативів [6, 7].

Стохастичні процеси широко використовуються для моделювання динаміки ризикових факторів. Геометричне броунівське рух, запропоноване Луї Башельє (1870-1946) у дисертації «Теорія спекуляцій» (1900), стало основою моделі Блека-Шоулза. Іто Кійосі (1915-2008) розвинув стохастичне числення для роботи з диференціальними рівняннями, що містять випадкові процеси.

Модель GBM для ціни активу [6, 7, 10] : $dS_t = \mu S_t dt + \sigma S_t dW_t$

Якісні методи аналізу ризиків відіграють фундаментальну роль у комплексній оцінці ризикових ситуацій, особливо коли кількісні дані відсутні або недостатні для статистичного аналізу. Так багато організаційних, стратегічних та інноваційних ризиків не піддаються прямому кількісному вимірюванню, але потребують системного аналізу та експертної оцінки [4, 5, 13].

Експертний аналіз базується на використанні знань та досвіду кваліфікованих спеціалістів для оцінки ризиків. Теоретичні основи експертних методів були закладені у роботах Нормана Далкі (1918-2003) з корпорації RAND, який у 1950-х роках розробив метод Дельфі для структурованого збору та аналізу експертних думок. Метод названий на честь давньогрецького Дельфійського оракула та характеризується анонімністю експертів, багатоетапністю опитування та зворотним зв'язком.

Олаф Хелмер (1910-2011) та Теодор Гордон (1930-2016) у роботі «Звіт про довгострокове прогнозування» (1964) систематизували принципи методу Дельфі: структурованість комунікації, анонімність експертів, ітеративність процесу та статистична обробка групової відповіді [13]. Модифікації методу включають політичний Дельфі, нечіткий Дельфі та гібридний Дельфі з елементами очного обговорення.

Ранжування та бальні оцінки дозволяють систематизувати якісну інформацію та забезпечити порівняльність різних ризиків. Томас Сааті (1926-2017) розробив метод аналітичної ієрархії, викладений у роботі «Прийняття рішень для лідерів» (1980). Метод базується на парних порівняннях елементів ієрархії та використанні власних векторів матриць порівнянь для визначення пріоритетів [4, 13].

Індекс консистентності (CI):

$$CI = \frac{\lambda_{max} - n}{n - 1}$$

де λ_{max} - максимальне власне значення матриці порівнянь, а n - розмірність матриці, дозволяє оцінити узгодженість експертних суджень.

Відношення консистентності $CR = CI/RI$, де RI - випадковий індекс, повинно не перевищувати 0,10 для прийнятної консистентності.

Сценарний аналіз, розвинений у корпорації Shell під керівництвом П'єра Вака (нар. 1930) у 1970-х роках, дозволяє досліджувати різні варіанти розвитку подій та їх вплив на організацію. Класична робота Кеес ван дер Хейдена (нар. 1938) «Сценарії: мистецтво стратегічної розмови» (1996) описує процес розробки сценаріїв як інструменту стратегічного планування в умовах невизначеності.

Розрізняють експлораторні сценарії (що може статися?) та нормативні сценарії (як досягти бажаного стану?). Морфологічний аналіз, розроблений Фріцем Цвікі (1898-1974), дозволяє систематично конструювати сценарії через комбінування різних значень ключових змінних.

SWOT-аналіз (Strengths, Weaknesses, Opportunities, Threats), приписуваний Альберту Хамфрі (1926-2005) зі Стенфордського дослідницького інституту, є одним із найпоширеніших інструментів стратегічного аналізу [4, 6, 13]. Хоча метод часто критикують за поверховість, його модифікації, такі як TOWS-матриця (матриця стратегій) Хайнца Вайгріха (1922-1999), дозволяють розробляти стратегічні альтернативи на основі комбінування внутрішніх та зовнішніх факторів [13].

Аналіз кореневих причин (Root Cause Analysis, RCA) фокусується на виявленні фундаментальних причин ризикових подій. Сакічі Тойода (1867-1930), засновник Toyota Motor Corporation, розробив техніку «5 чому» (5 Whys), яка передбачає послідовне запитання «чому?» для поглиблення аналізу причин [4, 13]. Іширо Ішікава (1915-1989) створив діаграму «риб'ячий скелет» (діаграма Ішікави), яка систематизує потенційні причини проблем за категоріями: люди, методи, матеріали, машини, вимірювання, середовище.

Дерева подій та дерева відмов є графічними методами аналізу причинно-наслідкових зв'язків. Дерево відмов (Fault Tree Analysis, FTA), розроблене Г.А. Вотсоном у Bell Telephone Laboratories у 1961 році для аналізу систем контролю запуску балістичних ракет Minuteman, використовує дедуктивний підхід «зверху вниз» для аналізу можливих причин небажаної події [4, 13].

Дерево подій (Event Tree Analysis, ETA) використовує індуктивний підхід «знизу вгору», починаючи з ініціюючої події та аналізуючи можливі наслідки через ланцюжок бар'єрних функцій. Ймовірність кінцевого сценарію розраховується як добуток ймовірностей спрацювання/неспрацювання бар'єрів [13].

$$P(\text{сценарію}) = \sum_{i=1}^n P(B_i)$$

де $P(B_i)$ — ймовірність спрацювання або відмови бар'єру.

Методи нечіткої логіки, розроблені Лотфі Задехом (1921-2017) у роботі «Нечіткі множини» (1965), дозволяють працювати з неточною та суб'єктивною інформацією. Нечітка логіка особливо корисна для моделювання лінгвістичних змінних типу «високий ризик», «середня ймовірність»,

«критичний вплив». Нечіткі числа дозволяють представити невизначеність у формі трикутних, трапецієподібних або гаусових функцій належності.

Інтегровані методи оцінки ризиків поєднують переваги кількісних та якісних підходів, забезпечуючи більш комплексне та всебічне розуміння ризикових ситуацій [1, 2, 3, 4, 5, 6, 11, 12, 14]. Сучасні організаційні ризики мають багатовимірний характер та потребують міждисциплінарного підходу до аналізу [5, 14]. Розвиток інтегрованих методів відображає еволюцію ризик-менеджменту від фрагментарних підходів до холістичного управління ризиками [5, 11, 14].

Інтегрований ризик-менеджмент (Enterprise Risk Management, ERM) як концепція сформувався у 1990-х роках під впливом корпоративних скандалів та фінансових криз [5, 11]. Фундаментальною роботою в цій сфері стала модель COSO ERM, розроблена Комітетом спонсорських організацій Комісії Трідвея (Committee of Sponsoring Organizations of the Treadway Commission) під керівництвом Джеймса Трідвея молодшого (нар. 1935) [11].

Модель COSO ERM, оновлена у 2017 році, визначає ризик-менеджмент як процес, що здійснюється радою директорів, менеджментом та іншими працівниками організації у стратегічному контексті та спрямований на ідентифікацію потенційних подій, управління ризиками та забезпечення розумної впевненості у досягненні організаційних цілей. Модель включає п'ять взаємопов'язаних компонентів: управління та культура, стратегія та постановка цілей, виконання, огляд та ревізія, інформація, комунікація та звітність [5, 11].

ISO 31000:2018 «Управління ризиками - Настанови» представляє міжнародний стандарт, розроблений Міжнародною організацією стандартизації [4, 5, 12, 14]. Стандарт визначає ризик як «вплив невизначеності на цілі» та пропонує принципи ефективного управління ризиками: інтеграція, структурованість та всеосяжність, адаптованість, включеність, динамічність, найкраща доступна інформація, людські та культурні фактори, постійне вдосконалення.

Процес управління ризиками згідно з ISO 31000 включає: встановлення контексту, оцінку ризиків (ідентифікація, аналіз, оцінювання), обробку ризиків, моніторинг та огляд, комунікацію та консультації. Стандарт забезпечує загальну мову для управління ризиками у різних секторах та юрисдикціях [4, 5, 12, 14].

Багатокритеріальний аналіз рішень (Multiple Criteria Decision Analysis, MCDA) дозволяє враховувати множинні, часто конфліктуючі критерії при оцінці ризиків. Бернард Руа (1934-2017) у роботах з школи ELECTRE (Elimination and Choice Translating Reality) розробив методи, що базуються на відношеннях переваги та несумісності між альтернативами.

Жан-Клод Ванснїк (нар. 1947) разом з Бертраном Маршаном (нар. 1952) розробили сімейство методів PROMETHEE (Preference Ranking Organization Method for Enrichment Evaluations), які використовують функції переваги для

порівняння альтернатив за кожним критерієм. Вони дозволяють працювати з якісними критеріями та неточною інформацією [14].

Байєсівські мережі, розвинені Джудеа Перлом (нар. 1936) у роботі «Імовірнісні міркування в інтелектуальних системах» (1988), дозволяють моделювати причинно-наслідкові зв'язки між ризиковими факторами в умовах невизначеності. Байєсівські мережі поєднують теорію ймовірностей з теорією графів для представлення знань та проведення висновків.

Уффе Б. К'ерульф та Андерс Л. Мадсен розширили застосування байєсівських мереж для аналізу ризиків, показавши, як ці методи можуть інтегрувати експертні знання з емпіричними даними. Динамічні байєсівські мережі дозволяють моделювати еволюцію ризиків у часі [7].

Реальні опціони як метод оцінки інвестиційних проєктів в умовах невизначеності були розвинені Стюартом Майерсом (нар. 1940) у 1970-х роках [6, 7, 10]. Фішер Блек (1938-1995), Майрон Шоулз (нар. 1941) та Роберт Мертон (нар. 1944) створили математичний апарат оцінки опціонів, який знайшов застосування у капітальному бюджетуванні.

Амір Бодурта (нар. 1956) та Лінос Тріантіс у роботі «Реальні опціони» (2001) систематизували застосування теорії опціонів для оцінки гнучкості управлінських рішень. Реальні опціони дозволяють кількісно оцінити вартість управлінської гнучкості: опціони на розширення, скорочення, відкладення, залишення проєкту.

Інтегровані показники ризику поєднують різні аспекти ризику в єдиній метриці. Економічний капітал вимірює капітал, необхідний для покриття неочікуваних втрат з певним рівнем довіри. Risk-Adjusted Return on Capital (RAROC), розроблений у Bankers Trust у 1980-х роках, дозволяє порівнювати ефективність різних бізнес-одиниць з урахуванням ризику.

Стрес-тестування як інтегрований метод оцінки стійкості до екстремальних сценаріїв набув особливої важливості після фінансової кризи 2008 року. Базельський комітет з банківського нагляду у документі «Принципи стрес-тестування» (2018) визначив стрес-тестування як ключовий інструмент управління ризиками та планування капіталу [6, 7, 10].

Цифрова трансформація радикально змінює підходи до оцінки та управління ризиками, створюючи нові можливості для аналізу великих обсягів даних, автоматизації процесів та підвищення точності прогнозування [1, 2, 3, 4].

Штучний інтелект та машинне навчання відкривають нові горизонти для аналізу ризиків. Артур Самюель (1901-1990), який ввів термін «машинне навчання» у 1959 році, визначив його як «галузь дослідження, яка дає комп'ютерам здатність навчатися без явного програмування» [4]. Сучасні алгоритми машинного навчання дозволяють виявляти складні нелінійні залежності в даних та автоматично адаптуватися до змін у ризиковому профілі.

Методи навчання з учителем (supervised learning) використовуються для прогнозування кредитних дефолтів, виявлення шахрайства та оцінки операційних ризиків [6]. Логістична регресія, розроблена Девідом Коксом

(1924-2022) у 1958 році, залишається базовим інструментом для бінарної класифікації ризикових подій.

Джеффри Хінтон (нар. 1947), «хрещений батько» глибокого навчання, розвинув архітектури нейронних мереж, які дозволяють автоматично вивчати складні залежності з даних. Сверточні нейронні мережі (CNN) ефективні для аналізу зображень та розпізнавання патернів у часових рядах. Рекурентні нейронні мережі (RNN) та їх модифікації LSTM (Long Short-Term Memory), розроблені Сеппом Гохрайтером (нар. 1967) та Юргеном Шмідхубером (нар. 1963), дозволяють моделювати послідовності та часові залежності.

Методи навчання без учителя (unsupervised learning) використовуються для виявлення аномалій та кластеризації ризиків. Алгоритми виявлення аномалій, такі як One-Class SVM та Isolation Forest, розроблений Фей Тоні Лю (нар. 1967) та його колегами, дозволяють ідентифікувати підозрілі транзакції та операційні збої без попереднього навчання на прикладах аномалій.

Обробка природної мови (Natural Language Processing, NLP) дозволяє аналізувати неструктуровану текстову інформацію для оцінки репутаційних та регуляторних ризиків. Сентимент-аналіз новин та соціальних медіа може передбачати зміни в ринкових настроях. Трансформерні моделі, такі як BERT (Bidirectional Encoder Representations from Transformers), розроблені командою Google AI під керівництвом Якоба Девліна у 2018 році, досягли значних успіхів у розумінні контексту та семантики текстів.

Великі дані (Big Data) створюють нові можливості для аналізу ризиків через інтеграцію структурованих та неструктурованих джерел інформації. Дуг Лені (нар. 1954) з Gartner визначив Big Data через модель «3V»: Volume (обсяг), Velocity (швидкість), Variety (різноманітність). Пізніше модель була розширена до «5V» з додаванням Veracity (достовірність) та Value (цінність).

Технології розподіленого зберігання та обробки, такі як Apache Hadoop, розроблений Дугом Каттінгом (нар. 1962) у Yahoo, дозволяють обробляти петабайти даних на кластерах звичайних серверів. Apache Spark, створений Матеєм Захарією (нар. 1984) в UC Berkeley, забезпечує швидку обробку даних в пам'яті та підтримує алгоритми машинного навчання.

Блокчейн технології створюють нові можливості для управління ризиками через забезпечення прозорості, відслідковуваності та незмінності записів. Сатоші Накамото (псевдонім) у whitepaper «Bitcoin: A Peer-to-Peer Electronic Cash System» (2008) описав принципи розподіленого реєстру, які знайшли застосування далеко за межами криптовалют.

Смарт-контракти, концепція яких була запропонована Ніком Сабо (нар. 1964) у 1990-х роках та реалізована на платформі Ethereum, дозволяють автоматизувати виконання договірних зобов'язань та зменшити контрагентський ризик. Децентралізовані автономні організації (DAO) можуть трансформувати управління ризиками через колективне прийняття рішень на основі токенизованого голосування.

Квантові обчислення обіцяють революційні зміни в оцінці ризиків, особливо у сферах оптимізації портфелів та моделювання складних

фінансових систем. Пітер Шор (нар. 1959) розробив квантовий алгоритм факторизації, який може загрожувати сучасним криптографічним системам. Лов Гровер (нар. 1961) створив квантовий алгоритм пошуку, який забезпечує квадратичне прискорення порівняно з класичними методами.

IBM, Google та інші технологічні гіганти розробляють квантові комп'ютери, які можуть розв'язувати задачі оптимізації портфелів з тисячами активів за лічені хвилини замість годин чи днів на класичних комп'ютерах. Квантова ймовірність може забезпечити більш точне моделювання фінансових ринків з урахуванням ефектів запутаності та суперпозиції.

Інтернет речей (IoT) створює нові джерела даних для оцінки операційних ризиків в реальному часі. Кевін Ештон (нар. 1968), який ввів термін «Інтернет речей» у 1999 році в Procter & Gamble, передбачив світ взаємопов'язаних пристроїв, які можуть збирати та передавати дані про стан об'єктів без людського втручання.

Сенсори IoT дозволяють моніторити параметри обладнання, навколишнього середовища та бізнес-процесів у режимі реального часу. Предиктивне обслуговування (predictive maintenance) використовує дані з IoT-пристроїв для прогнозування відмов обладнання до їх виникнення. Алгоритми машинного навчання аналізують вібрації, температуру, звук та інші параметри для виявлення аномалій у роботі обладнання.

Цифрові двійники (Digital Twins), концепція яких була запропонована Майклом Грівзом (нар. 1950) у 2003 році в Мічиганському університеті, представляють віртуальні копії фізичних об'єктів або процесів. Цифрові двійники дозволяють моделювати різні сценарії та тестувати стратегії управління ризиками без впливу на реальні системи. General Electric, Siemens та інші промислові компанії використовують цифрових двійників для оптимізації роботи турбін, двигунів та інших складних систем.

Хмарні обчислення забезпечують масштабованість та доступність інструментів оцінки ризиків. Amazon Web Services (AWS), запущений Джефом Безосом (нар. 1964) у 2006 році, Microsoft Azure та Google Cloud Platform пропонують потужні сервіси для аналітики даних та машинного навчання. Serverless архітектури дозволяють автоматично масштабувати обчислювальні ресурси залежно від навантаження.

Робототехніка та автоматизація процесів (Robotic Process Automation, RPA) трансформують операційні ризики через стандартизацію та автоматизацію рутинних завдань. UiPath, Automation Anywhere та Blue Prism надають платформи для створення програмних роботів, які можуть виконувати завдання з обробки документів, перевірки даних та звітності з мінімальною ймовірністю помилок.

Регуляторні технології (RegTech) спеціалізуються на автоматизації дотримання вимог регуляторів та управління комплаєнс-ризиками. Такі рішення використовують правила бізнес-логіки, машинне навчання та обробку природної мови для моніторингу транзакцій, виявлення підозрілої діяльності та автоматичної підготовки регуляторних звітів. Palantir Technologies, Ayasdi

та інші компанії розробляють спеціалізовані платформи для фінансових інститутів.

Кібербезпека та оцінка кіберризиків стають критично важливими в цифрову епоху. Брюс Шнайер (нар. 1963), всесвітньо відомий експерт з безпеки, у роботах «Прикладна криптографія» (1993) та «Секрети та брехня» (2000) заклав теоретичні основи сучасної інформаційної безпеки. NIST Cybersecurity Framework, розроблений Національним інститутом стандартів та технологій США, надає структуру для управління кіберризиками через функції: ідентифікація, захист, виявлення, реагування, відновлення.

Поведінкова аналітика користувачів (User and Entity Behavior Analytics, UEBA) використовує машинне навчання для створення базових профілів поведінки користувачів та виявлення аномальних дій, які можуть вказувати на внутрішні загрози або компрометацію акаунтів. Системи аналізують патерни доступу до даних, час роботи, географічне розташування та інші параметри.

Візуалізація даних та дашборди дозволяють представити складну інформацію про ризики у зрозумілому вигляді для прийняття управлінських рішень. Tableau Software, заснована Крісом Столті (нар. 1971), Петом Ханраханом (нар. 1954) та Крістіаном Чабо у 2003 році в Стенфордському університеті, революціонізувала підходи до бізнес-аналітики через інтуїтивні інтерфейси та потужні можливості візуалізації.

Інтерактивні дашборди ризиків дозволяють менеджерам відслідковувати ключові індикатори ризику (Key Risk Indicators, KRI) у реальному часі, проводити drill-down аналіз та моделювати різні сценарії. Heat maps, водоспади, діаграми Санкей та інші види візуалізації допомагають виявляти патерни та тренди в ризиковій експозиції.

Етичні аспекти використання ШІ в оцінці ризиків набувають особливої важливості у контексті алгоритмічної справедливості та прозорості. Кетрін О'Ніл (нар. 1972) у роботі «Зброя математичного знищення» (2016) показала, як алгоритми можуть посилювати соціальну нерівність та дискримінацію. Принципи Explainable AI (XAI), розвинені DARPA, вимагають, щоб алгоритми машинного навчання могли пояснити свої рішення зрозумілою для людини мовою.

Регуляторні вимоги, такі як Загальний регламент захисту даних (GDPR) в ЄС, надають фізичним особам право на пояснення автоматизованих рішень, що впливають на їх життя та створює нові виклики для розробки алгоритмів оцінки кредитних, страхових та інших ризиків.

Майбутні тенденції включають розвиток автономних систем управління ризиками, які можуть самостійно адаптуватися до змін у ризиковому середовищі. Федеративне навчання (Federated Learning), розроблене в Google під керівництвом Брендана МакМагена, дозволяє навчати моделі машинного навчання на розподілених даних без їх централізації, що має важливе значення для конфіденційності та безпеки.

Нейроморфні обчислення, що імітують роботу людського мозку, можуть забезпечити більш ефективну обробку складних ризикових патернів. Intel

Loihi, IBM TrueNorth та інші нейроморфні чіпи обіцяють радикальне підвищення енергоефективності та швидкості обробки для задач розпізнавання образів та прийняття рішень в умовах невизначеності.

Інтеграція цих технологій створює синергетичні ефекти, коли поєднання різних підходів дає кращі результати, ніж використання окремих методів [4].

Таким чином сучасні методи оцінки та вимірювання ризиків формують комплексний інструментарій для менеджерів, які прагнуть ефективно управляти невизначеністю в динамічному організаційному середовищі. Кількісні методи, такі як Value at Risk (VaR), Conditional Value at Risk (CVaR), імітаційне моделювання Монте-Карло та екстремальна теорія значень, спираючись на праці Карла Пірсона, Гаррі Марковіца, Фішера-Тіппетта-Гнеденка та інших, забезпечують об'єктивну оцінку ризиків через математичний і статистичний аналіз. Якісні методи, включаючи експертний аналіз (метод Дельфі, Норман Далкі), сценарний аналіз (П'єр Вак) та SWOT-аналіз, дозволяють менеджерам оцінювати ризики в умовах обмежених даних, інтегруючи суб'єктивні судження та стратегічний контекст. Інтегровані методи, такі як COSO ERM та ISO 31000:2018, поєднують кількісні та якісні підходи, забезпечуючи холістичне управління ризиками через структуровані процеси ідентифікації, аналізу та обробки ризиків. Цифрові технології, зокрема штучний інтелект (Хінтон), великі дані, блокчейн (Накамото) та цифрові двійники (Грівз), революціонізують оцінку ризиків, дозволяючи обробляти великі обсяги даних у реальному часі, виявляти аномалії та моделювати складні сценарії.

Для здобувачів третього освітньо-наукового рівня ці методи є критично важливими для розробки стратегій управління ризиками в умовах цифрової трансформації та глобальних викликів, таких як кіберзагрози, кліматична нестабільність чи регуляторні зміни. Наприклад, VaR і CVaR допомагають оцінювати фінансові ризики, тоді як сценарний аналіз і байєсівські мережі сприяють прогнозуванню стратегічних і операційних ризиків. Цифрові інструменти, такі як машинне навчання та IoT, дозволяють менеджерам створювати адаптивні системи управління, що підвищують резильєнтність організацій. Пропонується досліджувати синергетичні можливості інтеграції кількісних, якісних і цифрових методів у дисертаційних проєктах, розробляючи інноваційні моделі ризик-менеджменту, які враховують етичні, соціальні та технологічні аспекти.

ПИТАННЯ ДО ПРАКТИЧНОГО ЗАНЯТТЯ

1. Статистичні показники (дисперсія, стандартне відхилення, коефіцієнт варіації). Практичні приклади.
2. Метод Value at Risk (VaR) та його застосування для оцінки ринкових ризиків.
3. Відмінність між методом Дельфі та SWOT-аналізом у якісній оцінці ризиків.
4. Модель COSO ERM. П'ять компонентів моделі та їх застосування.

5. Переваги байєсівських мереж у інтегрованій оцінці ризиків.
6. Штучний інтелект і його застосування для виявлення аномалій у ризик-менеджменті.
7. Алгоритм Isolation Forest і його використання для оцінки кіберризиків.
8. Етичні аспекти використання ШІ в ризик-менеджменті.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ:

1. Розрахуйте кількісні показники ризику для інвестиційного портфеля. Для цього опишіть процес розрахунку ризику для гіпотетичного портфеля з трьох активів (наприклад, акції, облігації, нерухомість) з заданими даними про середню доходність і стандартне відхилення.

Розрахуйте дисперсію, стандартне відхилення, коефіцієнт варіації та Value at Risk (VaR) на рівні 5% за параметричним методом. Оберіть дані (наприклад, $\mu = 50\%$, $\sigma = 10\%$ для одного активу) і проаналізуйте, який актив має найвищий ризик.

2. Оберіть і розкрийте якісний метод аналізу ризиків для стратегічного проєкту для цього оберіть один якісний метод (наприклад, метод Дельфі або SWOT-аналіз) і розкрийте його застосування для оцінки ризиків у стратегічному проєкті компанії (наприклад, запуск нового продукту). Проаналізуйте переваги та обмеження методу, моделюючи 5–7 експертних думок для Дельфі або заповнюючи матрицю SWOT. Опишіть, як метод допомагає в умовах обмежених даних.

3. Проаналізуйте інтегрований метод для управління ризиками в організації для цього проаналізуйте модель COSO ERM або ISO 31000:2018 для управління ризиками в обраній організації (наприклад, банк або виробниче підприємство). Розкрийте п'ять компонентів моделі, оберіть 3 ризики (фінансовий, операційний, репутаційний) і розрахуйте ймовірність їх реалізації, поєднуючи кількісні (наприклад, CVaR) та якісні (наприклад, сценарний аналіз) підходи. Опишіть, як модель забезпечує холістичне управління.

4. Оберіть цифрову технологію для оцінки ризиків і розрахуйте її ефективність для цього оберіть одну цифрову технологію (наприклад, машинне навчання або IoT) і розрахуйте її застосування для оцінки ризиків у бізнес-процесі (наприклад, предиктивне обслуговування обладнання). Проаналізуйте алгоритм (наприклад, LSTM для прогнозування), оберіть гіпотетичні дані (вібрація, температура) і розрахуйте ймовірність аномалій. Опишіть етичні аспекти (наприклад, GDPR).

5. Розкрийте і проаналізуйте комплексну оцінку ризиків для інвестиційного проєкту для цього розкрийте процес комплексної оцінки ризиків для інвестиційного проєкту (наприклад, запуск стартапу). Оберіть комбінацію методів: розрахуйте VaR і CVaR для фінансових ризиків, проаналізуйте якісні ризики за SWOT, інтегруйте за ISO 31000 і застосуйте

цифрову технологію (наприклад, блокчейн для зниження контрагентського ризику). Опишіть рекомендації для менеджменту.

Питання для самоконтролю:

1. Яка формула стандартного відхилення як міри ризику, і як вона пов'язана з дисперсією? Наведіть приклад застосування в фінансах.
2. У чому полягає метод Value at Risk (VaR), і як обчислюється його параметричний варіант? Вкажіть обмеження методу.
3. Як метод Дельфі застосовується для якісної оцінки ризиків, і які його ключові принципи (анонімність, ітеративність)?
4. Що таке модель COSO ERM, і які її п'ять компонентів? Як вона інтегрує кількісні та якісні методи?

ТЕМИ ПРЕЗЕНТАЦІЙ ТА ПОВІДОМЛЕНЬ:

1. Кількісні методи оцінки ризиків від дисперсії до VaR і CVaR як приклади застосування в фінансовому менеджменті.
2. Якісні методи аналізу ризиків. Метод Дельфі та SWOT-аналіз як інструменти стратегічного планування.
3. Інтегровані методи. Модель COSO ERM і ISO 31000 у холістичному управлінні ризиками організації.
4. Цифрові технології в оцінці ризиків. Роль машинного навчання та IoT у сучасному ризик-менеджменті.
5. Сценарне та імітаційне моделювання як інструменти управління ризиками.
6. Інтеграція цифрових платформ у систему корпоративного ризик-менеджменту.

Література:

1. Кібік О., Слободянюк О., Кузнецова Л. Ризик-менеджмент : навч.-метод. посібник / Нац. ун-т «Одес. юрид. академія». Одеса : Фенікс, 2024. 84 с. URL: <https://hdl.handle.net/11300/27828>
2. Демченко Г. В. Ризик-менеджмент: навчальний посібник для здобувачів спеціальності 073 «Менеджмент» першого (бакалаврського) рівня. Харків: Харківський національний економічний університет імені Семена Кузнеця, 2021. 224 с. URL: <https://files.znu.edu.ua/files/Bibliobooks/Inshi81/0061258.pdf>
3. Боровик М. В. Ризик-менеджмент : конспект лекцій для здобувачів другого (магістерського) рівня вищої освіти спеціальності 073 – Менеджмент / М. В. Боровик ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2023. 63 с. URL: <https://files.znu.edu.ua/files/Bibliobooks/Inshi73/0054006.pdf>
4. Мороз В. М. Ризик-менеджмент: навчальний посібник. Харків: Національний технічний університет «Харківський політехнічний інститут», 2018. 240 с. URL:

<https://repository.kpi.kharkov.ua/server/api/core/bitstreams/f3be8995-acd3-4ab8-928f-1c5ff30f3584/content>

5. Савчук В. І. Ризик-менеджмент: навчальний посібник. Київ: Видавництво «Лабораторія», 2019. 320 с. URL: <https://laboratory.ua/products/ryzyk-menedzhment>

6. Долінський Л. Б. Фінансовий ризик-менеджмент: навчально-методичний посібник. Київ: Національний університет «Києво-Могилянська академія», 2022. 132 с. URL: https://fpk.in.ua/images/biblioteka/4bac_finan/Dolinskyy.-Finansovyy-ryzyk-menedzhment-2022_compressed.pdf

7. McNeil, A. J., Frey, R., & Embrechts, P. Quantitative risk management: concepts, techniques and tools. Princeton university press, 2015. URL: <http://ndl.ethernet.edu.et/bitstream/123456789/30397/1/141.Alexander%20J.McNeil.pdf>

8. Jorion, P. Value at Risk: The New Benchmark for Managing Financial Risk. McGraw-Hill, 2006.

9. Holton, G. A. Value-at-Risk: Theory and Practice. 2003. URL: https://first-edition.value-at-risk.net/wp-content/uploads/book_pdf/Holton-2003-Value-at-Risk.pdf

10. Christoffersen, P. Elements of Financial Risk Management. Academic Press, 2012. URL: <https://unidel.edu.ng/focelibrary/books/Elements%20of%20Financial%20Risk%20Management.pdf>

11. Committee of Sponsoring Organizations of the Treadway Commission (COSO). Enterprise Risk Management—Integrating with Strategy and Performance. 2017. URL: https://docs.wbcsd.org/2018/10/COSO_WBCSD_ESGERM_Guidance.pdf

12. ISO 31000:2018. Risk management — Guidelines. International Organization for Standardization.

13. Korombel, A. Qualitative risk analysis as a stage of risk management in investment projects: Advantages and disadvantages of selected methods—theoretical approach. Adalta Journal of Interdisciplinary Research, 2014. URL: https://www.magnanimitas.cz/ADALTA/0102/papers/A_korombel.pdf

14. A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. 2010. URL: <https://ferma.eu/wp-content/uploads/2019/02/a-structured-approach-to-erm-1.pdf>

ТЕМА 3. МОДЕЛІ ТА СТРАТЕГІЇ УПРАВЛІННЯ РИЗИКАМИ

Лекційні питання:

Мета вивчення/ роботи: ознайомлення з концептуальними засадами моделювання ризиків в управлінській діяльності, систематизація знань про стратегії реагування на ризики, формування розуміння інтегрованих систем ризик-менеджменту та динамічних моделей управління ризиками в умовах невизначеності сучасного бізнес-середовища.

1. Концептуальні моделі управління ризиками.
2. Стратегії реагування на ризики.
3. Інтегровані системи управління ризиками.
4. Динамічні моделі управління ризиками в умовах невизначеності.

Зміст лекції

Концептуальні моделі управління ризиками становлять теоретичну основу для розуміння природи ризиків та механізмів їх регулювання в організаційних системах. Сучасна теорія ризик-менеджменту базується на декількох фундаментальних моделях, кожна з яких відображає специфічні аспекти ризикової діяльності та пропонує відповідні інструментарії для управління [1, 2, 3, 4, 5, 6, 7].

Класична модель управління ризиками, запропонована Найтом у 1921 році, розрізняє ризик та невизначеність як два принципово різні явища. Згідно з даною моделлю, ризик характеризується можливістю кількісного оцінювання ймовірності настання несприятливих подій, тоді як невизначеність передбачає ситуації, де таке оцінювання неможливе [5, 7]. Зазначена концептуальна відмінність має фундаментальне значення для вибору методів управління, оскільки ризики піддаються статистичному аналізу та страхуванню, а невизначеність вимагає якісно іншого підходу, заснованого на гнучкості та адаптивності управлінських рішень [5, 7].

Математично ризик у найтовщій моделі може бути представлений як:

$$R = P \times I,$$

де R – рівень ризику, P – ймовірність настання ризикової події, I – величина потенційного впливу (збитку).

Портфельна модель Марковіца розширює розуміння ризику через призму диверсифікації та кореляції між різними видами ризиків. Основна ідея моделі полягає в тому, що загальний ризик портфеля активів не дорівнює простій сумі індивідуальних ризиків, а залежить від ступеня кореляції між ними. Дана модель дозволяє організаціям мінімізувати сукупний ризик через оптимальне поєднання різних видів діяльності, інвестицій або стратегічних ініціатив.

Дисперсія портфеля в моделі Марковіца визначається формулою [3, 4, 6, 11]:

$$\sigma_p^2 = \sum_i \sum_j w_i w_j \sigma_{ij}$$

де σ_p^2 – дисперсія портфеля, w_i і w_j – ваги активів у портфелі, σ_{ij} – коваріація між доходностями активів i та j .

Оптимальний портфель за Марковіцем знаходиться шляхом мінімізації дисперсії при заданому рівні очікуваної доходності [3, 4, 6, 11]:

$$\min \sigma_p^2 \text{ при } E(r_p) = \sum_i w_i E(r_i) = \mu_p$$

Системна модель управління ризиками розглядає організацію як складну адаптивну систему, де ризики виникають не лише з зовнішнього середовища, але й внаслідок внутрішніх взаємодій між елементами системи. Вказана модель підкреслює значення системних ризиків, які можуть виникати через каскадні ефекти, коли локальні порушення в одній частині системи призводять до масштабних наслідків для всієї організації.

Системний ризик може бути виражений через коефіцієнт системної важливості [8, 11]:

$$SII = (\Delta ES / GDP_s) / (LEV_i / LEV_s)$$

де SII – індекс системної важливості, ΔES – зміна очікуваного дефіциту, GDP_s – ВВП системи, LEV_i – левередж інституції, LEV_s – системний левередж.

Поведінкова модель управління ризиками інтегрує досягнення поведінкової економіки та когнітивної психології для пояснення того, як менеджери сприймають та реагують на ризики. Дана модель враховує систематичні когнітивні упередження, такі як надмірна самовпевненість, схильність до підтвердження та ефект фрейму, які можуть суттєво впливати на процеси оцінки ризиків та прийняття рішень [5, 7].

Функція корисності в поведінковій моделі може бути представлена як:

$$U(x) = x^\alpha \text{ для вигравів та } U(x) = -\lambda(-x)^\beta \text{ для програшів}$$

де α і β – параметри чутливості до вигравів і програшів відповідно, λ – коефіцієнт неприйняття втрат ($\lambda > 1$).

Стохастична модель управління ризиками базується на математичному апараті теорії ймовірностей та стохастичних процесів для моделювання динаміки ризиків у часі [3, 4, 6, 9, 11]. Зазначена модель особливо корисна для аналізу фінансових ризиків, де використовуються такі інструменти, як броунівський рух, процеси Пуассона та стохастичні диференціальні рівняння для прогнозування майбутніх станів ризикових параметрів [6, 11].

Геометричний броунівський рух для моделювання цінкових процесів описується рівнянням:

$$dS = \mu S dt + \sigma S dW$$

де S – ціна активу, μ – параметр зносу, σ – волатильність, dW – випадковий процес Вінера.

Модель Value-at-Risk (VaR) для оцінки ризику втрат:

$$VaR_{\alpha} = -F^{-1}(\alpha)$$

де F^{-1} – обернена функція розподілу прибутків і збитків, α – рівень довіри.

Стратегії реагування на ризики представляють собою систематизовані підходи до управління ідентифікованими ризиками, спрямовані на досягнення оптимального співвідношення між рівнем ризику та потенційною віддачею [1, 2, 5, 7, 9, 10]. Сучасна теорія ризик-менеджменту виділяє чотири основні стратегії реагування на ризики, кожна з яких має свої специфічні умови застосування та очікувані результати [5, 7, 9, 10].

Стратегія уникнення ризику передбачає повне усунення можливості настання ризикової події через відмову від певних видів діяльності, проектів або рішень. Вказана стратегія є найбільш радикальною та застосовується у випадках, коли потенційні негативні наслідки значно перевищують можливі вигоди, або коли організація не має достатніх ресурсів для ефективного управління конкретним ризиком. Проте уникнення ризику може призвести до втрати потенційно прибуткових можливостей та обмежити стратегічний розвиток організації.

Критерій вибору стратегії уникнення може бути формалізований як [5, 9]:

Якщо $E(L) > E(G) + C(R)$, то обрати уникнення

де $E(L)$ – очікувані втрати, $E(G)$ – очікувані вигоди, $C(R)$ – вартість управління ризиком.

Стратегія зменшення ризику спрямована на мінімізацію ймовірності настання ризикової події або зниження масштабу її потенційних наслідків. Дана стратегія реалізується через впровадження превентивних заходів, удосконалення процедур контролю, підвищення кваліфікації персоналу, технологічні інновації та інші заходи, що знижують рівень ризику до прийняттого рівня. Зменшення ризику часто є найбільш економічно ефективним підходом, оскільки дозволяє зберегти можливості для отримання вигод при одночасному контролі над ризиками [1, 2, 5, 7, 9, 10].

Ефективність зменшення ризику може бути оцінена через коефіцієнт ефективності [5, 9]:

$$E_r = (R_0 - R_1) / C_r$$

де R_0 – початковий рівень ризику, R_1 – рівень ризику після заходів, C_r – витрати на зменшення ризику.

Стратегія передачі ризику полягає в перенесенні відповідальності за ризик на третю сторону, зазвичай через механізми страхування, аутсорсингу або договірні зобов'язання. Зазначена стратегія особливо ефективна для ризиків з низькою ймовірністю настання, але високим потенціалом збитків, коли вартість передачі ризику є меншою за очікувані втрати. Проте передача ризику не завжди означає повне звільнення від відповідальності, оскільки

організація може зберігати залишковий ризик, пов'язаний з неспроможністю контрагента виконати свої зобов'язання [5, 7, 9].

Оптимальний рівень страхування визначається з умови:

$$\pi'(I) = \lambda p'(I) u'(w - L + I - \pi(I))$$

де $\pi'(I)$ – страхова премія, I – рівень страхового покриття, λ – коефіцієнт неприйняття ризику, $p(I)$ – ймовірність збитку, u – функція корисності.

Стратегія прийняття ризику передбачає свідоме рішення про збереження ризику в межах організації без активних заходів щодо його модифікації. Вказана стратегія застосовується у випадках, коли вартість інших стратегій перевищує потенційні втрати, або коли ризик знаходиться в межах толерантності організації. Прийняття ризику може бути активним, коли створюються резерви для покриття потенційних збитків, або пасивним, коли організація просто визнає існування ризику без специфічних приготувань [5, 7, 9].

Розмір резерву для покриття ризику розраховується за формулою:

$$R = VaR_{\alpha} + ES_{\alpha}$$

де VaR_{α} – Value-at-Risk на рівні довіри α , ES_{α} – очікуваний дефіцит (Expected Shortfall).

Гібридні стратегії представляють собою комбінації основних підходів, адаптовані до специфічних умов організації та характеристик конкретних ризиків. Наприклад, організація може частково передати ризик через страхування, одночасно впроваджуючи заходи для його зменшення та утримуючи залишковий ризик на прийнятному рівні [5, 7, 9, 10].

Загальна ефективність гібридної стратегії:

$$E_{total} = w_1 E_1 + w_2 E_2 + w_3 E_3 + w_4 E_4$$

де E_1, E_2, E_3, E_4 – ефективність стратегій уникнення, зменшення, передачі та прийняття відповідно, $w_1 + w_2 + w_3 + w_4 = 1$.

Інтегровані системи управління ризиками представляють собою комплексний підхід до ризик-менеджменту, що об'єднує всі аспекти управління ризиками в єдину систему, яка охоплює всі рівні організації та всі види діяльності. Даний підхід відходить від фрагментованого управління окремими категоріями ризиків на користь холістичного розгляду ризикового профілю організації як цілісної системи взаємопов'язаних елементів [5, 7, 8, 12].

Архітектура інтегрованої системи управління ризиками базується на принципах системного підходу та включає декілька ключових компонентів. Стратегічний рівень визначає ризик-апетит організації, встановлює загальні принципи управління ризиками та забезпечує відповідність ризик-менеджменту стратегічним цілям. Операційний рівень відповідає за практичну реалізацію процедур управління ризиками в повсякденній діяльності, включаючи ідентифікацію, оцінку, моніторинг та звітність про ризики.

Математична модель інтегрованої системи може бути представлена через систему рівнянь [8, 12]:

$$S = f(R_1, R_2, \dots, R_n, C_{12}, C_{13}, \dots, C_{ij})$$

де S – системний ризик, R_i – індивідуальні ризики, C_{ij} – коефіцієнти кореляції між ризиками.

Процесний компонент інтегрованої системи забезпечує стандартизацію методів управління ризиками по всій організації через розробку єдиних процедур, методик та інструментів. Зазначене включає створення корпоративних реєстрів ризиків, стандартизацію критеріїв оцінки ризиків, уніфікацію форматів звітності та встановлення чітких ролей і відповідальності в процесах ризик-менеджменту.

Індекс зрілості процесів управління ризиками [8, 12]:

$$PMI = \sum_i w_i \times M_i$$

де PMI – індекс зрілості процесів, w_i – ваги процесів, M_i – рівень зрілості i -го процесу (1-5).

Технологічний компонент інтегрованої системи передбачає використання спеціалізованого програмного забезпечення для управління ризиками, яке забезпечує централізоване збирання, обробку та аналіз інформації про ризики. Сучасні GRC-платформи (Governance, Risk, Compliance) дозволяють автоматизувати багато рутинних процедур, підвищити якість аналітики та забезпечити своєчасність управлінських рішень.

Ефективність технологічного компонента може бути виражена через коефіцієнт автоматизації [8, 12]:

$$A = (P_{auto} / P_{total}) \times 100\%$$

де P_{auto} – кількість автоматизованих процедур, P_{total} – загальна кількість процедур.

Культурний компонент інтегрованої системи спрямований на формування ризик-свідомої організаційної культури, де всі співробітники розуміють свою роль у процесах управління ризиками та активно беруть участь у їх реалізації. Дане завдання вимагає систематичного навчання персоналу, створення відповідних стимулів та інтеграції ризик-менеджменту в систему оцінки ефективності діяльності.

Рівень ризик-культури може бути кількісно оцінений через індекс [8, 12]:

$$RCI = \alpha_1 \times K + \alpha_2 \times A + \alpha_3 \times B + \alpha_4 \times C$$

де K – рівень знань про ризики, A – рівень обізнаності, B – поведінкові індикатори, C – рівень комунікації, $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1$.

Інтегровані системи управління ризиками забезпечують декілька ключових переваг порівняно з фрагментованими підходами. По-перше, вони

дозволяють отримати повну картину ризикового профілю організації, включаючи взаємозв'язки між різними ризиками та можливі кумулятивні ефекти. По-друге, інтегрований підхід підвищує ефективність використання ресурсів через усунення дублювання зусиль та оптимізацію розподілу відповідальності. По-третє, інтегровані системи забезпечують кращу координацію між різними підрозділами організації та підвищують якість стратегічного планування.

Показник синергетичного ефекту інтеграції [8, 12]:

$$SE = (V_{integrated} - \sum_i V_{individual}) / \sum_i V_{individual} \times 100\%$$

де $V_{integrated}$ – вартість інтегрованої системи, $V_{individual}$ – вартість окремих систем.

Динамічні моделі управління ризиками в умовах невизначеності представляють новий етап розвитку теорії ризик-менеджменту, що враховує мінливість та непередбачуваність сучасного бізнес-середовища. Вказані моделі виходять за межі традиційних статичних підходів, які розглядають ризики як відносно стабільні явища, та фокусуються на адаптивності й гнучкості управлінських систем [5, 6, 9, 10, 11].

Концепція динамічного управління ризиками базується на розумінні того, що ризики постійно еволюціонують під впливом змін у внутрішньому та зовнішньому середовищі організації. Традиційні моделі, які передбачають періодичне оновлення оцінок ризиків, виявляються недостатніми в умовах високої волатильності та структурних змін. Динамічні моделі передбачають безперервний моніторинг ризикового ландшафту та оперативну адаптацію управлінських стратегій відповідно до нових умов.

Динамічна модель ризику може бути описана стохастичним диференціальним рівнянням [6, 11]:

$$dR(t) = \mu(t, R)dt + \sigma(t, R)dW(t) + \int h(t, R, z)\tilde{N}(dt, dz)$$

де $R(t)$ – рівень ризику в часі t , $\mu(t, R)$ – функція тренду, $\sigma(t, R)$ – функція волатильності, $\tilde{N}(dt, dz)$ – компенсований пуассонівський випадковий процес.

Адаптивні системи управління ризиками використовують принципи машинного навчання та штучного інтелекту для автоматичного оновлення параметрів ризикових моделей на основі нової інформації. Зазначені системи здатні виявляти зміни в паттернах ризиків, ідентифікувати нові типи загроз та автоматично коригувати управлінські реакції. Особливо важливим є використання алгоритмів реального часу для обробки великих обсягів даних та виявлення слабких сигналів про потенційні ризики.

Алгоритм адаптивного навчання для оновлення параметрів моделі:

$$\theta(t+1) = \theta(t) + \eta \nabla L(\theta(t), D(t))$$

де $\theta(t)$ – параметри моделі в часі t , η – коефіцієнт навчання, L – функція втрат, $D(t)$ – дані в часі t .

Функція виявлення аномалій в режимі реального часу [11]:

$$A(t) = \|x(t) - \bar{x}(t)\|^2 > \tau$$

де $x(t)$ – поточні спостереження, $\bar{x}(t)$ – очікувані значення, τ – поріг виявлення.

Сценарне планування в динамічних моделях виходить за межі традиційного підходу з фіксованим набором сценаріїв та передбачає постійне оновлення та розширення сценарного простору. Використання методів Монте-Карло та агентного моделювання дозволяє досліджувати велику кількість потенційних траєкторій розвитку подій та ідентифікувати критичні точки, де невеликі зміни можуть призвести до кардинально різних наслідків [3, 6, 9, 11].

Модель динамічного сценарного планування [11]:

$$S(t+1) = f(S(t), E(t), U(t), \varepsilon(t))$$

де $S(t)$ – стан системи, $E(t)$ – зовнішні фактори, $U(t)$ – управлінські дії, $\varepsilon(t)$ – випадкові збурення.

Ймовірність переходу між сценаріями [11]:

$$P(S_{t+1}=j|S_t=i) = \exp(\beta \times U_{ij}) / \sum_k \exp(\beta \times U_{ik})$$

де U_{ij} – корисність переходу з стану i в стан j , β – параметр чутливості.

Реальні опціони представляють потужний інструмент динамічного управління ризиками, що дозволяє організаціям зберігати гнучкість у прийнятті рішень в умовах невизначеності. Підхід реальних опціонів передбачає структурування стратегічних ініціатив таким чином, щоб організація мала можливість розширювати, скорочувати, відкладати або припиняти проекти залежно від розвитку ситуації. Вказане дозволяє мінімізувати негативний вплив несприятливих сценаріїв при одночасному збереженні можливостей для використання сприятливих обставин [11].

Вартість реального опціону розраховується за формулою Блека-Шоулза:

$$C = S_0 N(d_1) - X e^{-rT} N(d_2)$$

$$\text{де } d_1 = \frac{\ln\left(\frac{C_0}{X}\right) + \left(r + \frac{1}{2}\sigma^2\right)T}{\sigma\sqrt{T}} \quad d_2 = d_1 - \sigma\sqrt{T}$$

C – вартість опціону, S_0 – поточна вартість активу, X – ціна виконання, r – безризикова ставка, T – час до погашення, σ – волатильність, $N()$ – функція нормального розподілу.

Антикрихкість як концепція динамічного управління ризиками передбачає створення систем, які не просто витримують шоки та стреси, але й стають сильнішими завдяки їм. Антикрихкі організації використовують волатильність та невизначеність як джерела конкурентних переваг через розвиток адаптивних здібностей, диверсифікацію стратегій та створення надлишкових ресурсів у критичних сферах [5, 9, 10].

Коефіцієнт антикрихкості може бути виражений як [11]:

$$AF = \partial^2 \pi / \partial \sigma^2 > 0$$

де π – прибуток, σ – волатильність зовнішнього середовища.

Індекс відновлюваності системи [5, 9]:

$$RI = 1 - [(t_{recovery} - t_{shock}) / T_{max}]$$

де $t_{recovery}$ – час відновлення, t_{shock} – час шоку, T_{max} – максимальний допустимий час відновлення.

Динамічні моделі інтегрують елементи теорії складності та теорії хаосу для розуміння нелінійних ефектів та емерджентних властивостей ризикових систем. Вказане включає використання фрактальної геометрії для моделювання екстремальних подій, теорії катастроф для аналізу точок біфуркації та мережевого аналізу для дослідження поширення ризиків через складні системи взаємозв'язків [11].

Фрактальна розмірність для моделювання екстремальних подій [11]:

$$D = \lim_{\epsilon \rightarrow 0} [\log N(\epsilon) / \log(1/\epsilon)]$$

де $N(\epsilon)$ – кількість покриваючих сфер радіусом ϵ .

Показник Херста для аналізу довгострокової залежності [11]:

$$H = \log(R/S) / \log(n)$$

де R/S – нормалізований розмах, n – розмір вибірки.

Модель поширення ризику в мережі [11]:

$$dI_i / dt = \beta \sum_j A_{ij} I_j (1 - I_i) - \gamma I_i$$

де I_i – рівень ризику у вузлі i , A_{ij} – матриця суміжності, β – швидкість поширення, γ – швидкість затухання.

Ефективність динамічних моделей управління ризиками значною мірою залежить від якості інформаційних систем та аналітичних здібностей організації. Вказане вимагає інвестицій у сучасні технології збору та обробки даних, розвиток компетенцій у сфері аналітики та створення організаційної культури, що підтримує експериментування та навчання на основі досвіду [11]

Показник інформаційної ефективності системи [11]:

$$IE = H(Y|X) / H(Y)$$

де $H(Y|X)$ – умовна ентропія, $H(Y)$ – повна ентропія результату.

Коефіцієнт адаптивності організації [5, 9, 10]:

$$AC = \Delta performance / \Delta environment$$

де $\Delta performance$ – зміна результативності, $\Delta environment$ – зміна зовнішнього середовища.

Загальна оцінка ефективності динамічної моделі управління ризиками [5, 9, 10]:

$$E_{dynamic} = w_1 \times Accuracy + w_2 \times Speed + w_3 \times Adaptability + w_4 \times Robustness$$

де $Accuracy$ – точність прогнозування, $Speed$ – швидкість реакції, $Adaptability$ – адаптивність, $Robustness$ – стійкість моделі.

Таким чином, моделі та стратегії управління ризиками еволюціонують від простих статичних підходів до складних динамічних систем, здатних

адаптуватися до мінливих умов невизначеності. Успішна імплементація зазначених підходів вимагає інтеграції теоретичних знань, практичного досвіду та сучасних технологій для створення стійких та адаптивних організаційних систем. Математичне обґрунтування представлених моделей забезпечує можливість кількісної оцінки ризиків та ефективності управлінських рішень, що є критично важливим для науково обґрунтованого підходу до ризик-менеджменту в сучасних умовах господарювання.

ПИТАННЯ ДО ПРАКТИЧНОГО ЗАНЯТТЯ

1. Концепція Френка Найта щодо розрізнення ризику та невизначеності та її вплив на вибір методів управління ризиками в організації.
2. Модель Марковіца для зменшення ризику через диверсифікацію та методику розрахунку ризику портфеля з урахуванням взаємозв'язків між активами.
3. Психологічні упередження в поведінковій моделі управління ризиками та їх вплив на оцінку ризиків у проєктах.
4. Відмінності між стратегіями уникнення, зменшення, передачі та прийняття ризику та оцінка їх ефективності на прикладі конкретного проєкту.
5. Комплексний підхід інтегрованих систем управління ризиками, таких як COSO ERM та оцінка їх ефективності щодо процесів ризик-менеджменту.
6. Застосування динамічних моделей, зокрема реальних опціонів, для забезпечення гнучкості в управлінні ризиками в умовах невизначеності.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ:

1. Опишіть концепцію Френка Найта щодо розрізнення ризику та невизначеності та оцініть її застосування для управління ризиками в обраній організації (наприклад, банківська установа, ІТ-компанія або виробниче підприємство). Проаналізуйте один фінансовий ризик (наприклад, валютний ризик) як приклад ризику з вимірюваною ймовірністю та один стратегічний ризик (наприклад, зміна ринкових умов) як приклад невизначеності. Запропонуйте управлінські рішення для кожного випадку.
2. Оберіть гіпотетичний інвестиційний портфель із трьох активів (наприклад, акції, облігації, нерухомість) із заданими частками, середньою доходністю та індивідуальними ризиками. Розрахуйте ризик портфеля, враховуючи взаємозв'язки між активами, та оцініть, як диверсифікація впливає на зниження загального ризику. Порівняйте результати для портфеля з різними частками активів.
3. Оберіть один операційний ризик у реальній або гіпотетичній організації (наприклад, збій у постачанні сировини) та проаналізуйте доцільність застосування однієї зі стратегій реагування: уникнення, зменшення, передачі або прийняття. Обґрунтуйте вибір стратегії, оцінивши потенційні втрати, вигоди та витрати на управління ризиком. Запропонуйте конкретні дії для реалізації обраної стратегії.

4. Виберіть модель інтегрованого управління ризиками (COSO ERM або ISO 31000) та проаналізуйте її застосування для комплексного управління ризиками в організації (наприклад, у банківському секторі чи ритейлі). Опишіть, як стратегічний, операційний, процесний, технологічний та культурний компоненти системи сприяють зниженню ризиків. Оцініть рівень зрілості процесів ризик-менеджменту в організації.

5. Розробіть сценарій для динамічного управління ризиками в умовах невизначеності, використовуючи концепцію реальних опціонів або антикрихкості. Оберіть проєкт (наприклад, запуск нового продукту) та опишіть, як організація може адаптуватися до змін ринкових умов, застосовуючи реальний опціон (розширення, скорочення, відкладення) або принципи антикрихкості. Проаналізуйте, як цифрова технологія (наприклад, машинне навчання) може підтримати динамічне управління.

Питання для самоконтролю:

1. У чому полягає основна відмінність між ризиком і невизначеністю за концепцією Френка Найта, і як це впливає на вибір підходів до управління ризиками в організації?

2. Як модель Марковіца використовує диверсифікацію для зниження ризику портфеля, і які ключові фактори враховуються при оцінці загального ризику?

3. Які психологічні упередження, такі як надмірна самовпевненість або ефект фрейму, впливають на оцінку ризиків у поведінковій моделі управління ризиками?

4. Які основні стратегії реагування на ризики (уникнення, зменшення, передача, прийняття) і в яких випадках доцільно застосовувати кожен з них?

ТЕМИ ПРЕЗЕНТАЦІЙ ТА ПОВІДОМЛЕНЬ:

1. Концепція Френка Найта щодо розрізнення ризику та невизначеності та її застосування в сучасному управлінні ризиками організацій.

2. Модель Марковіца як інструмент зниження ризиків через диверсифікацію: приклади використання в інвестиційному та стратегічному менеджменті.

3. Стратегії реагування на ризики (уникнення, зменшення, передача, прийняття): аналіз їх ефективності на прикладі реальних бізнес-кейсів.

4. Інтегровані системи управління ризиками (COSO ERM, ISO 31000): принципи побудови та їх роль у підвищенні стійкості організації.

Література:

1. Артим-Дрогомирецька З. Б., Негрей М. В. Економічний ризик: навч.-метод. посібник. Львів: Магнолія-2006, 2013. 320 с.

2. Аналіз моделювання і управління ризиком (в схемах та прикладах): навч. посіб. / Г. М. Азаренкова; Нац. банк України, Харків. ін-т банк. справи. Львів: Новий Світ-2000, 2011. 240 с.

3. Вітлінський В. В., Верченко П. І., Наконечний С. І. Аналіз, моделювання та управління економічним ризиком: навч. посіб. Київ : КНЕУ, 2000. 292 с.
4. Мороз В. М. Ризик-менеджмент: навчальний посібник. Харків: НТУ «ХП», 2018. 240 с. URL: <https://repository.kpi.kharkov.ua/server/api/core/bitstreams/f3be8995-acd3-4ab8-928f-1c5ff30f3584/content>.
5. Економічні ризики: методи вимірювання та управління: навчальний посібник / Н. С. Скопенко, І. В. Федулова, Л. В. Мазник, О. М. Кириченко, Л. І. Удворгелі ; за заг. ред. Н. С. Скопенко. Київ : Видавничий дім «Кондор», 2021. 348 с. URL: <https://dspace.nuft.edu.ua/handle/123456789/39065>
6. Долінський Л. Б. Фінансовий ризик-менеджмент: навчально-методичний посібник. Київ: НаУКМА, 2022. 132 с. URL: https://fpk.in.ua/images/biblioteka/4bac_finan/Dolinskyy.-Finansovyy-ryzyk-menedzhment-2022_compressed.pdf
7. Економічний ризик: методи оцінки та управління: навч. посібник / [Т. А. Васильєва, С. В. Леонов, Я. М. Кривич та ін.]; під заг. ред. д-ра екон. наук, проф. Т. А. Васильєвої, канд. екон. Наук Я. М. Кривич. – Суми : ДВНЗ “УАБС НБУ”, 2015. 208 с. URL: https://essuir.sumdu.edu.ua/bitstream/download/123456789/50229/5/Ekonomichnyi_ryzyk%20.pdf
8. Committee of Sponsoring Organizations of the Treadway Commission (COSO). Enterprise Risk Management—Integrating with Strategy and Performance. 2017. URL: https://docs.wbcsd.org/2018/10/COSO_WBCSD_ESGERM_Guidance.pdf
9. Committee of Sponsoring Organizations of the Treadway Commission (COSO). Enterprise Risk Management—Integrating with Strategy and Performance. 2017. URL: https://docs.wbcsd.org/2018/10/COSO_WBCSD_ESGERM_Guidance.pdf
10. Кібік О., Слободянюк О., Кузнецова Л. Ризик-менеджмент: навч.-метод. посібник. Одеса: Фенікс, 2024. 84 с. URL: <https://hdl.handle.net/11300/27828>
11. Боровик М. В. Ризик-менеджмент: конспект лекцій. Харків: ХНУМГ ім. О. М. Бекетова, 2023. 63 с. URL: https://eprints.kname.edu.ua/2318/1/Risk_management.pdf
12. McNeil, A. J., Frey, R., & Embrechts, P. Quantitative Risk Management: Concepts, Techniques and Tools. Princeton University Press, 2015. URL: <http://ndl.ethernet.edu.et/bitstream/123456789/30397/1/141.Alexander%20J.McNeil.pdf>
13. A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. 2010. URL: <https://ferma.eu/wp-content/uploads/2019/02/a-structured-approach-to-erm-1.pdf>

ТЕМА 4. РИЗИКИ В ЕКОНОМІЧНИХ СИСТЕМАХ

Лекційні питання:

Мета вивчення/ роботи: ознайомлення з основними типами ризиків, притаманних різним рівням економічних систем, вивчення механізмів їх виникнення, поширення та впливу на економічні процеси, а також формування компетенцій щодо ідентифікації, оцінювання та управління ризиками в макро- та мікроекономічному середовищі.

1. Системні ризики в макроекономічному середовищі.
2. Фінансові ризики банківських та небанківських установ.
3. Стратегічні та операційні ризики суб'єктів господарювання.
4. Поведінкові ризики в економічних системах.

Зміст лекції

Системні ризики в макроекономічному контексті являють собою ймовірність виникнення несприятливих подій або процесів, які здатні спричинити широкомасштабні порушення функціонування економічної системи загалом або її окремих підсистем. Їх специфіка полягає в здатності до каскадного поширення через взаємопов'язані елементи економічної системи, що призводить до синергетичного підсилення негативних ефектів [1, 2]. Природа таких ризиків обумовлена складною архітектурою сучасних економічних систем, які характеризуються високим рівнем інтеграції між різними секторами, ринками та економічними агентами [1]. Взаємозалежність між фінансовими інститутами, реальним сектором економіки, державними фінансами та зовнішньоекономічними зв'язками створює передумови для трансформації локальних порушень у системні кризи.

Макроекономічні системні ризики класифікуються за кількома критеріями. За джерелом виникнення виокремлюють ендегенні ризики, генеровані всередині економічної системи внаслідок дисбалансів у фінансовій або монетарній політиці, накопичення структурних диспропорцій чи формування спекулятивних бульбашок, та екзогенні ризики, спричинені зовнішніми шоками, такими як природні катастрофи, геополітичні конфлікти, пандемії або різкі зміни цін на світових товарних ринках. За механізмом поширення розрізняють ризики зараження, які передаються через прямі зв'язки між економічними агентами, та ризики спільної експозиції, що виникають внаслідок одночасного впливу несприятливих факторів на різні сегменти економіки. Ризики зараження особливо характерні для фінансової сфери, де банкрутство одного великого фінансового інституту може ініціювати ланцюгову реакцію неплатежів серед його контрагентів [1, 5].

Прояви системних ризиків у макроекономічному середовищі включають фінансові кризи, які характеризуються різким скороченням доступності кредитних ресурсів, волатильністю фінансових ринків та дестабілізацією банківської системи. Валютні кризи виявляються в різкій девальвації національної валюти, відпливі капіталу та порушенні платіжного балансу.

Боргові кризи виникають через неспроможність держави або приватного сектору обслуговувати накопичені зобов'язання, що може призвести до дефолту та реструктуризації боргу. Особливою категорією є структурні кризи, які відображають фундаментальні дисбаланси в економічній системі та вимагають кардинальних змін у моделі економічного розвитку. Такі кризи часто супроводжуються тривалою рецесією, високим рівнем безробіття та соціальною напругою.

Управління системними ризиками на макроекономічному рівні вимагає координації дій різних регулятивних органів та застосування комплексного підходу, що поєднує макропруденційну політику для зміцнення стійкості фінансової системи, активну фіскальну політику для згладжування економічних коливань та гнучку монетарну політику для забезпечення цінової стабільності й підтримки економічного зростання. Переходячи до аналізу ризиків на рівні окремих фінансових установ, слід відзначити, що системні ризики часто перетинаються з фінансовими ризиками банківських та небанківських установ, формуючи комплексну картину загроз для економічної стабільності [1, 5, 6].

Фінансові ризики банківських установ являють собою ймовірність виникнення збитків або недоотримання запланованих доходів внаслідок впливу різноманітних факторів невизначеності, притаманних банківській діяльності [5, 6]. Специфіка цих ризиків обумовлена роллю банків як фінансових посередників, які залучають кошти вкладників, надають кредити позичальникам і здійснюють трансформацію строків погашення, валют та ризиків. Кредитний ризик є найбільш значущим і полягає в можливості невиконання позичальниками зобов'язань перед банком. Він має багатофакторну природу, залежну від фінансового стану позичальника, якості забезпечення, макроекономічних умов та ефективності кредитних процедур банку. Управління кредитним ризиком передбачає ретельний аналіз кредитоспроможності позичальників, диверсифікацію кредитного портфеля, створення адекватних резервів під можливі втрати та застосування кредитних деривативів для передачі ризику.

Ринковий ризик виникає внаслідок несприятливих змін ринкових параметрів, таких як процентні ставки, валютні курси, ціни на цінні папери та товари. Процентний ризик є особливо актуальним через невідповідність між строками погашення активів та зобов'язань. Валютний ризик проявляється при відкритих валютних позиціях або кредитуванні в іноземній валюті клієнтів, доходи яких номіновані в національній валюті. Ризик ліквідності охоплює ризик фінансування, пов'язаний з можливістю неспроможності банку профінансувати зростання активів або виконати зобов'язання без значних витрат, та ринковий ризик ліквідності, який полягає в неможливості швидко закрити позицію за ринковою ціною через недостатню глибину ринку.

Операційний ризик [5, 6] включає можливі збитки внаслідок неадекватності або збоїв внутрішніх процесів, дій персоналу, функціонування систем чи зовнішніх подій. Він охоплює правовий ризик, але виключає

стратегічний та репутаційний ризики, набуваючи особливої актуальності з розвитком інформаційних технологій та цифровізацією банківських послуг [6]. Небанківські фінансові установи, такі як страхові компанії, пенсійні фонди, інвестиційні компанії, фонди та кредитні спілки, характеризуються специфічними профілями ризиків, обумовленими особливостями їх бізнес-моделей та регулятивного середовища [5].

Страхові компанії стикаються зі страховим ризиком, пов'язаним з невизначеністю щодо часу, частоти та розміру страхових виплат, актуарним ризиком через можливу неточність розрахунків та прогнозів, а також інвестиційним ризиком через необхідність інвестування резервів для забезпечення їх дохідності. Пенсійні фонди наражаються на довгострокові демографічні ризики, пов'язані зі змінами в структурі населення, тривалістю життя та рівнем народжуваності, а інвестиційні ризики є критичними через потребу в забезпеченні дохідності активів протягом тривалих періодів. Інвестиційні компанії та фонди підлягають ринковим ризикам через волатильність цін на інструменти, ризикам ліквідності при масових вилученнях коштів та операційним ризикам, включаючи ті, що пов'язані з управлінням активами [5].

Регулятивний підхід до управління ризиками у фінансовому секторі ґрунтується на принципах пропорційності, всебічності та превентивності. Банки дотримуються вимог щодо достатності капіталу відповідно до стандартів Базель III, які включають мінімальні коефіцієнти капіталу, буферні вимоги та показники ліквідності. Небанківські установи регулюються адаптованими нормативами. Такі фінансові ризики тісно переплітаються зі стратегічними та операційними ризиками суб'єктів господарювання, оскільки фінансові установи є частиною ширшого економічного ландшафту, де стратегічні рішення впливають на операційну стійкість [1, 2, 5, 6].

Стратегічні ризики суб'єктів господарювання являють собою ймовірність негативних наслідків для організації внаслідок неефективних стратегічних рішень, неналежної реалізації стратегій або неадекватного реагування на зміни зовнішнього середовища. Такі ризики мають довгостроковий характер і можуть суттєво вплинути на конкурентні позиції підприємства, його ринкову вартість та перспективи розвитку. Їх природа тісно пов'язана з процесами стратегічного планування та управління: ризики планування включають вибір неправильних цілей, неточний аналіз конкурентного середовища, переоцінку власних можливостей чи недооцінку загроз; ризики реалізації полягають у неефективному впровадженні ініціатив через недостатність ресурсів, опір змінам або неадекватність організаційної структури [2, 3].

Технологічні стратегічні ризики пов'язані з швидким технологічним розвитком і загрозою відставання, що особливо актуально в епоху цифрової трансформації, коли традиційні бізнес-моделі переглядаються. Ринкові стратегічні ризики охоплюють вибір сегментів ринку, позиціонування продукції, цінову стратегію та канали розподілу, де неправильна оцінка

трендів чи дій конкурентів призводить до втрат. Операційні ризики суб'єктів господарювання охоплюють загрози, пов'язані з повсякденним функціонуванням, маючи коротко- чи середньостроковий характер і стосуючись ефективності бізнес-процесів [2, 3].

Процесні операційні ризики виникають через неефективність процесів, проявляючись у помилках виробництва, затримках поставок чи порушеннях контролю; управління ними вимагає аналізу, оптимізації та автоматизації. Кадрові операційні ризики пов'язані з людським фактором, включаючи недостатню кваліфікацію, плинність кадрів чи шахрайство, і є критичними для знаннево-орієнтованих підприємств. Технологічні операційні ризики стосуються збоїв IT-систем, кібератак чи відмов обладнання. Зовнішні операційні ризики включають природні катастрофи, терористичні акти, страйки чи зміни регуляцій [2, 3].

Інтегроване управління стратегічними та операційними ризиками передбачає створення комплексної системи ризик-менеджменту, що охоплює ідентифікацію, оцінку, розробку стратегій реагування, контрольні заходи та моніторинг. Такі ризики посилюються поведінковими факторами, оскільки рішення суб'єктів господарювання залежать від психологічних аспектів поведінки економічних агентів [2, 4].

Поведінкові ризики в економічних системах являють собою ймовірність негативних наслідків внаслідок систематичних відхилень економічних агентів від раціональної поведінки, передбаченої класичною економічною теорією. Вони ґрунтуються на психологічних особливостях прийняття рішень в умовах невизначеності та обмеженої інформації. Теоретичним підґрунтям є поведінкова економіка, яка інтегрує психологічні інсайти в економічний аналіз, включаючи обмежену раціональність (використання евристик замість оптимізації), когнітивні упередження та роль емоцій.

Когнітивні упередження є основним джерелом: упередження підтвердження призводить до вибіркової інтерпретації інформації; ефект якоря – до залежності від першої інформації; упередження доступності – до переоцінки резонансних подій; ефект самовпевненості – до недостатньої диверсифікації. На фінансових ринках поведінкові ризики проявляються в стадній поведінці, що формує бульбашки чи паніку, та ефекті диспозиції, де прибутки фіксуються передчасно, а збитки утримуються. У корпоративному управлінні – в надмірній самовпевненості менеджменту чи ескалації зобов'язань. Групові ризики включають групомислення та дифузії відповідальності [4].

Макроекономічні поведінкові ризики посилюють циклічність через хвилі оптимізму/песимізму, ускладнюючи планування. Управління вимагає розуміння механізмів, структурованих процесів для зменшення упереджень, культури критичного мислення та використання технологій (алгоритмів, ШІ). Важливим є етичне застосування знань для захисту споживачів від маніпуляцій та розвитку стандартів у економічній практиці [4].

Розуміння та управління ризиками в економічних системах є ключовим елементом забезпечення стабільності та стійкості як на макро-, так і на мікроекономічному рівнях. Системні, фінансові, стратегічні, операційні та поведінкові ризики формують складну мережу викликів, які потребують комплексного підходу до аналізу та управління [1, 2, 3, 4, 5, 6]. Координація макропруденційної, фіскальної та монетарної політики, інтегроване управління ризиками в організаціях, а також врахування психологічних аспектів прийняття рішень дозволяють мінімізувати негативні наслідки та сприяти сталому економічному розвитку. Для здобувачів освітньо-наукового рівня вивчення цих ризиків відкриває можливості для розробки ефективних стратегій, спрямованих на підвищення конкурентоспроможності та стійкості економічних систем у динамічному глобальному середовищі.

ПИТАННЯ ДО ПРАКТИЧНОГО ЗАНЯТТЯ

1. Аналіз системних ризиків у макроекономічному середовищі: методи оцінки та управління.
2. Моделювання впливу фінансових ризиків на діяльність банківських установ.
3. Стратегічні та операційні ризики суб'єктів господарювання.
4. Поведінкові ризики в економічних системах: вплив когнітивних упереджень на прийняття рішень.
5. Розробка заходів із мінімізації ризиків у контексті економічної нестабільності.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ:

1. Описати основні джерела системних ризиків у макроекономічному середовищі України, враховуючи вплив зовнішніх шоків (наприклад, геополітичних конфліктів або змін цін на енергоносії).
2. Розрахувати потенційні втрати банківської установи від кредитного ризику на основі гіпотетичних даних про кредитний портфель (обсяг кредитів – 100 млн. грн., частка проблемних кредитів – 10%, рівень покриття резервами – 50%).
3. Описати приклади операційних ризиків на основі реального кейсу українського підприємства (наприклад, збої в ІТ-системах або помилки персоналу).
4. Проаналізувати вплив поведінкових ризиків на інвестиційні рішення, використовуючи приклад фондового ринку України.
5. Розробити план заходів із управління стратегічними ризиками для малого підприємства в умовах цифровізації бізнес-процесів.
6. Оцінити вплив валютної кризи на діяльність експортоорієнтованого підприємства, враховуючи девальвацію гривні на 20%.
7. Скласти матрицю ризиків для суб'єкта господарювання, визначивши ймовірність та наслідки основних типів ризиків (фінансових, операційних, стратегічних).

Питання для самоконтролю:

1. Які основні джерела системних ризиків у макроекономічному середовищі та як вони впливають на економічну стабільність?
2. У чому полягає різниця між кредитним, ринковим та операційним ризиками банківських установ?
3. Як стратегічні ризики впливають на конкурентоспроможність суб'єктів господарювання?
4. Які когнітивні упередження найчастіше проявляються в економічних рішеннях та як їх можна мінімізувати?
5. Які інструменти макропруденційної політики застосовуються для управління системними ризиками?

ТЕМИ ПРЕЗЕНТАЦІЙ ТА ПОВІДОМЛЕНЬ:

1. Вплив глобальних економічних криз на системні ризики в Україні.
2. Стратегії управління фінансовими ризиками в банківському секторі України.
3. Поведінкова економіка як роль когнітивних упереджень у формуванні економічних рішень.
4. Операційні ризики в цифровій економіці: виклики та рішення для українських підприємств.

Література:

1. Пріоритети розвитку фінансової системи України в умовах євроінтеграційних процесів : монографія / Л. Л. Гриценко, І. М. Боярко, Т. А. Васильєва та ін. ; за заг. ред. д-ра екон. наук Л. Л. Гриценко. Суми : Сумський державний університет, 2021. 379 с. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/83909/3/Hrytsenko_finansova_systema.pdf
2. Скопенко Н. С. (за заг. ред.), Федулова І. В., Мазник Л. В., Кириченко О. М., Удворгелі Л. І. Економічні ризики: методи вимірювання та управління: навч. посібн., Київ: НУХТ, 2021. 344 с.
3. Донець Л. І. Економічні ризики та методи їх вимірювання навч. посіб. К. : Центр навчальної літератури, 2006. 312 с. URL: https://shron1.chtyvo.org.ua/Donets_Liubov/Ekonomichni_ryzyky_ta_metody_yikh_vymiruvannia.pdf
4. Біла І. С. Поведінкова економіка в державному регулюванні бізнесу // *Економіка та суспільство*. 2024. № 65. URL: <https://doi.org/10.32782/2524-0072/2024-65-51>
5. Панченко О., Маслюк О., Гориленко А. Банківські ризики як об'єкт страхування в сучасних умовах. *Проблеми і перспективи економіки та управління*. 2021. № 4(24). С. 146–154. URL: <http://ppeu.stu.cn.ua/article/view/228214>
6. Петик Л., Міщенко К. Оцінка банківських ризиків в умовах війни. *Економіка та суспільство*. 2024. № 65. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4476?>

ТЕМА 5. КІБЕРРИЗИКИ ТА РИЗИКИ В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ

Лекційні питання:

Мета вивчення/ роботи: ознайомлення з сучасними видами кіберризиків та ризиків інформаційних технологій, вивчення методів їх ідентифікації, оцінки та управління в умовах цифровізації економіки, а також формування компетенцій щодо забезпечення інформаційної безпеки організацій та мінімізації технологічних ризиків у контексті цифрової трансформації бізнес-процесів.

1. Класифікація та характеристика кіберризиків.
2. Інформаційна безпека та захист персональних даних.
3. Ризики цифрової трансформації бізнес-процесів.
4. Ризики штучного інтелекту та автоматизації.

Зміст лекції

Кіберризики являють собою ймовірність виникнення збитків або порушень нормального функціонування організації внаслідок реалізації загроз у кіберпросторі, спрямованих проти інформаційних систем, мереж, даних або технологічних процесів [1, 2, 3, 5, 7]. Специфіка кіберризиків полягає в їх транснаціональному характері, високій швидкості поширення, складності ідентифікації джерела атак та потенційно катастрофічних наслідках для функціонування критично важливої інфраструктури [1, 3, 5].

Еволюція кіберризиків тісно пов'язана з розвитком інформаційних технологій та зростанням залежності суспільства від цифрових систем [3, 5, 7]. Якщо на початкових етапах розвитку комп'ютерних мереж кіберзагрози мали переважно аматорський характер та обмежений вплив, то сучасні кіберризики характеризуються професіоналізацією зловмисників, використанням складних технічних засобів та координованими атаками на критично важливу інфраструктуру [1, 3, 5].

За джерелом походження кіберризики класифікуються на зовнішні, що виникають з бок у сторонніх зловмисників, включаючи хакерські групи, кіберзлочинні організації, державні актори та терористичні угруповання, та внутрішні, пов'язані з діями власних співробітників організації, які можуть бути як навмисними, так і ненавмисними [1, 3, 7]. Внутрішні загрози особливо небезпечні через привілейований доступ інсайдерів до критично важливих систем та інформації [1, 5].

За типом впливу розрізняють кіберризики конфіденційності, спрямовані на несанкціоноване розкриття інформації, цілісності, що полягають у неавторизованій модифікації даних або систем, та доступності, які призводять до порушення нормального функціонування інформаційних ресурсів. Дана класифікація відповідає класичній тріаді інформаційної безпеки [3, 5] CIA (Confidentiality, Integrity, Availability) [3, 7].

Технічні кіберризики включають експлойти програмного забезпечення, що використовують вразливості в операційних системах, додатках або мережевих протоколах для несанкціонованого доступу до систем [1, 3, 5]. Малваре охоплює широкий спектр шкідливого програмного забезпечення, включаючи віруси, черв'яки, троянські програми, шпигунське програмне забезпечення та програми-вимагачі [1, 5]. Атаки типу відмови в обслуговуванні спрямовані на порушення доступності сервісів через перевантаження систем [3, 5].

Соціоінженерні кіберризики базуються на психологічній маніпуляції людьми для отримання несанкціонованого доступу до інформації або систем [4, 7]. Фішинг та його різновиди, такі як спір-фішинг та вішинг, використовують обманні повідомлення для отримання конфіденційної інформації. Претекстінг полягає в створенні вигаданих сценаріїв для обману жертв та отримання доступу до захищених ресурсів [4].

Сучасні кіберризики характеризуються зростаючою складністю та комплексністю [1, 3, 5]. Багатоетапні постійні загрози являють собою тривалі та цільові кампанії, спрямовані на конкретні організації або сектори економіки [1, 5]. Такі атаки можуть тривати місяцями або роками, поступово проникаючи все глибше в інфраструктуру жертви [3].

Атаки на ланцюг постачання представляють особливу категорію ризиків, коли зловмисники компрометують довірених постачальників програмного забезпечення або апаратних компонентів для досягнення доступу до систем кінцевих користувачів [1, 3]. Такі атаки особливо складні для виявлення та можуть мати широкомасштабний вплив [5].

Кіберризики критично важливої інфраструктури охоплюють загрози енергетичним системам, транспортній інфраструктурі, системам водопостачання, фінансовим мережам та іншим системам, порушення яких може мати катастрофічні наслідки для суспільства. Такі ризики підкреслюють стратегічне значення кібербезпеки на національному рівні.

Економічні наслідки кіберризиків включають прямі фінансові втрати від крадіжки коштів або шкоди обладнанню, непрямі втрати від порушення бізнес-процесів та втрати продуктивності, репутаційні збитки та втрату довіри клієнтів, а також витрати на відновлення систем та підвищення рівня безпеки. Додатково виникають регулятивні ризики, пов'язані з можливими санкціями за порушення вимог щодо захисту даних [1, 3, 5, 7].

Інформаційна безпека являє собою комплекс організаційних, технічних та правових заходів, спрямованих на забезпечення захисту інформації від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення [3, 5, 7]. Сучасна концепція інформаційної безпеки виходить за межі традиційного розуміння захисту даних та охоплює забезпечення стійкості всієї інформаційної екосистеми організації [3, 5].

Фундаментальними принципами інформаційної безпеки є конфіденційність, що забезпечує доступ до інформації лише авторизованих користувачів, цілісність, яка гарантує точність та повноту інформації протягом

всього її життєвого циклу, та доступність, що передбачає можливість своєчасного та надійного доступу до інформації для авторизованих користувачів [3, 7]. До цієї класичної тріади часто додають автентичність, що підтверджує справжність інформації та її джерела, та невідомність, яка забезпечує неможливість заперечення факту участі в інформаційному обміні [3].

Системний підхід до інформаційної безпеки базується на концепції багаторівневого захисту, який включає фізичний рівень безпеки, що охоплює захист приміщень, обладнання та носіїв інформації від несанкціонованого фізичного доступу, мережевий рівень, спрямований на захист мережевої інфраструктури та каналів передачі даних, системний рівень, що забезпечує безпеку операційних систем та системного програмного забезпечення, прикладний рівень, який стосується захисту додатків та баз даних, та рівень даних, що безпосередньо захищає інформаційні ресурси.

Управління ідентифікацією та доступом є критично важливим компонентом інформаційної безпеки. Системи автентифікації повинні надійно встановлювати особу користувача через різні фактори, включаючи знання (паролі, PIN-коди), володіння (смарт-карти, токени) та біометричні характеристики. Багатофакторна автентифікація значно підвищує рівень безпеки через використання комбінації різних факторів [3, 7].

Авторизація та контроль доступу визначають, які дії може виконувати автентифікований користувач. Моделі контролю доступу включають дискреційний контроль, де власники ресурсів самостійно визначають права доступу, обов'язковий контроль, який базується на мітках безпеки та рівнях допуску, та рольовий контроль, що надає права доступу на основі ролей користувачів в організації.

Криптографічні методи захисту є фундаментальним інструментом забезпечення інформаційної безпеки. Симетричне шифрування використовує один ключ для шифрування та дешифрування даних, забезпечуючи високу швидкість обробки великих обсягів інформації. Асиметричне шифрування використовує пару відкритий-закритий ключ, що дозволяє безпечно обмінюватися ключами та забезпечувати цифрові підписи [3, 5].

Захист персональних даних набув особливої актуальності в умовах цифровізації та посилення регулятивних вимог. Персональні дані включають будь-яку інформацію, що дозволяє прямо або опосередковано ідентифікувати фізичну особу. Спеціальні категорії персональних даних, такі як інформація про расове або етнічне походження, політичні переконання, релігійні вірування, стан здоров'я або сексуальну орієнтацію, потребують підвищеного рівня захисту.

Європейський Загальний Регламент із Захисту Даних встановив глобальні стандарти захисту персональних даних, включаючи принципи законності, справедливості та прозорості обробки, обмеження мети, мінімізації даних, точності, обмеження зберігання, цілісності та

конфіденційності. Регламент також запровадив концепцію підзвітності, згідно з якої контролери даних повинні демонструвати дотримання всіх принципів.

Права суб'єктів даних включають право на інформацію про обробку їх персональних даних, право доступу до даних, право на виправлення неточних даних, право на видалення даних у певних обставинах, право на обмеження обробки, право на портабельність даних та право заперечувати проти обробки. Ці права створюють додаткові зобов'язання для організацій та потребують впровадження відповідних технічних та організаційних заходів.

Оцінка впливу на захист даних є обов'язковою для операцій обробки, які можуть створювати високий ризик для прав та свобод фізичних осіб. Така оцінка повинна включати опис операцій обробки, аналіз необхідності та пропорційності, оцінку ризиків для суб'єктів даних та заходи для зниження цих ризиків.

Технічні та організаційні заходи захисту персональних даних включають псевдонімізацію та шифрування даних, забезпечення постійної конфіденційності, цілісності, доступності та стійкості систем обробки, здатність швидко відновлювати доступність та доступ до даних у випадку технічного або фізичного інциденту, та регулярні процедури тестування, оцінки та підтвердження ефективності заходів безпеки [3, 5, 7].

Цифрова трансформація бізнес-процесів являє собою фундаментальну зміну способу функціонування організацій через інтеграцію цифрових технологій у всі аспекти діяльності, що призводить до зміни операційних моделей, створення нової вартості для клієнтів та трансформації організаційної культури. Однак цей процес супроводжується виникненням нових категорій ризиків, які потребують ретельного аналізу та управління.

Стратегічні ризики цифрової трансформації пов'язані з можливістю вибору неправильної стратегії цифровізації або неефективної її реалізації. Ризик технологічного невідповідності виникає, коли обрані технологічні рішення не відповідають довгостроковим потребам бізнесу або швидко застарівають. Ризик недооцінки масштабу змін полягає в неадекватній оцінці складності та ресурсоемності процесу трансформації, що може призвести до перевитрати бюджету та затримок у реалізації проектів.

Культурні та організаційні ризики є одними з найбільш критичних для успіху цифрової трансформації. Опір змінам з боку співробітників може значно уповільнити або навіть призупинити процес трансформації. Даний опір часто обумовлений страхом втрати роботи, необхідністю освоєння нових навичок або зміною звичних робочих процедур. Ризик втрати ключових співробітників може виникнути через неспроможність організації забезпечити необхідне навчання та підтримку персоналу в процесі адаптації до нових технологій.

Технологічні ризики цифрової трансформації включають ризики інтеграції систем, що виникають при об'єднанні нових цифрових рішень з існуючими застарілими системами. Несумісність технологій може призвести до порушень у роботі критично важливих бізнес-процесів. Ризики

масштабування пов'язані з можливістю неспроможності нових систем впоратися зі зростаючим навантаженням або розширенням функціональності.

Хмарні технології, які є ключовим компонентом багатьох ініціатив цифрової трансформації, створюють специфічні ризики. Ризики безпеки даних у хмарі включають можливість несанкціонованого доступу до конфіденційної інформації, втрати контролю над даними та залежності від постачальників хмарних послуг. Ризики доступності хмарних сервісів можуть призвести до порушень у роботі критично важливих бізнес-процесів.

Ризики взаємозалежності виникають через зростаючу складність та інтеграцію цифрових систем. Збій в одному компоненті може спричинити каскадний ефект, що призведе до порушення роботи всієї системи. Безпосередньо для організацій, які впроваджують комплексні цифрові екосистеми з множинними взаємопов'язаними компонентами [3, 7].

Регулятивні ризики цифрової трансформації обумовлені необхідністю дотримання зростаючої кількості правових вимог щодо захисту даних, кібербезпеки та цифрової звітності. Швидкі зміни в регулятивному середовищі можуть призвести до ситуації, коли нові цифрові рішення не відповідають актуальним правовим вимогам.

Економічні ризики включають ризик перевитрати бюджету на проекти цифрової трансформації, що часто пов'язано з недооцінкою складності впровадження або необхідності додаткових інвестицій у навчання персоналу та зміну процесів. Ризик невиправдання очікувань щодо рентабельності інвестицій може виникнути через завищені прогнози ефективності або недооцінку часу, необхідного для досягнення запланованих результатів.

Ризики кібербезпеки значно зростають в процесі цифрової трансформації через розширення поверхні атак та збільшення кількості точок входу для потенційних зловмисників. Інтернет речей створює нові вразливості через підключення до мережі пристроїв, які можуть мати обмежені можливості безпеки. Мобільні додатки та BYOD-політики розширюють периметр безпеки за межі традиційних корпоративних мереж [3].

Управління ризиками цифрової трансформації потребує інтегрованого підходу, який включає стратегічне планування з урахуванням можливих ризиків, поетапне впровадження з регулярною оцінкою проміжних результатів, інвестиції в навчання та розвиток персоналу, створення культури інновацій та адаптивності, впровадження надійних систем кібербезпеки та забезпечення відповідності регулятивним вимогам [3, 5, 7].

Штучний інтелект та автоматизація представляють революційні технології, які кардинально змінюють способи ведення бізнесу та функціонування суспільства. Однак їх впровадження супроводжується виникненням нових категорій ризиків, які мають як технічний, так і етичний, соціальний та економічний характер [2, 3, 6].

Технічні ризики систем штучного інтелекту включають ризики алгоритмічних помилок, які можуть виникати через недоліки в дизайні алгоритмів, неякісні тренувальні дані або неправильну інтерпретацію

результатів. Особливо критичними є помилки в системах, що приймають рішення в галузях охорони здоров'я, фінансових послуг або автономного транспорту, де наслідки можуть бути катастрофічними.

Ризики якості даних є фундаментальними для систем машинного навчання, оскільки якість вихідних результатів безпосередньо залежить від якості вхідних даних. Неповні, неточні або упереджені дані можуть призвести до систематичних помилок у роботі II-систем. Ризики дрейфу даних виникають, коли характеристики даних змінюються з часом, що може призвести до деградації продуктивності моделей машинного навчання.

Проблема "чорної скриньки" є особливо актуальною для складних моделей глибокого навчання, рішення яких важко пояснити та інтерпретувати. Відсутність прозорості може створювати регулятивні ризики в галузях з високими вимогами до підзвітності, таких як фінансові послуги або медицина, що ускладнює процес виявлення та виправлення помилок в алгоритмах [2, 4, 6].

Етичні ризики III включають проблеми алгоритмічної упередженості, коли системи II відтворюють або підсилюють існуючі соціальні упередження. Це може призвести до дискримінації окремих груп населення в процесах прийняття рішень щодо працевлаштування, кредитування, страхування або правоохоронної діяльності. Упередженість може виникати на різних етапах розробки II-систем, від збору даних до дизайну алгоритмів та інтерпретації результатів.

Ризики приватності та захисту персональних даних особливо актуальні для II-систем, які часто потребують великих обсягів персональних даних для навчання. Технології розпізнавання облич, аналізу поведінки та прогнозової аналітики можуть створювати загрози для приватності громадян. Ризик реідентифікації полягає в можливості встановлення особи людини навіть з анонімізованих або псевдонімізованих даних.

Соціально-економічні ризики автоматизації включають ризик технологічного безробіття, коли впровадження II та роботизації призводить до скорочення робочих місць швидшими темпами, ніж створення нових. Особливо вразливими є професії, що включають рутинні та передбачувані завдання. Ризик поляризації ринку праці може призвести до зростання нерівності між високооплачуваними робочими місцями, що потребують високої кваліфікації, та низькооплачуваними послугами.

Системні ризики III пов'язані з можливістю одночасного впливу на множинні сфери суспільства та економіки. Концентрація II-технологій у руках невеликої кількості великих технологічних компаній може призвести до монополізації та зниження конкуренції. Ризики автономії полягають у можливості прийняття II-системами рішень, які виходять за межі запланованих параметрів або конфліктують з людськими цінностями [2, 6].

Ризики кібербезпеки II-систем включають можливість адверсаріальних атак, коли зловмисники навмисно спотворюють вхідні дані для маніпулювання поведінкою II-систем. Атаки на моделі машинного навчання

можуть включати отруєння даних під час навчання, evasion-атаки під час роботи системи та model extraction attacks для крадіжки інтелектуальної власності.

Регулятивні та правові ризики ШІ обумовлені відставанням законодавчої бази від темпів технологічного розвитку. Питання юридичної відповідальності за рішення, прийняті ІІ-системами, залишаються недостатньо врегульованими. Міжнародні відмінності в підходах до регулювання ШІ можуть створювати додаткові складності для глобальних компаній [2, 4, 7].

Ризики надмірної залежності від ІІ-систем включають можливість втрати критичних навичок людьми, деградації професійних компетенцій та зниження здатності до критичного мислення. Організації можуть стати занадто залежними від автоматизованих рішень, втрачаючи здатність до ручного управління в разі збоїв систем.

Управління ризиками ШІ та автоматизації потребує мультидисциплінарного підходу, який включає технічні заходи з забезпечення надійності та безпеки систем, етичні принципи розробки та використання ІІ, соціальні програми перекваліфікації та підтримки працівників, регулятивні механізми забезпечення підзвітності та прозорості, міжнародну співпрацю в розробці стандартів та норм, та постійний моніторинг впливу технологій на суспільство.

Принципи відповідального ІІ включають справедливість та недискримінацію, прозорість та пояснюваність рішень, підзвітність розробників та користувачів, повагу до людської автономії та гідності, забезпечення конфіденційності та безпеки даних, та сприяння загальному благополуччю суспільства. Такі принципи повинні бути інтегровані в процес розробки та впровадження ІІ-систем на всіх етапах їх життєвого циклу [2, 6].

Кіберризики та ризики інформаційних технологій становлять значні виклики для сучасних організацій у контексті цифровізації економіки. Забезпечення інформаційної безпеки, захист персональних даних, управління ризиками цифрової трансформації та відповідальний підхід до використання штучного інтелекту є невід’ємними складовими ефективного менеджменту в умовах технологічної революції. Інтегрований підхід, що поєднує технічні, організаційні та правові заходи, дозволяє організаціям не лише мінімізувати вразливості, але й трансформувати виклики в можливості для інноваційного розвитку. Опанування цих питань відкриває перспективи для створення стійких бізнес-моделей, здатних адаптуватися до викликів цифрової епохи.

ПИТАННЯ ДО ПРАКТИЧНОГО ЗАНЯТТЯ

1. Ідентифікація та класифікація кіберризиків у діяльності організацій.
2. Розробка системи інформаційної безпеки для малого підприємства.
3. Оцінка ризиків цифрової трансформації на прикладі української компанії.
4. Аналіз етичних та соціальних ризиків використання штучного інтелекту в бізнес-процесах.

5. Моделювання кібератаки та розробка плану реагування на основі сценарію.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ:

1. Описати основні типи кіберризиків (технічні, соціоінженерні, атаки на ланцюг постачання) та їх вплив на діяльність організацій в Україні.
2. Розрахувати потенційні економічні втрати від кібератаки типу ransomware для підприємства з річним доходом 50 млн грн, враховуючи простий бізнес-процесів на 3 дні та витрати на відновлення даних (10% доходу).
3. Описати принципи інформаційної безпеки (CIA) та запропонувати заходи для їх забезпечення в організації з 50 співробітниками.
4. Розробити план оцінки впливу на захист персональних даних (DPIA) для компанії, яка впроваджує хмарні технології.
5. Оцінити ризики впровадження штучного інтелекту в автоматизації бізнес-процесів, враховуючи проблему "чорної скриньки" та алгоритмічну упередженість.
6. Скласти перелік технічних та організаційних заходів для захисту від соціоінженерних атак (фішинг, претекстінг) в умовах BYOD-політики.

Питання для самоконтролю:

1. Які основні типи кіберризиків та як вони класифікуються за джерелом походження і типом впливу?
2. Які принципи інформаційної безпеки є основою захисту персональних даних?
3. Як ризики цифрової трансформації впливають на операційну діяльність організацій?
4. Які етичні та соціально-економічні ризики пов'язані з використанням штучного інтелекту?
5. Які технічні та організаційні заходи необхідні для управління кіберризиками в хмарних технологіях?

ТЕМИ ПРЕЗЕНТАЦІЙ ТА ПОВІДОМЛЕНЬ:

1. Кіберризики в українському бізнес-середовищі.
2. Захист персональних даних в умовах дії GDPR.
3. Цифрова трансформація в Україні: баланс між інноваціями та ризиками.
4. Етичні аспекти використання штучного інтелекту в Україні.

Література:

1. Кришталь Г., Самофалова М., Сахно Л., Федина, В., Мокієнко Т., Ермолаєва М. Кіберризики у фінансовій та банківській системі: аналіз прямих і систематичних втрат. *Financial and Credit Activity Problems of Theory and*

Practice, 2(61), 2025. С. 125–140. URL: <https://doi.org/10.55643/fcaptp.2.61.2025.4672>

2. Трофименко О. Г., Логінова Н.І., Соколов А. В., Чикунів П. О., Ахматметьєва Г. В. Штучний інтелект у військовій сфері. Кібербезпека: освіта, наука, техніка. 2024. № 1(25). С. 199-212. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/600>

3. Муравський В.В. Облік та кібербезпека. : монографія. Тернопіль : ЗУНУ. 2023. 200 с. URL: <https://dspace.wunu.edu.ua/bitstream/316497/52083/1/%D0%9C%D1%83%D1%80%D0%B0%D0%B2%D1%81%D1%8C%D0%BA%D0%B8%D0%B9%20%D0%92.%D0%92.%20-%D0%9E%D0%B1%D0%BB%D1%96%D0%BA%20%D1%82%D0%B0%20%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0.pdf>

4. Біла І. С. Поведінкова економіка в державному регулюванні бізнесу. *Економіка та суспільство*. 2024. № 65. URL: <https://doi.org/10.32782/2524-0072/2024-65-51>

5. Панченко О., Маслюк О., Гориленко А. Банківські ризики як об'єкт страхування в сучасних умовах. *Проблеми і перспективи економіки та управління*. 2021. № 4(24). С. 146–154. URL: <http://ppeu.stu.cn.ua/article/view/228214>

6. Петик Л., Міщенко К. Оцінка банківських ризиків в умовах війни. *Економіка та суспільство*. 2024. № 65. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4476>

7. Гайдур Г.І., Гахов С.О., Скибун О.Ж. Оцінка стану кібербезпеки критичної інфраструктури з використанням штучного інтелекту. *Сучасний захист інформації*, 2025, № 2(62). URL: [file:///C:/Users/O_S/Downloads/3233-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-9756-1-10-20250628%20\(2\).pdf](file:///C:/Users/O_S/Downloads/3233-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-9756-1-10-20250628%20(2).pdf)

8. Слободянюк О.В., Калмикова Н.Ю. Фінансова складова економічної безпеки розвитку суб'єктів господарювання. Наукові інновації та передові технології. (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка») : журнал. 2023. № 13(27) 2023. С. 574-584. URL: <http://perspectives.pp.ua/index.php/nauka/issue/view/188/279>

9. Koval, V., Gonchar, V., Udovychenko, V., Kalinin, O., Slobodianiuk, O., & Soloviova, O. (2023). Risk management analysis of environmental investment in economic security. *Journal of Geology, Geography and Geoecology*, 32(3), 540-549. URL: <https://geology-dnu.dp.ua/index.php/GG/article/view/1040>

10. Harkava V., Kibik O., Tytok V., Klim N., Cervinskaya L., Voit S. Economic security of the country for stable development. *AD ALTA: Journal of Interdisciplinary research*. 2021. 11/02-XXII. P. 138-142. <http://www.magnanimitas.cz/11-02-xxii>

ТЕМА 6. РИЗИКИ СТАЛОГО РОЗВИТКУ

Лекційні питання:

Мета вивчення/ роботи: ознайомлення з концептуальними засадами ризиків сталого розвитку, вивчення взаємозв'язків між екологічними, соціальними та економічними факторами ризику, а також формування компетенцій щодо ідентифікації, оцінки та управління ризиками, що можуть загрожувати довгостроковій стійкості організацій і суспільства в контексті концепції ESG та Цілей сталого розвитку ООН.

1. Екологічні ризики та кліматичні зміни.
2. Соціальні ризики та демографічні виклики.
3. ESG-ризики в корпоративному управлінні.
4. Інтегроване управління ризиками сталого розвитку.

Зміст лекції

Кліматичні зміни становлять фундаментальний виклик для глобального та національного сталого розвитку, генерують системні ризики, що впливають на всі сфери життєдіяльності організацій і суспільства. Фізичні ризики кліматичних змін включають гострі ризики, пов'язані з екстремальними погодними явищами - посухами, повеннями, ураганами, лісовими пожежами, та хронічні ризики, що виникають внаслідок довгострокових змін клімату - підвищення температури, зміни опадів, підвищення рівня моря. Перехідні ризики виникають у процесі трансформації економіки до низьковуглецевої моделі та включають регуляторні зміни, технологічні зрушення, ринкові трансформації та репутаційні ризики [1, 5, 6, 8].

Дослідження UNEP FI (2024) демонструють, що кліматичний ризик-ландшафт характеризується зростаючою складністю взаємозв'язків між фізичними та перехідними ризиками. Організації стикаються з необхідністю проведення аналізу кліматичних сценаріїв для ідентифікації потенційних впливів сценаріїв потепління на 1.5/2°C та 4°C на їхню діяльність [5, 8]. Невизначеність кліматичної політики, як показано у дослідженні Persakis (2024), значно впливає на ESG-ефективність, інтенсивність викидів вуглецю та загальну ефективність компаній Fortune 1000, створюючи додаткові виклики для корпоративного планування та інвестиційних стратегій [1].

Екосистемні ризики включають деградацію біорізноманіття, порушення екосистемних послуг, забруднення повітря, води та ґрунтів, виснаження природних ресурсів. Втрата біорізноманіття загрожує стабільності харчових систем, доступу до чистої води, регулюванню клімату та іншим критично важливим екосистемним функціям. Забруднення навколишнього середовища створює прямі ризики для здоров'я людини та економічної продуктивності, особливо в промислово розвинених регіонах [5, 6, 8].

Ресурсні ризики пов'язані з вичерпанням критично важливих природних ресурсів, включаючи прісну воду, родючі ґрунти, мінеральні ресурси, енергоносії. Зростання глобального населення та економічного розвитку

збільшує тиск на природні ресурси, створюючи потенціал для конфліктів за доступ до ресурсів та економічної нестабільності. Водний стрес стає особливо актуальним викликом для багатьох регіонів світу, впливаючи на сільське господарство, промисловість та урбанізовані території [6, 8].

Демографічні трансформації створюють комплекс соціальних ризиків, що загрожують довгостроковій стійкості соціально-економічних систем організацій і суспільства. Старіння населення у розвинених країнах призводить до зростання навантаження на системи соціального забезпечення, охорони здоров'я та пенсійного забезпечення, одночасно скорочуючи трудові ресурси та економічну продуктивність. Демографічний перехід характеризується зниженням народжуваності та збільшенням тривалості життя, що кардинально змінює вікову структуру населення та створює системні виклики для довгострокової стійкості суспільства.

В українському контексті соціальні ризики набувають особливої актуальності в умовах воєнного стану та необхідності післявоєнного відновлення. Демографічна криза, посилена військовими діями та міграційними процесами, створює додаткові виклики для реалізації Цілей сталого розвитку України до 2030 року. Урбанізація та міграційні процеси створюють додаткові соціальні ризики. Неконтрольоване зростання міст призводить до утворення нетрів, погіршення якості життя, збільшення соціальної нерівності та екологічного навантаження. Міграційні потоки, особливо кліматична міграція та вимушені переміщення внаслідок воєнних дій, створюють тиск на приймаючі регіони та можуть призводити до соціальних напружень і конфліктів [10, 11].

Освітні та навичкові розриви становлять значний соціальний ризик в умовах технологічної трансформації. Невідповідність навичок робочої сили потребам цифровізованої економіки призводить до структурного безробіття та поглиблення соціальної нерівності. Доступ до якісної освіти та можливостей професійного розвитку стає критично важливим фактором соціальної мобільності та економічного зростання організацій і суспільства загалом.

Охорона здоров'я представляє комплекс соціальних ризиків, включаючи пандемічні загрози, зростання хронічних захворювань, нерівність у доступі до медичних послуг. Репродуктивне здоров'я населення безпосередньо пов'язано з демографічними тенденціями та довгостроковою соціальною стабільністю. Психічне здоров'я населення стає дедалі важливішим соціальним ризиком в умовах технологічного стресу, соціальних трансформацій та воєнних травм.

Соціальна нерівність та ексклюзія створюють ризики для соціальної згуртованості та політичної стабільності. Нерівність доходів, гендерна нерівність, етнічна дискримінація, віковий розрив у доступі до можливостей підривають соціальний капітал та довіру до інституцій. Молодіжне безробіття та обмежені можливості для молодого покоління створюють довгострокові ризики для економічного зростання та соціальної стабільності суспільства [4, 11].

ESG-ризика в корпоративному управлінні представляють інтегровані виклики, що виникають із взаємодії екологічних, соціальних факторів та факторів корпоративного управління з бізнес-операціями організацій в контексті концепції ESG та Цілей сталого розвитку ООН. Екологічні ризики включають вплив кліматичних змін на операційну діяльність, витрати на дотримання екологічних регуляцій, ризики репутації через екологічні інциденти, стрендові ризики переходу до сталих технологій та циркулярної економіки [1, 4, 6, 12].

В Україні впровадження ESG-принципів набуває особливого значення в контексті євроінтеграції та адаптації європейських стандартів корпоративного управління. Національна комісія з цінних паперів та фондового ринку (НКЦПФР) розробила додаток з питань корпоративного управління і сталого розвитку (ESG) до Кодексу корпоративного управління, що демонструє системний підхід до інтеграції принципів сталого розвитку в українську корпоративну практику. Соціальні ризики охоплюють управління людськими ресурсами, безпеку праці, стосунки зі спільнотами, ланцюги постачання та права людини. Дослідження Susen та Etter (2024) демонструють позитивну кореляцію між вищими рівнями ESG-ефективності та задоволеністю співробітників у компаніях S&P 500, що підтверджує важливість соціальних факторів для корпоративної ефективності організацій і суспільства [4, 12].

Ризики корпоративного управління включають структури управління, незалежність ради директорів, системи внутрішнього контролю, прозорість звітності, етику бізнесу та боротьбу з корупцією. Слабке корпоративне управління може призводити до значних фінансових втрат, правових проблем та репутаційних ризиків, що загрожує довгостроковій стійкості організацій.

Регуляторні ESG-ризика зростають у зв'язку з посиленням вимог до нефінансової звітності та розкриття ESG-інформації [1, 4, 6, 12]. Європейське управління з цінних паперів та ринків (ESMA) у 2024 році оновило керівні принципи для фондів з ESG- або пов'язаними із стійкістю термінами у назвах, створюючи додаткові вимоги до менеджерів фондів. Невідповідність регуляторним вимогам може призводити до штрафів, обмежень діяльності та втрати ліцензій.

Фінансові ESG-ризика проявляються через вплив на доступ до капіталу, вартість фінансування, інвестиційну привабливість та ринкову вартість [1, 4, 5]. Інвестори дедалі більше враховують ESG-фактори при прийнятті інвестиційних рішень, що створює конкурентні переваги для компаній з сильними ESG-показниками та додаткові ризики для компаній з поганою ESG-ефективністю в контексті довгострокової стійкості [1, 4].

Репутаційні ESG-ризика пов'язані із сприйняттям стейкхолдерів, медіа-висвітленням, активізмом споживачів та інвесторів. В епоху соціальних мереж та підвищеної прозорості ESG-інциденти можуть швидко набувати глобального резонансу та призводити до значних репутаційних втрат, бойкотів продукції та втрати довіри стейкхолдерів, що загрожує довгостроковій стійкості організацій і суспільства [4, 12].

Інтегроване управління ризиками сталого розвитку вимагає системного підходу, що враховує взаємозв'язки між екологічними, соціальними та економічними ризиками в контексті довгострокової стійкості організацій і суспільства в рамках концепції ESG та Цілей сталого розвитку ООН [2, 3, 4, 7, 9, 13]. Традиційні підходи до управління ризиками часто розглядають окремі категорії ризиків ізольовано, що не відображає реальної складності та взаємопов'язаності викликів сталого розвитку [2, 4, 7].

В українському контексті інтегроване управління ризиками набуває особливого значення з огляду на адаптацію національної системи Цілей сталого розвитку, розроблену протягом 2016-2017 років з урахуванням специфіки національного розвитку [10, 11]. Кожна глобальна ціль була переглянута, беручи до уваги особливості українського контексту, що створило підґрунтя для формування компетенцій щодо ідентифікації, оцінки та управління ризиками сталого розвитку.

Системний підхід до ризик-менеджменту включає ідентифікацію каскадних ефектів та зворотних зв'язків між різними типами ризиків [2, 4, 7]. Кліматичні ризики можуть посилювати соціальні напруження, що, у свою чергу, впливає на корпоративне управління та фінансову стабільність організацій і суспільства [4, 7]. Демографічні зміни взаємодіють з екологічними викликами, створюючи комплексні виклики для урбанізації, ресурсної безпеки та соціальних систем [4, 11].

Ризик-фреймворки для сталого розвитку повинні інтегрувати довгострокове планування з короткостроковим ризик-менеджментом в контексті концепції ESG та Цілей сталого розвитку ООН [2, 3, 4, 7, 13]. Включають розробку сценаріїв розвитку, стрес-тестування бізнес-моделей, інтеграцію ESG-факторів у корпоративну стратегію та операційну діяльність. Багатокритеріальне оцінювання ризиків дозволяє врахувати не лише фінансові, але й екологічні та соціальні наслідки ризиків для довгострокової стійкості організацій і суспільства [2, 4, 13].

Стейкхолдер-орієнтований підхід до управління ризиками включає активну взаємодію з усіма зацікавленими сторонами - інвесторами, працівниками, спільнотами, регуляторами, постачальниками та споживачами. Прозорість та підзвітність стають критично важливими елементами ефективного ризик-менеджменту, особливо в контексті зростаючих вимог до нефінансової звітності та формування компетенцій щодо управління ризиками [4, 12].

Адаптивне управління ризиками передбачає створення гнучких систем, здатних реагувати на мінливі умови та нові виклики, що можуть загрожувати довгостроковій стійкості організацій і суспільства. Включає розвиток організаційної стійкості, диверсифікацію ризиків, створення резервних можливостей та планування безперервності бізнесу. Цифровізація та аналіз великих даних створюють нові можливості для моніторингу ризиків та прогнозування майбутніх викликів [2, 3, 4, 13].

Колаборативні підходи до управління ризиками включають партнерства між приватним та публічним секторами, міжнародне співробітництво, обмін найкращими практиками та спільне фінансування ризик-мітигаційних заходів. Глобальний характер багатьох ризиків сталого розвитку вимагає координованих дій на місцевому, національному та міжнародному рівнях у контексті концепції ESG та Цілей сталого розвитку ООН [7, 9, 11].

Інноваційні фінансові інструменти, такі як зелені облігації, облігації стійкості, страхування кліматичних ризиків, катастрофічні облігації, створюють нові можливості для фінансування заходів з управління ризиками та адаптації до кліматичних змін. Розвиток ESG-інвестування та сталого фінансування забезпечує капітал для проєктів, спрямованих на зменшення ризиків сталого розвитку та забезпечення довгострокової стійкості організацій і суспільства [1, 2, 3, 4].

Отже ризики сталого розвитку є багатогранними викликами, що вимагають інтегрованого підходу до управління для забезпечення довгострокової стійкості організацій і суспільства. Поєднання екологічних, соціальних і управлінських факторів у стратегічному плануванні, узгодження з Цілями сталого розвитку ООН та використання інноваційних інструментів дозволяють трансформувати ризики в можливості. В українському контексті, враховуючи воєнні та демографічні виклики, формування компетенцій з управління ризиками є критично важливим для євроінтеграції та післявоєнного відновлення.

ПИТАННЯ ДО ПРАКТИЧНОГО ЗАНЯТТЯ

1. Аналіз кліматичних ризиків для промислового підприємства в Україні.
2. Оцінка соціальних ризиків у контексті демографічної кризи в Україні.
3. Розробка ESG-стратегії для українського малого чи середнього бізнесу.
4. Моделювання впливу водного стресу на аграрний сектор України.
5. Впровадження інтегрованого управління ризиками в українській організації.
6. Аналіз впливу репутаційних ESG-ризиків на діяльність української компанії в умовах євроінтеграції.
7. Оцінка потенційних ризиків втрати біорізноманіття для аграрного сектору України.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ:

1. Охарактеризувати фізичні та перехідні кліматичні ризики та їх вплив на економіку України.
2. Розрахувати економічні втрати від посухи для аграрного підприємства (500 га, втрата 15% врожаю, витрати на відновлення – 3% доходу).

3. Проаналізувати вплив воєнної міграції на соціальну згуртованість в Україні.
4. Описати принципи стейкхолдер-орієнтованого підходу до управління ESG-ризиками.
5. Розробити план мітігації репутаційних ризиків для української компанії.
6. Оцінити вплив європейських ESG-регуляцій на український енергетичний сектор.
7. Скласти матрицю суттєвості для ідентифікації пріоритетних ризиків організації.

Питання для самоконтролю:

1. Які основні категорії екологічних ризиків і як вони впливають на економіку?
2. Як демографічні зміни впливають на соціальні ризики в Україні?
3. Які компоненти ESG-ризиків є ключовими для корпоративного управління?
4. У чому полягає системний підхід до управління ризиками сталого розвитку?
5. Які інструменти застосовуються для фінансування мітігації ризиків?
6. Як інноваційні фінансові інструменти, такі як зелені облігації, сприяють зменшенню кліматичних ризиків?
7. Які виклики виникають при інтеграції ESG-факторів у стратегічне планування українських компаній?

ТЕМИ ПРЕЗЕНТАЦІЙ ТА ПОВІДОМЛЕНЬ:

1. Кліматичні ризики та їх вплив на економіку України.
2. Соціальні виклики України в умовах демографічної кризи та війни.
3. Впровадження ESG-принципів в українському корпоративному секторі.
4. Інтегроване управління ризиками: український досвід і перспективи.
5. Вплив регуляторних ESG-вимог на інвестиційну привабливість українських компаній.
6. Міграційні процеси як фактор соціальних ризиків в Україні: виклики та можливості.
7. Використання аналізу великих даних для прогнозування ризиків сталого розвитку.

Література:

1. Persakis A. The impact of climate policy uncertainty on ESG performance, carbon emission intensity and firm performance: evidence from Fortune 1000 firms. *Environment, Development and Sustainability*. 2024. Vol. 26, №9. P. 24031–24081. URL: https://ideas.repec.org/a/spr/endesu/v26y2024i9d10.1007_s10668-023-03634-

[x.html](#)

2. Kibik, O., Slobodianiuk, O., Kotlubai, V., Belous, K., Kornilova, O., & Prymachenko, I. (2025). Managing sustainable development projects through a risk-oriented framework. *International Journal of Organizational Leadership*, 14 (First Special Issue), 95-106. URL: <https://doi.org/10.33844/ijol.2025.60462>
3. Kibik, O., Slobodianiuk, O., Belous, K., Redina, Y., Kornilova, O. and Prymachenko, I. (2024). Strategy for Developing Competitive Advantages of Market Entities in the Era of Digitalization. *Econ. Aff.*, 69 (Special Issue) : 139-147. URL: <https://ndpublisher.in/admin/issues/EAv69n1p.pdf>
4. Navigating the Challenges of Environmental, Social, and Governance (ESG) Reporting: The Path to Broader Sustainable Development. *Sustainability*. 2024. Vol. 16, №2, 606. URL: <https://www.mdpi.com/2071-1050/16/2/606>
8. From risk to resilience: Climate change risk, ESG investments engagement and Firm's value. 2024. PMC. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10920155/>
9. Climate change, ESG criteria and recent regulation: challenges and opportunities. 2024. ResearchGate. URL: https://www.researchgate.net/publication/378985703_Climate_change_ESG_criteria_and_recent_regulation_challenges_and_opportunities
10. UN. Transforming our world: the 2030 Agenda for Sustainable Development. — United Nations. 2015. URL: <https://sdgs.un.org/2030agenda>
8. UNEP FI. Climate Risk Landscape Report 2024. *United Nations Environment Programme Finance Initiative*. 2024. URL: <https://www.unepfi.org/wordpress/wp-content/uploads/2024/04/Climate-Risk-Landscape-2024.pdf>
9. UN. SDG Indicators Global Database. *United Nations*. URL: <https://unstats.un.org/sdgs/indicators/database/>
10. Указ Президента України "Про Цілі сталого розвитку України на період до 2030 року" від 30 вересня 2019 року № 722/2019. URL: <https://zakon.rada.gov.ua/go/722/2019>
11. Міністерство освіти і науки України. Цілі сталого розвитку. URL: <https://mon.gov.ua/nauka/innovatsiyna-diyalnist-ta-transfer-tehnologiy/analitichni-materiali-2/tsili-stalogo-rozvitku>
12. Національна комісія з цінних паперів та фондового ринку (НКЦПФР). Розвиток сталого фінансування: додаток про ESG до Кодексу корпоративного управління. 2024. URL: <https://www.nssmc.gov.ua/1175312-2/>
13. Кібік О., Котлубай В., Белоус К., Корнілова О., Калмикова Н., Кузнецова Л. Розробка та реалізація стратегічних рішень в умовах змін: навчальний посібник. Одеса: Електронне видання. 2024. 216 с.

ТЕМА 7. РИЗИКИ В УМОВАХ ГЛОБАЛІЗАЦІЇ ТА МІЖНАРОДНОЇ ДІЯЛЬНОСТІ

Лекційні питання:

Мета вивчення/ роботи: ознайомлення з концептуальними засадами ризиків глобалізованого економічного середовища, вивчення взаємозв'язків між геополітичними, валютними, операційними та регуляторними ризиками міжнародної діяльності, а також формування компетенцій щодо ідентифікації, оцінки та управління ризиками, що можуть загрожувати довгостроковій стійкості організацій у контексті міжнародних економічних відносин та глобальних ланцюгів створення вартості.

1. Геополітичні ризики та міжнародні економічні відносини.
2. Валютні ризики та ризики міжнародних фінансових ринків.
3. Ризики міжнародних ланцюгів постачання.
4. Регуляторні ризики міжнародної діяльності.

Зміст лекції

Процеси глобалізації, що інтенсивно розвиваються впродовж останніх десятиліть, кардинально трансформували архітектуру світового економічного простору, створивши безпрецедентні можливості для міжнародної співпраці, торгівлі та інвестування [1, 10]. Водночас глобальна взаємопов'язаність економічних систем породила нові категорії ризиків, що характеризуються підвищеною складністю, системністю та трансграничним характером поширення. Сучасні організації, що функціонують у міжнародному середовищі, стикаються з багатовимірними викликами, які вимагають комплексного розуміння природи глобальних ризиків та розробки адаптивних стратегій управління ними.

Теоретичні засади дослідження ризиків у глобалізованому середовищі базуються на інтеграції класичної теорії ризику з концепціями міжнародної економіки, геополітики та системної динаміки [2, 11]. Особливість ризиків глобального характеру полягає в їх здатності до каскадного поширення через міжнародні фінансові ринки, торговельні мережі та інформаційні системи, що може призводити до синергетичних ефектів та непропорційних наслідків для окремих суб'єктів господарювання.

Геополітичні ризики представляють собою ймовірність настання несприятливих подій, пов'язаних із політичними рішеннями, конфліктами або зміною геостратегічного балансу сил, що можуть істотно вплинути на міжнародні економічні відносини та діяльність транснаціональних корпорацій. Сучасна геополітична архітектура характеризується фрагментацією міжнародного порядку, посиленням регіональних протистоянь та ерозією багатосторонніх інститутів, що створює структурні передумови для виникнення системних ризиків [10].

Природа геополітичних ризиків визначається складною взаємодією факторів внутрішньої та зовнішньої політики держав, економічними

інтересами провідних глобальних гравців, технологічним суперництвом та боротьбою за контроль над стратегічними ресурсами [3, 7, 11]. Особливого значення набувають ризики, пов'язані з торговельними війнами, економічними санкціями, територіальними суперечками та міжнародними конфліктами, які можуть призводити до порушення усталених торговельних потоків та переформатування глобальних ланцюгів створення вартості.

Вплив геополітичних ризиків на міжнародну економічну діяльність проявляється через декілька ключових механізмів. По-перше, політична нестабільність та конфлікти можуть призводити до раптового закриття ринків, заборони на експорт або імпорту певних товарів, що створює операційні труднощі для компаній, залежних від міжнародної торгівлі. По-друге, геополітичні напруження часто супроводжуються волатильністю на фінансових ринках, що ускладнює планування інвестицій та підвищує вартість фінансування. По-третє, довгострокові геополітичні тренди можуть призводити до фундаментального переформатування глобальної економіки, включаючи процеси деглобалізації, регіоналізації та технологічного роз'єднання [3, 10].

Аналіз сучасних геополітичних ризиків свідчить про формування нового типу міжнародного середовища, що характеризується підвищеною невизначеністю та фрагментацією. Традиційні механізми міжнародного економічного співробітництва піддаються ерозії під впливом зростаючого стратегічного суперництва між великими державами, що вимагає від організацій розробки більш гнучких та адаптивних стратегій управління геополітичними ризиками [7, 11].

Валютні ризики становлять одну з найбільш поширених та значущих категорій фінансових ризиків, з якими стикаються організації, що здійснюють міжнародну діяльність [4]. Сутність валютного ризику полягає в ймовірності виникнення збитків внаслідок несприятливих змін обмінних курсів валют, що може вплинути на вартість активів, зобов'язань, доходів та витрат компанії. Складність управління валютними ризиками в сучасних умовах обумовлена високою волатильністю валютних ринків, взаємозалежністю національних економік та впливом макроекономічних факторів глобального характеру [11].

Теоретичні основи аналізу валютних ризиків базуються на концепціях міжнародних фінансів, які розглядають обмінні курси як результат складної взаємодії економічних, політичних та психологічних факторів [5]. Класифікація валютних ризиків традиційно включає трансакційний ризик, що пов'язаний із конкретними угодами в іноземній валюті, трансляційний ризик, що виникає при консолідації фінансової звітності іноземних підрозділів, та економічний ризик, що відображає вплив валютних коливань на довгострокову конкурентоспроможність та ринкову вартість компанії.

Ризики міжнародних фінансових ринків охоплюють ширший спектр факторів, що можуть вплинути на фінансові результати міжнародної діяльності. До основних категорій таких ризиків належать ризики ліквідності, кредитні ризики, ризики зміни процентних ставок та ризики фінансової

нестабільності. Особливістю сучасних міжнародних фінансових ринків є їх висока інтегрованість та швидкість передачі шоків між різними сегментами та регіонами, що може призводити до каскадних ефектів та системних криз [4, 11].

Управління валютними ризиками та ризиками міжнародних фінансових ринків вимагає комплексного підходу, що поєднує стратегічне планування, операційні заходи та використання фінансових інструментів хеджування [4, 5]. Стратегічні методи управління включають диверсифікацію географічних ринків, природне хеджування через збалансованість валютних потоків та вибір оптимальної структури фінансування. Операційні заходи передбачають використання деривативів, форвардних контрактів та інших фінансових інструментів для зниження експозиції до валютних ризиків.

Сучасні тенденції розвитку міжнародних фінансових ринків, включаючи цифровізацію, появу криптовалют та зміни в монетарній політиці провідних центральних банків, створюють нові виклики для управління фінансовими ризиками. Організації повинні адаптувати свої системи ризик-менеджменту до мінливого середовища та розробляти інноваційні підходи до оцінки та управління фінансовими ризиками міжнародної діяльності [4, 11].

Міжнародні ланцюги постачання представляють собою складні мережі взаємопов'язаних організацій, процесів та інфраструктурних елементів, що забезпечують переміщення товарів, послуг та інформації від початкових постачальників до кінцевих споживачів через національні кордони [6, 8, 12]. Глобалізація виробничих процесів та прагнення до оптимізації витрат призвели до створення розгалужених та географічно розосереджених ланцюгів постачання, що, незважаючи на економічні переваги, породили нові категорії операційних та стратегічних ризиків.

Ризики міжнародних ланцюгів постачання характеризуються багатовимірністю та взаємозалежністю, що робить їх особливо складними для ідентифікації та управління. До основних категорій таких ризиків належать ризики постачальників, що включають їх фінансову нестабільність, операційні збої та порушення якості продукції, логістичні ризики, пов'язані з транспортуванням, митним оформленням та складуванням товарів, а також ризики попиту, що відображають волатильність ринкових умов та зміни споживчих переваг [8, 12].

Особливе місце в структурі ризиків міжнародних ланцюгів постачання займають природні та техногенні катастрофи, пандемії, геополітичні конфлікти та кібератаки, які можуть призводити до серйозних порушень функціонування глобальних мереж постачання. Пандемія COVID-19 продемонструвала вразливість сучасних ланцюгів постачання до системних шоків та необхідність розробки більш стійких та адаптивних моделей організації міжнародної виробничої співпраці [6, 12].

Управління ризиками міжнародних ланцюгів постачання вимагає системного підходу, що поєднує стратегічне планування, операційні заходи та технологічні рішення. Стратегічні ініціативи включають диверсифікацію

постачальників та географічних регіонів, розробку альтернативних маршрутів постачання та створення стратегічних запасів критично важливих матеріалів. Операційні заходи передбачають впровадження систем моніторингу та раннього попередження, розробку планів реагування на надзвичайні ситуації та укладання страхових угод для покриття потенційних збитків [8].

Технологічні рішення, включаючи використання штучного інтелекту, великих даних та блокчейн технологій, відкривають нові можливості для підвищення прозорості, відстежуваності та стійкості міжнародних ланцюгів постачання. Цифрові платформи дозволяють організаціям отримувати режим реального часу інформацію про стан ланцюгів постачання, прогнозувати потенційні ризики та швидко адаптуватися до змін у зовнішньому середовищі [6, 12].

Регуляторні ризики міжнародної діяльності виникають внаслідок різноманітності та мінливості правових та регуляторних режимів різних країн, а також потенційних конфліктів між національними юрисдикціями [9, 12]. Сучасне міжнародне бізнес-середовище характеризується складною мозаїкою правових систем, регуляторних вимог та стандартів, що створює значні виклики для організацій, що прагнуть розширити свою діяльність за межі національних кордонів.

Природа регуляторних ризиків обумовлена фундаментальними розбіжностями в правових традиціях, економічних моделях та політичних системах різних держав. Такі розбіжності проявляються в різних підходах до регулювання корпоративної діяльності, захисту прав інтелектуальної власності, екологічних стандартів, трудового законодавства та фінансового регулювання. Додаткову складність створюють процеси гармонізації та уніфікації правових норм на регіональному та глобальному рівнях, які можуть призводити до тимчасових невідповідностей та правової невизначеності [9, 12].

Основні категорії регуляторних ризиків включають ризики зміни законодавства, що можуть вплинути на умови ведення бізнесу, ризики недотримання вимог регуляторів, що можуть призвести до штрафів та інших санкцій, та ризики правової невизначеності, що ускладнюють стратегічне планування та прийняття інвестиційних рішень. Особливої уваги заслуговують ризики, пов'язані з екстратериторіальним застосуванням національного законодавства, коли країни поширюють дію своїх правових норм на діяльність іноземних організацій [9].

Сучасні тенденції розвитку міжнародного регуляторного середовища характеризуються посиленням вимог до корпоративної відповідальності, захисту даних, кліматичної політики та соціальних стандартів. Організації повинні адаптуватися до зростаючих очікувань стейкхолдерів щодо дотримання принципів сталого розвитку, етичної поведінки та прозорості діяльності, що вимагає розробки комплексних програм комплаєнсу та корпоративної соціальної відповідальності [9, 12].

Управління регуляторними ризиками вимагає проактивного підходу, що включає систематичний моніторинг змін у правовому середовищі, оцінку впливу нових регуляторних ініціатив на діяльність організації та розробку стратегій адаптації до мінливих вимог. Ефективні системи управління регуляторними ризиками передбачають створення спеціалізованих підрозділів комплаєнсу, встановлення партнерських відносин з місцевими юридичними радниками та регуляторними консультантами, а також впровадження технологічних рішень для автоматизації процесів моніторингу та звітності [9, 12].

Аналіз ризиків у контексті глобалізації та міжнародної діяльності свідчить про формування принципово нової парадигми управління ризиками, що відповідає реаліям взаємопов'язаного та швидко мінливого світового економічного простору [1, 2, 9, 10]. Сучасні організації стикаються з безпрецедентним за складністю та масштабом комплексом ризиків, що вимагає розробки інтегрованих та адаптивних підходів до їх ідентифікації, оцінки та управління.

Геополітичні ризики набувають особливого значення в умовах фрагментації міжнародного порядку та посилення стратегічного суперництва між провідними державами [3, 7, 10, 11]. Організації повинні розвивати здатність до швидкої адаптації до змін у геополітичному ландшафті та диверсифікації своїх операцій для зниження концентрації ризиків у окремих регіонах.

Валютні ризики та ризики міжнародних фінансових ринків вимагають комплексного підходу, що поєднує стратегічне планування, використання фінансових інструментів хеджування та постійний моніторинг ринкових умов [4, 5, 11]. Цифровізація фінансових ринків створює нові можливості для управління ризиками, але водночас породжує нові виклики, пов'язані з кібербезпекою та технологічними збоями.

Ризики міжнародних ланцюгів постачання потребують переосмислення традиційних підходів до організації глобальних виробничих мереж з урахуванням необхідності забезпечення стійкості та адаптивності до системних шоків [6, 8, 12]. Технологічні інновації відкривають нові можливості для підвищення прозорості та керованості ланцюгів постачання.

Регуляторні ризики міжнародної діяльності вимагають проактивного підходу до моніторингу змін у правовому середовищі та розробки комплексних систем комплаєнсу [9, 12]. Зростаючі вимоги до корпоративної відповідальності та сталого розвитку трансформують регуляторний ландшафт та створюють нові виклики для міжнародного бізнесу.

Успішне управління ризиками в умовах глобалізації потребує інтеграції всіх розглянутих категорій ризиків у єдину систему корпоративного ризик-менеджменту, що базується на принципах системності, адаптивності та безперервного вдосконалення. Організації, що здатні ефективно управляти комплексом глобальних ризиків, отримують конкурентні переваги та можуть

використовувати виклики глобалізації як можливості для розвитку та зростання [1, 2, 9, 10].

ПИТАННЯ ДО ПРАКТИЧНОГО ЗАНЯТТЯ

1. Аналіз впливу геополітичних ризиків на експорт аграрної продукції України.
2. Оцінка валютних ризиків для української компанії, що здійснює експорт до ЄС.
3. Розробка стратегії диверсифікації ланцюгів постачання для українського промислового підприємства.
4. Аналіз регуляторних ризиків для української компанії при виході на європейський ринок.
5. Моделювання впливу санкційних режимів на міжнародну діяльність української енергетичної компанії.
6. Оцінка логістичних ризиків для українського експортера в умовах блокади західних кордонів.
7. Розробка плану управління кіберризиками в ланцюгах постачання для міжнародної компанії.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ:

1. Проаналізувати вплив російсько-української війни на глобальні ланцюги постачання зерна.
2. Розрахувати потенційні втрати від валютних ризиків для української компанії з експортним контрактом у розмірі 1 млн доларів США за умов девальвації гривні на 10%.
3. Оцінити вплив санкційних режимів на інвестиційну привабливість України.
4. Розробити план мітігації регуляторних ризиків для українського експортера, що планує вихід на ринок США.
5. Проаналізувати вплив кліматичних міграційних потоків на геополітичні ризики в Україні.
6. Оцінити вплив зростання транспортних тарифів на ефективність ланцюгів постачання української металургійної компанії.
7. Скласти матрицю ризиків для міжнародної компанії, що працює в Україні, з урахуванням геополітичних, валютних і регуляторних факторів.

Питання для самоконтролю:

1. Які основні типи геополітичних ризиків впливають на міжнародні економічні відносини?
2. Як валютні ризики впливають на конкурентоспроможність компаній на міжнародних ринках?
3. Які фактори сприяють вразливості глобальних ланцюгів постачання?
4. У чому полягає суть регуляторних ризиків міжнародної діяльності?
5. Як санкційні режими впливають на міжнародний бізнес?

20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%96%20%D0%9C%D0%95%D0%92.pdf

5. . Міжнародні економічні відносини : підручник / за ред. В. П. Новицького. Київ: КНЕУ, 2003. 583 с. URL: <https://eir.kntu.net.ua/jspui/bitstream/123456789/347/1/%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D1%96%20%D0%B5%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D1%87%D0%BD%D1%96%20%D0%B2%D1%96%D0%B4%D0%BD%D0%BE%D1%81%D0%B8%D0%BD%D0%B8.pdf>

6. Бойко О. П. Глобалістика : навч. посіб. Суми: СумДУ, 2018. 280 с. URL: https://essuir.sumdu.edu.ua/bitstream/123456789/71504/1/Boiko_Hlobalistyka.pdf

7. Bremmer I., Keat P. The Fat Tail: The Power of Political Knowledge for Strategic Investing / Ian Bremmer, Preston Keat. New York: Oxford University Press, 2009. 272 p.

8. Gereffi G. Global Value Chains and Development Cambridge: Cambridge University Press, 2018. 403 p.

9. Renn O. Risk Governance: Coping with Uncertainty in a Complex World London: Earthscan, 2008. 455 p.

10. Юрчишин В., Якименко Ю. та ін. Сучасні трансформації світового економічного порядку. Виклики і можливості для України: аналітична доповідь / Центр Разумкова. Київ : Центр Разумкова, 2025. 112 с. URL: <https://razumkov.org.ua/images/2025/04/24/2025-Yurchyshyn-FIN.pdf>

11. Федоров Е. В. Вплив сучасного глобального середовища на формування економічної безпеки України. *Економіка: реалії часу*. 2023. № 2. С. 74–85. URL: <https://economics.net.ua/files/archive/2023/No2/74.pdf>

12. Мельник М. І., Борщевський В. В., Бабець І. Г. та ін. Глобальні чинники та ризики ендегенного розвитку регіонів : наукове видання. ДУ «Інститут регіональних досліджень імені М. І. Долишнього НАН України». Львів: ПП «Арал», 2022. 150 с. URL: <https://ird.gov.ua/irdp/p20220039.pdf>

ПИТАННЯ ДЛЯ ПІДГОТОВКИ ДО ЕКЗАМЕНУ

1. Філософські основи ризикології та їх значення для науки про ризики.
2. Методологічні підходи до дослідження ризиків у сучасному науковому контексті.
3. Концептуальні підходи до визначення ризику та невизначеності.
4. Еволюція наукових поглядів на природу ризику.
5. Системний підхід до дослідження ризикових явищ.
6. Взаємозв'язок ризику та невизначеності у економічних процесах.
7. Природа ризику у контексті глобальної економіки.
8. Класифікація ризиків та їх характеристика в теоретичному аспекті.
9. Основні методологічні школи ризикології.
10. Ризик як об'єкт управлінської діяльності та стратегічного планування.
11. Сучасні концепції оцінки ризику та їх наукове обґрунтування.
12. Роль невизначеності у прийнятті управлінських рішень.
13. Вплив системності на ефективність управління ризиками.
14. Інтеграція класичної та сучасної теорії ризику у практиці управління.
15. Кількісні методи оцінки ризику та їх практичне застосування.
16. Якісні методи аналізу ризиків у бізнес-процесах.
17. Інтегровані методи оцінки ризиків у комплексному аналізі.
18. Використання сучасних цифрових технологій для оцінки ризиків.
19. Прогностичні моделі для кількісної оцінки ризику.
20. Аналіз сценаріїв як інструмент управління невизначеністю.
21. Методика експертних оцінок для управлінських рішень.
22. Ризик-матриці та їх застосування у прийнятті рішень.
23. Методи статистичного аналізу для оцінки фінансових ризиків.
24. Використання симуляцій для моделювання ризикових ситуацій.
25. Методи вимірювання ймовірності та впливу ризику.
26. Порівняння ефективності кількісних та якісних методів оцінки.
27. Використання великих даних та аналітики для управління ризиками.
28. Практичні підходи до комбінування кількісних та цифрових методів.
29. Концептуальні моделі управління ризиками у сучасному бізнесі.
30. Стратегії реагування на ризики: уникнення, зниження, передача, прийняття.
31. Інтегровані системи управління ризиками та їх роль у компаніях.
32. Динамічні моделі управління ризиками в умовах невизначеності.
33. Ризик-менеджмент у стратегічному плануванні.
34. Моделювання ризиків для оцінки сценаріїв розвитку.
35. Використання системної динаміки у прогнозуванні ризиків.
36. Розробка корпоративних політик щодо ризиків.
37. Інструменти інтегрованого контролю ризиків у організаціях.
38. Методи оцінки ефективності стратегій управління ризиками.

39. Динамічні моделі реагування на непередбачувані події.
40. Застосування цифрових платформ для моніторингу ризиків.
41. Використання аналітики великих даних у моделюванні ризиків.
42. Роль системної адаптивності у забезпеченні стійкості компаній.
43. Системні ризики в макроекономічному середовищі.
44. Фінансові ризики банківських та небанківських установ.
45. Стратегічні та операційні ризики суб'єктів господарювання.
46. Поведінкові ризики в економічних системах.
47. Механізми виникнення та поширення економічних ризиків.
48. Вплив макроекономічної політики на формування ризиків.
49. Фінансова нестабільність як джерело системних ризиків.
50. Оцінка ризику інвестицій в економічних системах.
51. Моделі прогнозування економічних криз.
52. Ризики підприємницької діяльності в умовах невизначеності.
53. Роль поведінкових факторів у виникненні економічних ризиків.
54. Взаємозв'язок стратегічних та операційних ризиків.
55. Управління ризиками в макро- та мікроекономічному середовищі.
56. Методи зниження економічних та фінансових ризиків у компаніях.
57. Класифікація та характеристика кіберризиків.
58. Інформаційна безпека та захист персональних даних.
59. Ризики цифрової трансформації бізнес-процесів.
60. Ризики штучного інтелекту та автоматизації.
61. Методи ідентифікації кіберризиків у компаніях.
62. Управління ризиками у хмарних технологіях та ІТ-системах.
63. Кіберзлочинність як загроза для організацій.
64. Оцінка впливу технологічних ризиків на бізнес.
65. Використання аналітики для управління кіберризиками.
66. Створення систем раннього попередження в ІТ-середовищі.
67. Регуляторні вимоги до кібербезпеки в міжнародному контексті.
68. Застосування блокчейн та криптографії для зниження кіберризиків.
69. Ризики цифрових платформ та інтернет-речей.
70. Розробка корпоративних політик інформаційної безпеки.
71. Екологічні ризики та зміни клімату.
72. Соціальні ризики та демографічні виклики.
73. ESG-ризики у корпоративному управлінні.
74. Інтегроване управління ризиками сталого розвитку.
75. Вплив екологічних факторів на економічну стійкість компаній.
76. Соціальна відповідальність як інструмент зниження ризиків.
77. Методи оцінки ESG-ризиків у бізнес-процесах.
78. Ризики зміни законодавства щодо сталого розвитку.
79. Фінансові наслідки кліматичних ризиків.
80. Інноваційні підходи до управління соціальними ризиками.
81. Роль компаній у забезпеченні довгострокової стійкості.
82. Взаємозв'язок економічних, соціальних та екологічних ризиків.

83. Використання цифрових технологій для моніторингу сталих ризиків.
84. Розробка стратегій адаптації до глобальних викликів сталого розвитку.
85. Геополітичні ризики та їх вплив на міжнародну економіку.
86. Політична нестабільність та конфлікти як фактори глобальних ризиків.
87. Торговельні війни та санкції як джерела ризику міжнародної діяльності.
88. Територіальні суперечки та регіональні конфлікти у глобальному бізнес-середовищі.
89. Соціальні та екологічні ризики глобалізації.
90. Валютні ризики та їх вплив на фінансові результати компаній.
91. Трансакційний, трансляційний та економічний ризики валютних коливань.
92. Кредитні, ліквідні та процентні ризики міжнародних фінансових ринків.
93. Хеджування та фінансові інструменти для управління валютними ризиками.
94. Ризики міжнародних ланцюгів постачання: логістичні та операційні.
95. Пандемії та глобальні ризики порушення ланцюгів постачання.
96. Використання AI та блокчейн для підвищення стійкості ланцюгів постачання.
97. Диверсифікація постачальників та стратегічні запаси як методи управління ризиками.
98. Різноманітність правових режимів та регуляторні ризики міжнародної діяльності.
99. Недотримання регуляторних вимог як джерело юридичних та фінансових ризиків.
100. Роль транснаціональних корпорацій і міжнародних організацій у формуванні та управлінні ризиками.

РЕКОМЕНДОВАНИЙ ПЕРЕЛІК ДЖЕРЕЛ

1. Артими-Дрогомирецька З. Б., Негрей М. В. Економічний ризик: навч.-метод. посібник. Львів: Магнолія-2006, 2013. 320 с.
2. Азаренкова Г. М. Аналіз моделювання і управління ризиком (в схемах та прикладах): навч. посіб. Львів: Новий Світ-2000, 2011. 240 с.
3. Біла І. С. Поведінкова економіка в державному регулюванні бізнесу. Економіка та суспільство. 2024. № 65. URL: <https://doi.org/10.32782/2524-0072/2024-65-51>
4. Бойко О. П. Глобалістика: навч. посіб. Суми: СумДУ, 2018. 280 с. URL: https://essuir.sumdu.edu.ua/bitstream/123456789/71504/1/Boiko_Hlobalistyka.pdf
5. Боровик М. В. Ризик-менеджмент: конспект лекцій для здобувачів другого (магістерського) рівня вищої освіти спеціальності 073 – Менеджмент. Харків: ХНУМГ ім. О. М. Бекетова, 2023. 63 с. URL: <https://files.znu.edu.ua/files/Bibliobooks/Inshi73/0054006.pdf>
6. Бугріменко Р. М., Смірнова П. В. Ризикологія: навч. посіб. Харків: Форт, 2022. 148 с.
7. Бхаттачарджи А., Ситник Н. Методологія та організація наукових досліджень: дослідження в соціально-економічних науках: навч. посібн. 2-ге вид., перероб. і доп. Київ: НТУУ «КПІ ім. Ігоря Сікорського», 2022. 173 с.
8. Вітлінський В. В., Великоіваненко Г. І. Ризикологія в економіці та підприємництві: монографія. Київ: КНЕУ, 2004. 480 с.
9. Вітлінський В. В., Верченко П. І., Наконечний С. І. Аналіз, моделювання та управління економічним ризиком: навч. посіб. Київ: КНЕУ, 2000. 292 с.
10. Гайдур Г. І., Гахов С. О., Скибун О. Ж. Оцінка стану кібербезпеки критичної інфраструктури з використанням штучного інтелекту. Сучасний захист інформації, 2025, № 2(62). URL: [file:///C:/Users/O_S/Downloads/3233-D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-9756-1-10-20250628%20\(2\).pdf](file:///C:/Users/O_S/Downloads/3233-D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-9756-1-10-20250628%20(2).pdf)
11. Герасименко О. М. Ризик-орієнтоване управління в системі економічної безпеки підприємства: дис. ... д-ра екон. наук: 21.04.02. Київ: Університет «КРОК», 2021. 667 с.
12. Глобалізація та регіоналізація як вектори розвитку міжнародних економічних відносин: колект. монографія / за ред. А. П. Голікова. Харків: ХНУ ім. В. Н. Каразіна, 2018. 342 с. URL: <https://international-relations-tourism.karazin.ua/themes/irtb/resources/42161ce839301ec3a298d6e5b69ae2d5.pdf>
13. Гриценко Л. Л., Боярко І. М., Васильєва Т. А. та ін. Пріоритети розвитку фінансової системи України в умовах євроінтеграційних процесів: монографія / за заг. ред. Л. Л. Гриценко. Суми: Сумський державний університет, 2021. 379 с. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/83909/3/Hrytsenko_finansova_systema.pdf

14. Данильян О. Г., Дзьобань О. П. Методологія наукових досліджень: підручник. 2-ге вид., переробл. і доповн. Харків: Право, 2023. 488 с.
15. Демченко Г. В. Ризик-менеджмент: навчальний посібник для здобувачів спеціальності 073 «Менеджмент» першого (бакалаврського) рівня. Харків: Харківський національний економічний університет імені Семена Кузнеця, 2021. 224 с. URL: <https://files.znu.edu.ua/files/Bibliobooks/Inshi81/0061258.pdf>
16. Долінський Л. Б. Фінансовий ризик-менеджмент: навчально-методичний посібник. Київ: Національний університет «Києво-Могилянська академія», 2022. 132 с. URL: https://fpk.in.ua/images/biblioteka/4bac_finan/Dolinskyi.-Finansovyy-ryzyk-menedzhment-2022_compressed.pdf
17. Донець Л. І. Економічні ризики та методи їх вимірювання: навч. посіб. Київ: Центр навчальної літератури, 2006. 312 с. URL: https://shron1.chtyvo.org.ua/Donets_Liubov/Ekonomichni_ryzyky_ta_metody_yikh_vymiruvannia.pdf
18. ДСТУ ISO 31000:2018. Менеджмент ризиків. Настанова (ISO 31000:2018, IDT). Київ: ДП «УкрНДНЦ», 2018. 28 с.
19. Економічні ризики: методи вимірювання та управління: навчальний посібник / Н. С. Скопенко, І. В. Федулова, Л. В. Мазник, О. М. Кириченко, Л. І. Удворгелі; за заг. ред. Н. С. Скопенко. Київ: Видавничий дім «Кондор», 2021. 348 с. URL: <https://dspace.nuft.edu.ua/handle/123456789/39065>
20. Економічний ризик: методи оцінки та управління: навч. посібник / Т. А. Васильєва, С. В. Леонов, Я. М. Кривич та ін.; під заг. ред. Т. А. Васильєвої, Я. М. Кривич. Суми: ДВНЗ «УАБС НБУ», 2015. 208 с. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/50229/5/Ekonomichniyi_ryzyk%20.pdf
21. Етичний кодекс ученого України: постанова загальних зборів НАН України №2 від 15.04.2009. URL: <https://ips.ligazakon.net/document/MUS12440>
22. Кібік О., Слободянюк О., Кузнецова Л. Ризик-менеджмент: навч.-метод. посібник. Одеса: Фенікс, 2024. 84 с. URL: <https://hdl.handle.net/11300/27828>
23. Кібік О., Котлубай В., Белоус К., Корнілова О., Калмикова Н., Кузнецова Л. Розробка та реалізація стратегічних рішень в умовах змін: навчальний посібник. Одеса: Електронне видання, 2024. 216 с.
24. Кібік О. М., Редіна Є. В., Хаймінова Ю. В., Котлубай В. О., Белоус К. В., Скрипник М. О. Менеджмент організацій. Проектний менеджмент: навч.-метод. посібн. Одеса: Фенікс, 2020. 143 с.
25. Кібік О. М., Хаймінова Ю. В., Котлубай В. О. Стратегічне управління. Антикризове управління: навч. посібн. Одеса: Фенікс, 2019. 208 с.
26. Кришталь Г., Самофалова М., Сахно Л., Федина В., Мокієнко Т., Єрмолаєва М. Кіберризики у фінансовій та банківській системі: аналіз прямих і систематичних втрат. Financial and Credit Activity Problems of Theory and

Practice, 2025, 2(61), 125–140. URL: <https://doi.org/10.55643/fcaptp.2.61.2025.4672>

27. Липов В. В. Глобальна економіка: навч. посіб. Харків: ХНЕУ ім. С. Кузнеця, 2017. 368 с. URL: <https://repository.hneu.edu.ua/bitstream/123456789/18469/1/2017-%D0%9B%D0%B8%D0%BF%D0%BE%D0%B2%20%D0%92%20%D0%92.pdf>

28. Мельник М. І., Борщевський В. В., Бабець І. Г. та ін. Глобальні чинники та ризики ендogenousного розвитку регіонів: наукове видання. Львів: ПП «Арал», 2022. 150 с. URL: <https://ird.gov.ua/irdp/p20220039.pdf>

29. Міжнародні економічні відносини: підручник / за ред. В. П. Новицького. Київ: КНЕУ, 2003. 583 с. URL: <https://eir.kntu.net.ua/jspui/bitstream/123456789/347/1/%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D1%96%20%D0%B5%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D1%87%D0%BD%D1%96%20%D0%B2%D1%96%D0%B4%D0%BD%D0%BE%D1%81%D0%B8%D0%BD%D0%B8.pdf>

30. Мороз В. М. Ризик-менеджмент: навчальний посібник. Харків: Національний технічний університет «Харківський політехнічний інститут», 2018. 240 с. URL: <https://repository.kpi.kharkov.ua/server/api/core/bitstreams/f3be8995-acd3-4ab8-928f-1c5ff30f3584/content>

31. Муравський В. В. Облік та кібербезпека: монографія. Тернопіль: ЗУНУ, 2023. 200 с. URL: <https://dspace.wunu.edu.ua/bitstream/316497/52083/1/%D0%9C%D1%83%D1%80%D0%B0%D0%B2%D1%81%D1%8C%D0%BA%D0%B8%D0%B9%20%D0%92.%D0%92.%20-%20%D0%9E%D0%B1%D0%BB%D1%96%D0%BA%20%D1%82%D0%B0%20%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0.pdf>

32. Міністерство освіти і науки України. Цілі сталого розвитку. URL: <https://mon.gov.ua/nauka/innovatsiyna-diyalnist-ta-transfer-tekhnologiy/analitichni-materiali-2/tsili-stalogo-rozvitku>

33. Національна комісія з цінних паперів та фондового ринку (НКЦПФР). Розвиток сталого фінансування: додаток про ESG до Кодексу корпоративного управління. 2024. URL: <https://www.nssmc.gov.ua/1175312-2/>

34. Панченко О., Маслюк О., Гориленко А. Банківські ризики як об'єкт страхування в сучасних умовах. Проблеми і перспективи економіки та управління. 2021. № 4(24). С. 146–154. URL: <http://ppeu.stu.cn.ua/article/view/228214>

35. Петик Л., Міщенко К. Оцінка банківських ризиків в умовах війни. Економіка та суспільство. 2024. № 65. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4476>

36. Петруня Ю. Є., Літовченко Б. В., Пасічник Т. О. та ін. Прийняття управлінських рішень: навч. посібн. / за ред. Ю. Є. Петруні. [4-те вид., переробл. і доп.]. Дніпро: Університет митної справи та фінансів, 2020. 276 с.

37. Про затвердження Методичних рекомендацій з організації управління ризиками в банках України: Постанова Правління Національного банку України від 15.03.2018 № 29. URL: <https://zakon.rada.gov.ua/laws/show/v0029500-18#Text>

38. Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах: Постанова Правління Національного банку України від 11.06.2018 № 64. URL: <https://zakon.rada.gov.ua/laws/show/v0064500-18#Text>

39. Про кібербезпеку: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

40. Про затвердження Порядку здійснення оцінки ризиків у системі запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Наказ Міністерства фінансів України від 28.08.2018 № 764. URL: <https://zakon.rada.gov.ua/laws/show/z1030-18#Text>

41. Ризики в сучасній системі міжнародних економічних відносин: монографія / О. І. Шнирков, А. С. Філіпенко, О. В. Бутко та ін. Київ: ВПЦ «Київський університет», 2020. 312 с. URL: <https://www.iir.edu.ua/sites/default/files/2023-03/%D0%A0%D0%B8%D0%B7%D0%B8%D0%BA%D0%B8%20%D0%B2%20%D1%81%D1%83%D1%87%D0%B0%D1%81%D0%BD%D1%96%D0%B9%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%96%20%D0%9C%D0%95%D0%92.pdf>

42. Савчук В. І. Ризик-менеджмент: навчальний посібник. Київ: Видавництво «Лабораторія», 2019. 320 с. URL: <https://laboratory.ua/products/ryzyk-menedzhment>

43. Слободянюк О. В., Калмикова Н. Ю. Фінансова складова економічної безпеки розвитку суб'єктів господарювання. Наукові інновації та передові технології (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»). 2023. № 13(27). С. 574–584. URL: <http://perspectives.pp.ua/index.php/nauka/issue/view/188/279>

44. Степанов В. М. Ризикологія: основи, додатки, тезаурус. Одеса: ІПРЕІ НАН України, 2019. 292 с.

45. Сучасна міжнародна економіка: навч. посіб. / В. М. Тарасевич, Л. В. Білоцерківець, Н. С. Завгородня, І. В. Золотарьова; за ред. В. М. Тарасевича. Київ: Центр учбової літератури, 2019. 520 с. URL: https://fpk.in.ua/images/biblioteka/3fmb_finan/Suchasna-mizh.-ekonomika.2019Bilotserkovets.pdf

46. Трофименко О. Г., Логінова Н. І., Соколов А. В., Чикунів П. О., Ахметьєва Г. В. Штучний інтелект у військовій сфері. Кібербезпека: освіта,

наука, техніка. 2024. № 1(25). С. 199–212. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/600>

47. Указ Президента України "Про Цілі сталого розвитку України на період до 2030 року" від 30 вересня 2019 року № 722/2019. URL: <https://zakon.rada.gov.ua/go/722/2019>

48. Федоров Е. В. Вплив сучасного глобального середовища на формування економічної безпеки України. Економіка: реалії часу. 2023. № 2. С. 74–85. URL: <https://economics.net.ua/files/archive/2023/No2/74.pdf>

49. Якименко І., Штефан Є., Лук'янихін В. Управління науковими проєктами: навч. посібн. Київ: НУХТ, 2022. 139 с.

50. Юрчишин В., Якименко Ю. та ін. Сучасні трансформації світового економічного порядку. Виклики і можливості для України: аналітична доповідь. Київ: Центр Разумкова, 2025. 112 с. URL: <https://razumkov.org.ua/images/2025/04/24/2025-Yurchyshyn-FIN.pdf>

51. A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. 2010. URL: <https://ferma.eu/wp-content/uploads/2019/02/a-structured-approach-to-erm-1.pdf>

52. Beck, U. Risk Society: Towards a New Modernity. London: Sage Publications, 1992. 260 p. (Original: Risikogesellschaft, 1986). URL: <http://www.riversimulator.org/Resources/Anthropology/RiskSociety/RiskSocietyTowardsAnewModernity1992Beck.pdf>

53. Bremmer I., Keat P. The Fat Tail: The Power of Political Knowledge for Strategic Investing. New York: Oxford University Press, 2009. 272 p.

54. Christoffersen, P. Elements of Financial Risk Management. Academic Press, 2012. URL: <https://unidel.edu.ng/focelibrary/books/Elements%20of%20Financial%20Risk%20Management.pdf>

55. Committee of Sponsoring Organizations of the Treadway Commission (COSO). Enterprise Risk Management—Integrating with Strategy and Performance. 2017. URL: https://docs.wbcsd.org/2018/10/COSO_WBCSD_ESGERM_Guidance.pdf

56. From risk to resilience: Climate change risk, ESG investments engagement and Firm's value. 2024. PMC. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10920155/>

57. Gereffi G. Global Value Chains and Development. Cambridge: Cambridge University Press, 2018. 403 p.

58. Harkava V., Kibik O., Tytok V., Klim N., Cervinskaya L., Voit S. Economic security of the country for stable development. AD ALTA: Journal of Interdisciplinary Research, 2021, 11/02-XXII, 138–142. URL: <http://www.magnanimitas.cz/11-02-xxii>

59. Holling, C. S. Resilience and Stability of Ecological Systems. Annual Review of Ecology and Systematics, 1973, Vol. 4, 1–23. DOI: 10.1146/annurev.es.04.110173.000245

60. Holton, G. A. Value-at-Risk: Theory and Practice. 2003. URL: https://first-edition.value-at-risk.net/wp-content/uploads/book_pdf/Holton-2003-Value-at-Risk.pdf
61. ISO 31000:2018. Risk management — Guidelines. International Organization for Standardization.
62. Jorion, P. Value at Risk: The New Benchmark for Managing Financial Risk. McGraw-Hill, 2006.
63. Kahneman, D., & Tversky, A. Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 1979, Vol. 47, No. 2, 263–291. DOI: 10.2307/1914185. URL: <https://www.jstor.org/journal/econometrica>
64. Kibik O., Kotlubai V., Slobodianiuk M., Kornuta L., Kornilova O., Prymachenko I. Management of Changes in the Process of Safe Development of Economic Agents. *Economic Affairs*, 2022, № 67, 04s, 803–813.
65. Kibik O., Slobodianiuk O., Belous K., Redina Y., Kornilova O., Prymachenko I. Strategy for Developing Competitive Advantages of Market Entities in the Era of Digitalization. *Economic Affairs*, 2024, № 69 (Special Issue), 139–147. URL: <https://ndpublisher.in/admin/issues/EAv69n1p.pdf>
66. Kibik, O., Slobodianiuk, O., Kotlubai, V., Belous, K., Kornilova, O., & Prymachenko, I. Managing sustainable development projects through a risk-oriented framework. *International Journal of Organizational Leadership*, 2025, 14 (First Special Issue), 95–106. URL: <https://doi.org/10.33844/ijol.2025.60462>
67. Knight, F. H. Risk, Uncertainty and Profit. Boston: Houghton Mifflin, 1921. 381 p. URL: <https://archive.org/details/riskuncertaintyp00knig>
68. Koval, V., Gonchar, V., Udovychenko, V., Kalinin, O., Slobodianiuk, O., & Soloviova, O. Risk management analysis of environmental investment in economic security. *Journal of Geology, Geography and Geoecology*, 2023, 32(3), 540–549. URL: <https://geology-dnu.dp.ua/index.php/GG/article/view/1040>
69. Korombel, A. Qualitative risk analysis as a stage of risk management in investment projects: Advantages and disadvantages of selected methods – theoretical approach. *Adalta Journal of Interdisciplinary Research*, 2014. URL: https://www.magnanimitas.cz/ADALTA/0102/papers/A_korombel.pdf
70. McNeil, A. J., Frey, R., & Embrechts, P. Quantitative Risk Management: Concepts, Techniques and Tools. Princeton University Press, 2015. URL: <http://ndl.ethernet.edu.et/bitstream/123456789/30397/1/141.Alexander%20J.McNeil.pdf>
71. Navigating the Challenges of Environmental, Social, and Governance (ESG) Reporting: The Path to Broader Sustainable Development. *Sustainability*, 2024, Vol. 16, №2, 606. URL: <https://www.mdpi.com/2071-1050/16/2/606>
72. Persakis A. The impact of climate policy uncertainty on ESG performance, carbon emission intensity and firm performance: evidence from Fortune 1000 firms. *Environment, Development and Sustainability*, 2024, Vol. 26, №9, 24031–24081. URL: https://ideas.repec.org/a/spr/endesu/v26y2024i9d10.1007_s10668-023-03634-x.html

73. Popper, K. The Logic of Scientific Discovery. London: Routledge, 2002 (Original: Logik der Forschung, 1934). 544 p.
74. Renn O. Risk Governance: Coping with Uncertainty in a Complex World. London: Earthscan, 2008. 455 p.
75. Taleb, N. N. The Black Swan: The Impact of the Highly Improbable. New York: Random House, 2007. 400 p.
76. UN. SDG Indicators Global Database. United Nations. URL: <https://unstats.un.org/sdgs/indicators/database/>
77. UN. Transforming our world: the 2030 Agenda for Sustainable Development. United Nations, 2015. URL: <https://sdgs.un.org/2030agenda>
78. UNEP FI. Climate Risk Landscape Report 2024. United Nations Environment Programme Finance Initiative, 2024. URL: <https://www.unepfi.org/wordpress/wp-content/uploads/2024/04/Climate-Risk-Landscape-2024.pdf>
79. Von Bertalanffy, L. General System Theory: Foundations, Development, Applications. New York: George Braziller, 1968. 295 p.

Ресурси відкритого доступу

1. <http://portal.rada.gov.ua> - Офіційний веб-сайт Верховної Ради України
2. <http://www.kmu.gov.ua> - Урядовий портал України
3. <http://www.ukrstat.gov.ua> - Державна служба статистики
4. <http://www.me.gov.ua> - Міністерство економіки України
5. <http://www.minfin.gov.ua> - Міністерство фінансів України
6. <http://www.minjust.gov.ua> - Міністерство юстиції України
7. <http://sfs.gov.ua> - Податкова служба України
8. <http://dspace.onua.edu.ua> - eNUOLAIR – репозитарій (архів) НУ ОЮА
9. <http://www.niss.gov.ua> - Національний інститут стратегічних досліджень
10. <http://www.nbu.gov.ua> - Національна бібліотека ім. В. І. Вернадського
11. <https://mon.gov.ua> - Міністерство освіти і науки України
12. <http://www.iso.org> - Офіційний веб-сайт Міжнародної організації зі стандартизації (ISO), що містить інформацію про стандарти управління ризиками, зокрема ISO 31000.
13. <https://www.coso.org> - Офіційний веб-сайт Комітету організацій-спонсорів Комісії Тредвея (COSO), який публікує рекомендації з управління ризиками.
14. <https://www.rims.org> - Офіційний веб-сайт Інституту управління ризиками (Risk and Insurance Management Society), що пропонує ресурси з ризик-менеджменту.

НАВЧАЛЬНЕ ВИДАННЯ

*Ольга СЛОБОДЯНЮК
Ольга КІБІК,
Вячеслав КОТЛУБАЙ*

РИЗИКОЛОГІЯ

Навчально-методичний посібник
для здобувачів третього (освітньо-наукового) рівня вищої освіти
зі спеціальності «Менеджмент»

Електронне видання

В авторській редакції

Ум-друк. арк. 4,68.
Зам. № 2509-08.

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net