МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Балтовський О.А., Моргунова Т.І., Самойлов С.В.

«СИСТЕМНИЙ АНАЛІЗ ТА ПРОГНОЗУВАННЯ РИЗИКІВ»

Навчальний посібник

Одеса 2025

Рекомендовано до друку науково-методичною радою Одеського державного університету внутрішніх справ

Авторський колектив:
Балтовський О.А. – доктор технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій ОДУВС;
Моргунова Т.І. – кандидат технічних наук, доцент, доцент кафедри кримінального аналізу та інформаційних технологій ОДУВС;
Самойлов С.В. - кандидат юридичних наук, начальник 3-го управління (інформаційних технологій та програмування) Департамента кіберполіції НПУ.

Рецензенти:
Олексій ВОЛОШКО – начальник УКА ГУНП в Одеській області, полковник поліції;
Карен ІСМАЙЛОВ – заступник начальника 5-го відділу (інформаційних технологій та програмування в південному регіоні) (м. Одеса) 3-го управління (інформаційних технологій та програмування) Департаменту кіберполіції Національної поліції України, підполковник поліції, кандидат юридичних наук, доцент.

Балтовський О.А., Моргунова Т.І., Самойлов С.В. Системний аналіз та прогнозування ризиків: навчальний посібник / За заг. ред. д.т.н., доц. О.А. Балтовського. Одеський держ. унів-т внутр. справ, 2025. **139** с.

Навчальний посібник «Системний аналіз та прогнозування ризиків» є комплексним міждисциплінарним виданням, що поєднує теоретико-методологічні засади системного підходу із сучасними прикладними технологіями аналізу, оцінювання, прогнозування та управління ризиками в складних системах. Його зміст спрямований на формування цілісного бачення ризику як категорії, що має системну природу та вимагає комплексного осмислення через призму взаємозв'язків між елементами, підсистемами та середовищем.

У фокусі видання – вивчення ризиків у технічних, соціальних, організаційних, кіберфізичних та інформаційних системах. Посібник охоплює чотири структуровані розділи, кожен з яких детально розкриває логіку етапів системного аналізу ризиків – від філософії та категоріального апарату до інструментальних засобів моделювання і прогнозування та до практик інтеграції ризик-менеджменту в управлінські системи.

Посібник може бути використаний у навчальних програмах магістерського та бакалаврського рівнів для дисциплін, пов'язаних із системним аналізом, ризик-менеджментом, кібербезпекою, екологічним аналізом, управлінням проектами, а також у системах професійної підготовки кадрів у сфері державного та корпоративного управління.

УДК 303.732.4(477)

ЗМІСТ

ВСТУП

У сучасному світі, що характеризується високим рівнем складності, динаміки та невизначеності, питання прогнозування та управління ризиками постає як ключове у різних галузях знань і практики. Ризики більше не мають локального або одномірного характеру – вони системні, взаємопов'язані, здатні до каскадного поширення та виникають унаслідок дії різнорідних факторів: технічних, соціальних, екологічних, інформаційних та організаційних. У таких умовах традиційні підходи до аналізу ризиків не здатні забезпечити належну ефективність, адже вони часто ігнорують множинність взаємозв'язків, зворотних впливів та динамічну природу складних систем.

Системний аналіз, як міждисциплінарна наукова методологія, дає змогу досліджувати ризики не ізольовано, а в контексті взаємодії елементів, підсистем та середовища. Завдяки своїм концептуальним основам, він дозволяє мислити категоріями цілісності, емерджентності, ієрархічності та адаптивності, що відкриває нові горизонти у розумінні природи ризиків. У цьому контексті ризик розглядається як властивість складної системи, що виникає в результаті невизначеності у поведінці компонентів та складності їхньої взаємодії. Отже, системний підхід дозволяє моделювати багатофакторні процеси, враховувати часові затримки, слабкі сигнали, приховані впливи та нелінійні зворотні зв'язки.

Навчальний посібник «Системний аналіз та прогнозування ризиків розроблено з метою формування системного мислення та аналітичної культури у здобувачів вищої освіти. Його зміст охоплює широкий спектр питань – від філософсько-методологічних засад системного підходу до практичного використання інструментів аналізу, оцінювання, прогнозування та управління ризиками. Посібник побудовано за логікою поступового занурення у проблематику: від базових понять і концепцій до інноваційних моделей і сучасних цифрових рішень у сфері ризик-менеджменту. Кожен розділ поєднує теоретичний матеріал із прикладними прикладами, що дозволяє забезпечити баланс між абстрактним рівнем засвоєння знань і практичною їх реалізацією.

Перший розділ висвітлює теоретико-методологічні основи системного аналізу ризиків, включаючи історію становлення, базові поняття, принципи і класифікації систем. Тут також аналізується специфіка різних типів систем – технічних, соціальних, кіберфізичних – та особливості їхньої взаємодії з ризиками. Другий розділ зосереджений на системних методах ідентифікації та оцінювання ризиків, зокрема йдеться про мультикритеріальні підходи, когнітивне моделювання, аналіз чутливості та роботу з невизначеністю. У третьому розділі розглядаються сучасні інструменти прогнозування ризиків – від статистичних моделей до штучного інтелекту, цифрових платформ та симуляційних середовищ. Четвертий розділ присвячено інтеграції ризик-менеджменту в системи управління: висвітлюються питання стратегічного планування, управління в умовах кризи, підтримки рішень у

багатокритеріальному середовищі та стійкості критичної інфраструктури.

Особливістю цього посібника є акцент на практичній значущості знань. Усі теоретичні викладки супроводжуються прикладами з реального життя, аналітичними схемами, візуалізаціями та кейсами, що спрямовані на розвиток навичок системного аналізу реальних проблем. Значну увагу приділено використанню цифрових інструментів – інтелектуальних систем підтримки рішень, когнітивних моделей, платформ візуалізації та інструментів на основі штучного інтелекту. Це дозволяє підготувати здобувачів вищої освіти до роботи в умовах новітніх викликів, де цифрова аналітика та моделювання ризиків стають ключовими елементами управлінських рішень.

У результаті опанування матеріалу цього посібника здобувачі вищої освіти зможуть не лише розуміти природу ризиків у складних системах, а й застосовувати набуті знання для прийняття ефективних рішень у професійній діяльності. Вони зможуть аналізувати складні соціотехнічні ситуації, будувати моделі сценаріїв розвитку подій, використовувати цифрові платформи для моніторингу та оцінювання, адаптувати стратегії до динаміки середовища та забезпечувати стійкість керованих систем до ризиків.

Таким чином, цей навчальний посібник є не лише джерелом знань, але й методологічною основою для підготовки майбутніх фахівців у сферах аналітики, управління, безпеки, цифрових технологій, стратегічного планування та державного адміністрування. Його зміст зорієнтований на потреби сучасного світу, в якому аналітична обґрунтованість, адаптивність і системне мислення є критично важливими навичками.

РОЗДІЛ 1. СИСТЕМНИЙ АНАЛІЗ У ДОСЛІДЖЕННІ РИЗИКІВ: ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ

1.1. Історія виникнення та розвиток системного аналізу як наукової дисципліни

Системний аналіз – це науково-методологічний інструментарій, що забезпечує всебічне вивчення складних об’єктів, процесів і явищ шляхом розгляду їх як систем. Його становлення і розвиток відображає зміну парадигм наукового пізнання та розширення аналітичних можливостей дослідника в умовах зростаючої складності світу. У цьому підрозділі розглянуто історичні витоки системного підходу, внесок класиків системного аналізу, а також сучасні тенденції його міждисциплінарного використання, зокрема у сфері аналізу та прогнозування ризиків.

Становлення системного підходу

Системний підхід виник як реакція на обмеження класичної редукціоністської науки, яка зводила складні явища до суми їх частин. У XX столітті в умовах наростання технологічної складності, глобалізації та розвитку обчислювальної техніки зросла потреба у нових підходах до вирішення задач управління, організації та прогнозування.

Таблиця 1.1

Хронологія розвитку системного підходу

Період	Основні риси	Представники	Ключові досягнення
Довоєнний етап (до 1940-х)	Інтуїтивне використання системних понять у філософії, біології	І. Кант, Г. Гегель, Ч. Дарвін	Формування ідеї цілісності, взаємозв’язку
1940-1950-ті	Формалізація загальної теорії систем	Л. фон Берталанфі	Заснування системології як науки
1960-1970-ті	Інституціоналізація системного аналізу	Дж. Форрестер, Р. Акерофф, Р. Черчман	Розробка моделей динаміки, системне моделювання
1980-1990-ті	Розвиток методів оптимізації та ієрархічного моделювання	Т. Сааті, В. Стеффі	Метод аналізу ієрархій (AHP), динаміка багаторівневих систем
2000-2020-ті	Інтеграція з ІТ, ШІ, Big Data	Міждисциплінарні команди	Прогностичні моделі, кіберфізичні системи

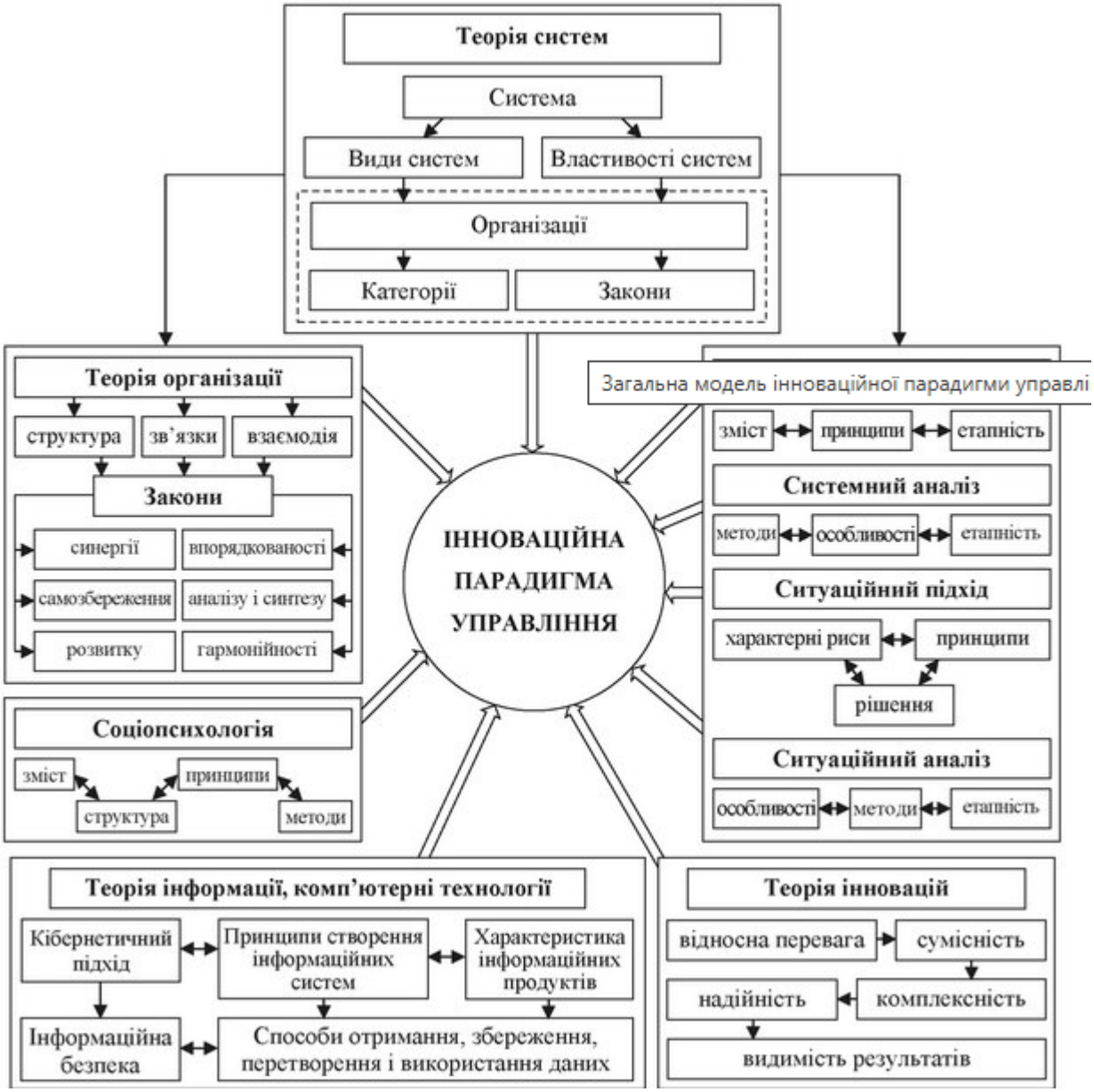

Рис.1.1. Еволюція парадигми системного підходу

Класики системного аналізу: Людвіг фон Берталанфі, Форрестер, Черчман

Людвіг фон Берталанфі (1901–1972)

Людвіг фон Берталанфі – австрійсько-канадський біолог, філософ науки та один із головних мислителів XX століття, який започаткував науковий напрям, що згодом оформився як загальна теорія систем (General Systems Theory, GST). Його роботи стали одними з найвпливовіших у формуванні сучасного розуміння системного підходу, що відіграв ключову роль у розвитку системного аналізу як міждисциплінарної наукової галузі.

У першій половині XX століття природничі науки здебільшого були зосереджені на редукціоністському підході, тобто вивченні складних явищ через розклад їх на елементарні складові. Однак цей підхід виявився

недостатнім для пояснення багатьох біологічних, соціальних і технічних процесів, які демонструють нелінійність, зворотні зв'язки та еволюційність. У цьому контексті і з'явилася потреба в новій концептуальній парадигмі, здатній охопити цілісні властивості складних об'єктів.

Берталанфі поставив під сумнів доцільність виключно редукціоністського підходу, наголошуючи на тому, що цілісність, взаємодія, структура та динаміка системи мають самостійне значення.

Основною метою фон Берталанфі було створення універсального, міждисциплінарного підходу до дослідження комплексних систем, незалежно від їхньої природи – біологічної, технічної, економічної чи соціальної. Його загальна теорія систем – це концептуальний каркас, який описує закономірності функціонування, розвитку та взаємодії складних систем.

На відміну від замкнених механістичних моделей, запропонованих у класичній фізиці, Берталанфі розробив модель відкритої системи, яка постійно обмінюється енергією, матерією та інформацією з навколишнім середовищем. Саме це дозволяє системі підтримувати гомеостаз і адаптуватися до змін.

Таблиця 1.2

Ключові ідеї Людвига фон Берталанфі, що стали підґрунтям системного аналізу

Ключова ідея	Зміст	Значення для системного аналізу
Відкриті системи	Системи, які не ізольовані від середовища та перебувають у постійній взаємодії з ним	Забезпечує динамічне розуміння складних процесів у реальному середовищі
Емерджентність	Властивості цілого не зводяться до властивостей частин	Пояснює феномени, які не можуть бути вивчені ізольовано на рівні елементів
Ієрархічна структура	Системи складаються з підсистем, які у свою чергу можуть містити підпідсистеми	Створює основу для багаторівневого аналізу та моделювання складних структур
Самоорганізація	Здатність систем до спонтанної організації без зовнішнього керівництва	Важливо для розуміння еволюції соціальних, екологічних та кіберфізичних систем
Гомеостаз та рівновага	Спроможність системи зберігати стабільність у змінних умовах	Ключова ідея для проектування стійких організаційних і технологічних систем

Загальна теорія систем Берталанфі мала винятковий вплив на формування багатьох новітніх дисциплін, зокрема:

– кібернетики та інформатики – розвиток ідей зворотного зв'язку, управління та обробки інформації;

– біоінформатики та молекулярної біології – аналіз генетичних і клітинних систем як відкритих, взаємопов'язаних структур;

– соціальних наук – концептуалізація соціальних інститутів і організацій як складних динамічних систем;

– екології – розуміння екосистем як адаптивних відкритих систем з балансом енергії та інформації.

У сучасному системному аналізі ризиків ідеї фон Берталанфі використовуються як концептуальна база для:

– моделювання складних соціотехнічних систем;

– ідентифікації критичних вузлів і точок відмови;

– вивчення взаємозалежностей між компонентами системи, які можуть призвести до каскадних ризиків.

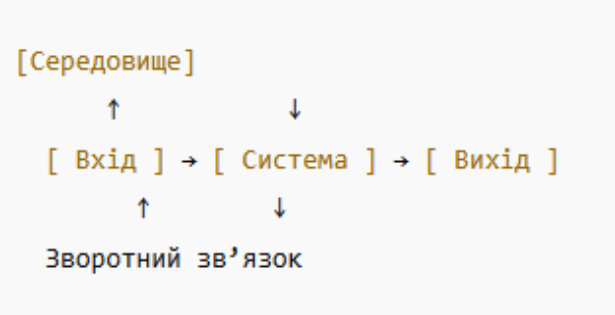

Рис. 1.2. Схема відкритої системи з входами, виходами та зворотним зв'язком у взаємодії з середовищем.

Таблиця 1.3

Оцінка впливу Людвіга фон Берталанфі на розвиток методології системного аналізу

Критерій	Вплив Людвіга фон Берталанфі
Формування поняття системи	Замість аналізу частин – фокус на цілісних властивостях систем
Розробка універсальних моделей	Моделі, що можуть застосовуватися в біології, техніці, економіці тощо
Підтримка міждисциплінарності	Сприяння об'єднанню знань із різних наукових напрямів
Підхід до ризиків	Урахування взаємозв'язків і динаміки в оцінці ризиків у складних системах

Людвіг фон Берталанфі не просто розширив наукову методологію – він запропонував новий світогляд, який дозволяє мислити системно, охоплюючи цілісність, динаміку, взаємозалежність і складність. Його внесок став наріжним каменем сучасного системного аналізу, особливо у сферах, де

ризики та невизначеність є ключовими факторами прийняття рішень.

Людвіг фон Берталанфі є засновником загальної теорії систем (General Systems Theory, GST), яка стала фундаментом для подальших напрямів системного аналізу. Його підхід полягав у тому, що системи мають властивості, яких не можна пояснити лише аналізом їх елементів.

Основні ідеї:

1) Відкрита система як об'єкт, що обмінюється енергією з навколишнім середовищем
2) Емерджентність (властивості цілого, які не притаманні частинам)
3) Ієрархічність та організація систем

Таблиця 1.4

Ключові концепції Людвіга фон Берталанфі

Концепт	Опис
Відкриті системи	Взаємодія із зовнішнім середовищем
Емерджентність	Властивості, що виникають у системі
Гомеостаз	Здатність підтримувати стабільний стан

Джей Форрестер (1918–2016)

Джей Форрестер – видатний американський інженер, вчений та мислитель, чия діяльність справила глибокий вплив на розвиток сучасного системного аналізу, зокрема в його ключовому напрямі – системній динаміці. Як професор Массачусетського технологічного інституту (MIT), він зробив вагомий внесок у теоретичне обґрунтування та практичне впровадження методів математичного моделювання складних систем. Його ідеї стали фундаментальними для аналізу та управління соціальними, економічними, технологічними й екологічними процесами в умовах невизначеності та динаміки.

Форрестер розпочав свою кар'єру як інженер-електронщик, беручи участь у розробці радарних систем під час Другої світової війни. Згодом він перейшов до проєктів, пов'язаних із створенням комп'ютерів, зокрема розробив один із перших магнітних запам'ятовуючих пристроїв – магнітне ядро пам'яті (magnetic core memory), що стало стандартом у комп'ютерній техніці на кілька десятиліть. У другій половині XX століття його інтереси сфокусувалися на більш глобальних і міждисциплінарних проблемах, які виходили за межі технічної інженерії.

Внесок у системний аналіз а саме включення поняття «петля зворотного зв'язку».

Один із ключових концептів, який Джей Форрестер ввів у науковий обіг, – петля зворотного зв'язку (feedback loop). Він розглядав будь-яку складну систему (від економіки до урбаністики) як сукупність взаємопов'язаних елементів, які перебувають у безперервній взаємодії через механізми позитивного або негативного зворотного зв'язку. Цей підхід дозволив пояснювати, як неочевидні причинно-наслідкові зв'язки можуть

породжувати нестабільність, коливання або самопідсилення певних ефектів у системах.

Форрестер створив низку математичних моделей, що дозволяли описувати динаміку складних соціально-економічних систем. Серед найвідоміших:

1) Модель міста (Urban Dynamics, 1969) – досліджувала розвиток міського середовища, зокрема механізми зростання населення, безробіття та міської інфраструктури. Форрестер показав, що традиційні політики розвитку міст часто приводять до парадоксальних і небажаних результатів через ігнорування зворотних зв'язків.

2) Модель «Світ-3» (World3) – була центральною у знаменитій доповіді «Межі зростання» (The Limits to Growth, 1972), створеній на замовлення Римського клубу. Ця модель стала глобальним комп'ютерним симулятором, який описував взаємодію п'яти основних параметрів: населення, індустріалізація, виробництво продовольства, вичерпання ресурсів і забруднення навколишнього середовища. Модель ілюструвала, як зростання в умовах обмежених ресурсів неминуче призводить до кризових явищ.

Форрестер одним із перших почав застосовувати обчислювальне моделювання як інструмент прогнозування та стратегічного планування в реальному часі. Його підходи до моделювання дозволили урядам, корпораціям та міжнародним організаціям бачити довгострокові наслідки поточних рішень, враховуючи системні взаємозв'язки й часові затримки. Системна динаміка стала корисною для сценарного аналізу, розробки політик, розуміння складних причинно-наслідкових залежностей у соціотехнічних системах.

Форрестер заснував Лабораторію системної динаміки MIT, навколо якої сформувалася глобальна спільнота дослідників і практиків, що й сьогодні застосовують системну динаміку в таких галузях, як охорона здоров'я, екологія, енергетика, освіта, військова стратегія, менеджмент і публічне управління. Його методологія надихнула створення нових підходів до навчання, зокрема інтеграцію системного мислення в шкільну освіту.

Джей Форрестер був не лише піонером у галузі комп'ютерної техніки, а й реформатором у сфері управлінської науки та системного аналізу. Його здатність бачити світ як комплексну динамічну систему, що саморегулюється через зворотні зв'язки, стала підґрунтям для нової парадигми мислення, яка сьогодні необхідна для вирішення глобальних викликів. Його ідеї залишаються актуальними в епоху кліматичних змін, криз управління ресурсами та технологічних зрушень.

Рассел Черчман (1913-2006)

Рассел Черчман – одна з ключових постатей у розвитку системного мислення у XX столітті. Його науковий доробок став підґрунтям для формування «м'якого системного підходу» (*Soft Systems Methodology*, SSM), що суттєво відрізняється від традиційних «жорстких» методів аналізу

складних систем. У своїй роботі Черчман зосереджувався не лише на формалізованих моделях та технократичних аспектах управління, а й на глибоко людиноцентричному підході, де на перший план виходять цінності, переконання, соціальні контексти та етичні дилеми.

Основні ідеї та принципи підходу Черчмана:

1. Людино-центричність системного мислення.

На відміну від класичного інженерного чи математичного системного аналізу, що часто ігнорує емоції, переконання та соціальну динаміку, підхід Черчмана надає перевагу глибокому розумінню людського контексту. Системи, з його точки зору, завжди є частиною людської діяльності, а тому не можуть бути нейтральними або суто технічними.

Люди – це не лише користувачі чи споживачі систем, а активні учасники, які формують і змінюють ці системи залежно від індивідуальних та групових поглядів, культурних особливостей, моральних орієнтирів. Тому розв'язання проблем має будуватися не лише на логіці та даних, а й на глибокому розумінні смислів і мотивацій.

2. Пріоритет цінностей та альтернативності рішень.

Черчман стверджував, що жодна проблема не має єдиного «правильного» розв'язку – існує спектр альтернатив, кожна з яких відповідає певним ціннісним орієнтирам. Системне мислення має не просто обирати оптимальний варіант, а враховувати, які цінності переважають у різних зацікавлених сторін, та як ці цінності впливають на ухвалення рішень.

Він наголошував на тому, що будь-який системний підхід неминуче вбудований у ціннісний контекст, і тому об'єктивність є обмеженою. Саме тому важливо досліджувати альтернативні перспективи, відкрито визнавати конфлікти інтересів і етичні дилеми, та шукати рішення, які максимально узгоджуються з різними соціальними позиціями.

3. М'який системний підхід (Soft Systems Methodology, SSM).

Підхід Черчмана став основою для подальшої розробки м'якої системної методології, яку найбільш активно розвивав його учень Пітер Чекленд. SSM базується на тому, що реальні проблеми в соціально-технічних системах є «розмитими», погано структурованими і часто не мають чітко визначеного формулювання.

Замість пошуку «вірного рішення» м'який системний підхід зосереджується на формуванні розуміння ситуації через участь усіх зацікавлених сторін, моделюванні різних точок зору, виявленні суперечностей і побудові змін, які можуть бути прийнятними для більшості учасників. Такий підхід є інтерактивним, діалогічним і адаптивним, що робить його надзвичайно актуальним у контексті складних соціальних та управлінських завдань.

Рассел Черчман зробив вирішальний крок у напрямку гуманізації системного аналізу. Його ідеї лягли в основу нової парадигми, де інтуїція, етика, культура та соціальна реальність стали невід'ємною частиною аналітичного процесу. У сучасному контексті – особливо у сфері управління змінами, стратегічного мислення, державного управління та соціальних

інновацій – підхід Черчмана зберігає свою теоретичну актуальність і практичну цінність.

Таблиця 1.5

Схематичне порівняння підходів Джей Форрестера і Рассела Черчмана

Критерій	Джей Форрестер	Рассел Черчман
Тип моделі	Жорстка, кількісна	М'яка, якісна
Орієнтація	Технічна	Соціальна
Інструментарій	Диференційні рівняння, комп'ютерне моделювання	Картування проблем, діалог

Системний аналіз у сучасних міждисциплінарних дослідженнях

У XXI столітті системний аналіз трансформувався з інструмента структурного мислення в універсальний міждисциплінарний підхід, здатний забезпечити цілісне бачення складних соціально-технічних систем. Його розвиток визначається стрімким прогресом інформаційних технологій, зокрема впровадженням обчислювального моделювання, штучного інтелекту (ШІ), машинного навчання (МН), технологій великих даних (Big Data) і хмарних обчислень. Ці технології не лише розширили можливості аналізу складних систем, а й забезпечили інтеграцію різнорідних знань і даних у єдині аналітичні моделі.

Сьогодні системний аналіз виступає методологічною платформою, яка забезпечує ефективну комунікацію між науками – як природничими, так і соціально-гуманітарними.

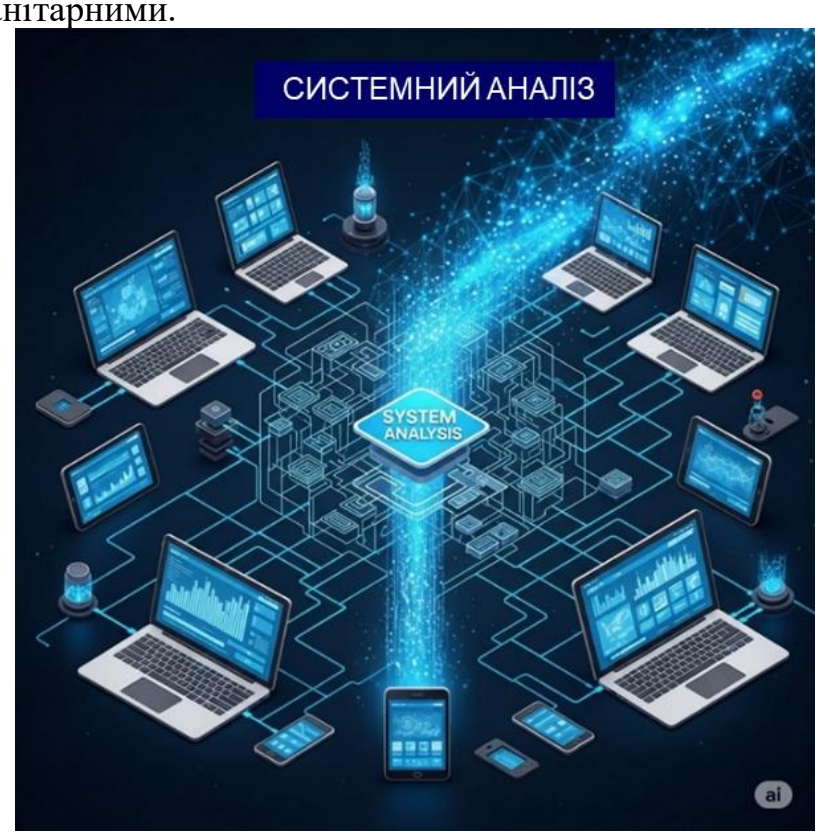

Рис. 1.3. Інтеграція системного аналізу з цифровими технологіями

Його інтерфейс з галузями, що мають високий ступінь складності й невизначеності, такими як екологія, медицина, енергетика, національна безпека, кібербезпека, економіка, урбаністика та біоінженерія**,** створює нові можливості для прогнозування, оптимізації та прийняття рішень у динамічному середовищі. Наприклад, у медицині системний підхід дозволяє поєднувати клінічні дані, геномні дослідження, епідеміологічні моделі та поведінкову аналітику для формування персоналізованих протоколів лікування. В екології – застосовуються складні моделі симуляції кліматичних змін, що охоплюють економічні, політичні та біосферні фактори.

Таблиця 1.6

Приклади міждисциплінарного використання системного аналізу

Галузь	Приклад застосування	Методи
Енергетика	Прогнозування попиту та оптимізація генерації	Системна динаміка, AHP
Медицина	Моделювання епідемій	Агентне моделювання
Екологія	Моделі сталого розвитку	Мережевий аналіз, GIS
Кібербезпека	Аналіз загроз і вразливостей	Байєсівський аналіз, графові моделі
Управління ризиками	Аналіз сценаріїв ризику	FMEA, Monte Carlo Simulation

Сучасний системний аналіз – це не просто набір методів; це цілісна філософія дослідження, яка враховує багаторівневу взаємодію технологічних, соціальних, екологічних, політичних та економічних факторів**.** Особливо важливою є здатність системного підходу враховувати не лише прямі причинно-наслідкові зв’язки, а й латентні ризики, нелінійність процесів, часові затримки та складну динаміку адаптивних середовищ.

У сфері управління ризиками, де системний аналіз набув особливої актуальності, інтегруються кількісні методи (імовірнісне моделювання, аналіз сценаріїв, баєсівський підхід) та якісні методики (експертне оцінювання, SWOT-аналіз, Delphi-метод), що дозволяє будувати багатошарові системи підтримки прийняття рішень. Ризик сприймається не лише як ймовірність негативної події, а як характеристика складної системи в умовах невизначеності, де необхідне моделювання поведінки всієї системи, а не лише її окремих компонентів.

Таким чином, системний аналіз в умовах сучасної наукової парадигми є потужним міждисциплінарним інструментом, що поєднує аналітичні, обчислювальні та прогностичні можливості. Його роль не обмежується техніко-економічною сферою: він є невід’ємним елементом стратегічного планування, розробки політик, інноваційного дизайну та трансформації складних організаційно-технологічних систем. З огляду на це, системний аналіз можна розглядати як ключову методологію майбутнього для дослідження взаємодії людини, технологій і природи в умовах глобальних трансформацій

1.2. Основні поняття системного аналізу: система, структура, зв’язки, цілі, середовище

Поняття «система» в системному аналізі

У межах системного аналізу категорія «система» розглядається як фундаментальна концептуальна одиниця, що слугує базисом для моделювання, оптимізації, прийняття рішень та управління складними об’єктами і процесами різної природи. Термін «система» (від грец. *systēma* – ціле, складене з частин) інтерпретується як організована сукупність взаємопов’язаних елементів, що знаходяться у функціональній взаємодії один з одним і з зовнішнім середовищем з метою досягнення певної цілі або реалізації визначеної функції.

У системному підході система не зводиться лише до арифметичної суми складників; натомість, вона характеризується принципом *емерджентності* – появою нових властивостей на рівні цілого, які не притаманні окремим елементам у ізоляції. Саме це дозволяє говорити про систему як про якісно нову сутність, що має властивості, відмінні від властивостей її частин.

Класифікація систем.

У системному аналізі системи класифікуються за низкою критеріїв, а саме: За природою елементів: (*Матеріальні* (фізичні системи: технічні пристрої, біологічні організми); *Ідеальні* (логічні, математичні, інформаційні моделі); *Соціальні* (суспільства, організації); *Кіберфізичні* (поєднання апаратного та програмного компонентів із зворотним зв’язком – як у системах Інтернету речей)). За рівнем організації: (Прості, Складні, Ієрархічні, Гетерогенні (різнорідні).

За відношенням до зовнішнього середовища: (*Закриті* системи (ізольовані від зовнішніх впливів); *Відкриті* системи (взаємодіють із зовнішнім середовищем, адаптуються та змінюються)).

Основні системні характеристики включають до себе наступне:

1. Цілісність (інтегративність). Усі елементи системи об’єднані в єдине ціле, внаслідок чого виникає синергетичний ефект: результат функціонування системи перевищує суму ефектів окремих компонентів. Це забезпечує системну якість, яка не може бути пояснена лише через властивості елементів.

2. Взаємозв’язки та взаємодія елементів. Компоненти системи перебувають у стані функціональної взаємодії через потоки інформації, енергії або матеріалу. Такі зв’язки можуть бути: *Лінійними* (прямий причинно-наслідковий зв’язок); *Нелінійними* (наявність складних зворотних зв’язків); *Ієрархічними* (підпорядкованість у структурі); *Мережевими* (децентралізовані, поліструктурні взаємодії – характерні для кіберфізичних або соціотехнічних систем).

3. Структурованість. Система має чітко організовану внутрішню архітектуру, яка визначає порядок і способи об'єднання елементів. Структура може бути: *Функціональною* (розподіл за функціями); *Морфологічною*

(просторова чи логічна конфігурація); *Динамічною* (структура, що змінюється з часом відповідно до адаптивних процесів).

4. Цілеспрямованість (телологічність). Будь-яка система орієнтована на досягнення конкретної мети або реалізацію функціонального призначення. У цьому контексті важливою є концепція керованості системи, яка забезпечується через механізми управління (як правило, у вигляді зворотного зв'язку) та здатність до саморегуляції.

5. Взаємодія із середовищем. У відкритих системах середовище виступає джерелом інформації, ресурсів і факторів впливу. Такі системи вимагають постійної адаптації, прогнозування змін середовища та стратегічного управління. Вони характеризуються такими властивостями, як гомеостаз (стійкість до змін) та адаптивність (здатність до змін у відповідь на зовнішні виклики).

Приклади систем у різних дисциплінах:

1) У техніці: енергетична система, інформаційно-керована система (ІКС), авіаційний навігаційний комплекс.

2) У біології: нервова система, екосистема, імунна система.

3) У соціології: політична система, освітня система, система правосуддя.

4) У економіці: банківська система, система фінансового контролю, система управління ризиками.

5) У кібербезпеці: система виявлення вторгнень (IDS), система управління інформаційною безпекою (ISMS), криптографічна система.

Системне мислення дозволяє не лише моделювати складні об'єкти, а й переходити до формування комплексних стратегій управління, аналізу ризиків, розробки інноваційних технологічних рішень. Це особливо актуально в умовах цифрової трансформації, коли виникають гібридні об'єкти – соціотехнічні, кіберфізичні та когнітивно-інформаційні системи, які потребують міжгалузевого аналізу та інтероперабельності

Типи систем

У контексті безпеки та управління ризиками важливо мати чітке уявлення про типологію систем, які можуть бути об'єктами аналізу. Розуміння типів систем дозволяє точніше визначити характер можливих загроз, вразливостей, а також адаптувати методики управління ризиками до специфіки конкретної системи.

Системи можуть класифікуватися за різними критеріями, зокрема: за природою компонентів (технічні, біологічні, соціальні, змішані), за ступенем автоматизації (ручні, автоматизовані, автономні), за рівнем взаємодії з навколишнім середовищем (відкриті, закриті), за інформаційною насиченістю (інформаційно активні / пасивні).

Проте для завдань ідентифікації ризиків та захисту технічних систем найважливішими типами є, а саме:

1. Технічні системи
2. Соціальні системи
3. Кіберфізичні системи

Розглянемо ідентифікацію ризиків та захисту технічних систем більш детальніше.

1. Технічні системи

Технічна система – це сукупність взаємопов’язаних технічних елементів, які функціонують з метою виконання заданих функцій. Основу складають апаратні компоненти: машини, пристрої, інструменти, мережі, механізми тощо.

Приклади систем: Енергетичні установки (ТЕС, АЕС), Автоматизовані виробничі лінії, Інженерні мережі (водопостачання, електропостачання).

Особливості ризиків: Переважно фізичні та механічні загрози (відмова обладнання, поломки, аварії). Основні методи управління ризиками – технічне обслуговування, резервування, діагностика стану.

2. Соціальні системи

Соціальні системи – це сукупності людей, об'єднаних у рамках певної організації, структури або суспільної взаємодії. Їхня діяльність регулюється нормами, правилами, ієрархією та соціальними механізмами.

Приклади систем: Колективи співробітників підприємств, Громадські інститути (освіта, охорона здоров’я), Органи влади, правоохоронні структури.

Особливості ризиків: Людський фактор (помилки, порушення інструкцій, зловмисна діяльність). Неформальні впливи (корупція, конфлікти, психологічний тиск). Методи управління ризиками: тренінги, контроль процедур, культура безпеки.

3. Кіберфізичні системи (КФС)

Кіберфізичні системи (Cyber-Physical Systems, CPS) – це інтегровані системи, що поєднують фізичні об’єкти та процеси з цифровими технологіями моніторингу, управління та зв’язку. Основна мета – забезпечення адаптивного, автономного функціонування з можливістю взаємодії з зовнішнім середовищем у реальному часі.

Приклади систем: Розумні електромережі (smart grid), Автономні транспортні системи (безпілотні автомобілі), Індустрія 4.0: автоматизовані фабрики, які самостійно приймають рішення.

Особливості ризиків: Комбінація фізичних і кіберзагроз. Підвищена вразливість до атак через інтерфейси зв’язку. Методи управління ризиками: захист каналів зв’язку, виявлення аномалій, багаторівнева автентифікація.

Таблиця 1.7

Порівняльна таблиця типів систем

Критерій	Технічні системи	Соціальні системи	Кіберфізичні системи
Основні компоненти	Механізми, пристрої, техніка	Люди, соціальні структури	Взаємодія фізичних об'єктів з IT-системами
Приклади	Генератори, лінії електропередач	Команди, колективи, організації	Smart Grid, IoT-пристрої, автономні машини
Типи загроз	Поломки, зношення, фізичні аварії	Людські помилки, конфлікти, саботаж	Кібератаки, збої в керуванні, фізичне пошкодження
Методи захисту	Резервування, ТО, діагностика	Процедури, навчання, дисципліна	Кібербезпека, адаптивні алгоритми, моніторинг
Рівень складності	Середній	Високий (через непередбачуваність)	Дуже високий (інтердисциплінарний характер)

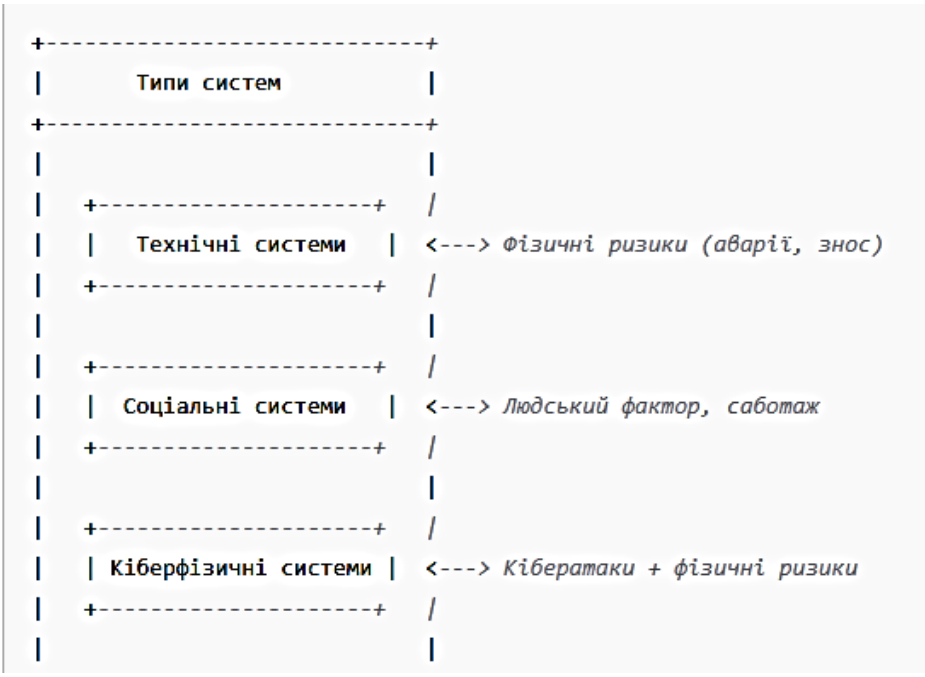

Рис. 1.4. Схематичне зображення типів систем (технічні, соціальні, кіберфізичні)

Класифікація систем за типом є важливим кроком для вибору методів аналізу ризиків, розробки захисних стратегій та забезпечення стійкості до загроз. Технічні системи потребують традиційних підходів до безпеки, соціальні – зосередженості на поведінці людей, а кіберфізичні – комплексного поєднання кіберзахисту та фізичної безпеки.

У подальших розділах буде детально розглянуто методи аналізу ризиків, специфічні для кожного типу систем, а також інструменти

моніторингу та виявлення аномалій, які враховують особливості взаємодії компонентів.

Цільові функції та критерії ефективності

Будь-яка система, зокрема технічна, створюється не випадково, а для досягнення визначеної мети, яка відображає потребу в певній функції, дії чи результаті. У системному аналізі мету формалізують у вигляді функції цілі (англ. *objective function*), що дозволяє застосовувати методи оптимізації, моделювання та прогнозування для визначення найкращих способів реалізації цієї мети в заданих умовах.

Функція цілі: сутність і роль

Функція цілі – це математична або логічна модель, яка формалізує бажаний результат функціонування системи. Вона визначає, що вважається успішною роботою системи та яким чином ця успішність може бути виміряна.

Приклади функцій цілі: Мінімізація витрат при заданому рівні якості продукції (у виробничій системі). Максимізація надійності при фіксованому бюджеті на обслуговування (в інфраструктурній системі). Мінімізація часу відгуку в кіберфізичних системах управління. Максимізація задоволеності користувачів у соціально-організаційній системі.

Критерії ефективності – це кількісні або якісні показники, які використовуються для оцінювання, наскільки успішно система виконує свою функцію цілі. Вони дозволяють порівнювати альтернативи, приймати управлінські рішення, здійснювати контроль і корекцію функціонування системи.

Найпоширенішими критеріями ефективності є:

1. Ефективність

Ефективність (англ. *Efficiency*) – це відношення отриманого результату до витрачених ресурсів. Вона може розглядатися як загальний показник доцільності існування або роботи системи.

Приклади:

1) Кількість оброблених одиниць продукції на одиницю енергії.
2) Обсяг виконаних транзакцій на одиницю часу.
3) Економічна рентабельність інвестицій у кіберзахист.

Чим вище ефективність, тим краще система виконує свою функцію цілі з меншими витратами.

2. Надійність

Надійність (англ. *Reliability*) – це здатність системи безвідмовно функціонувати протягом визначеного часу та в заданих умовах. Вона є критичним критерієм для технічних та інформаційно-керованих систем, особливо в умовах ризику.

Визначальні показники:

1) Середній час безвідмовної роботи (MTBF).
2) Імовірність відмови в заданому інтервалі.
3) Частота відмов та відновлення.

Надійність визначає ступінь довіри до системи як до стабільного елемента в умовах невизначеності.

3. Адаптивність

Адаптивність (англ. *Adaptability*) – це здатність системи адаптувати свою поведінку, структуру або параметри у відповідь на зміни середовища або внутрішнього стану.

Типи адаптивності, а саме: Структурна: зміна конфігурації (наприклад, переключення на резервні канали). Функціональна: зміна логіки роботи або сценаріїв управління. Поведінкова: здатність навчатися (штучний інтелект, машинне навчання).

Приклади:

1) Автоматичне регулювання тиску в трубопроводах у відповідь на збої.

2) Перебудова маршруту автономного автомобіля при виявленні перешкоди.

3) Реагування на аномалії в кіберзагрозах за допомогою AI-алгоритмів.

Високий рівень адаптивності є важливою умовою стійкості системи до ризиків і зовнішніх впливів.

Таблиця 1.8

Порівняльна таблиця критеріїв ефективності

Критерій	Сутність	Ключові метрики	Значення для системи
Ефективність	Відношення результату до ресурсів	Продуктивність, ROI, витрати/результат	Визначає доцільність функціонування
Надійність	Ймовірність безвідмовної роботи у визначених умовах	MTBF, частота відмов, час простою	Забезпечує стабільність і передбачуваність роботи
Адаптивність	Здатність реагувати на зміни середовища чи внутрішніх умов	Час перебудови, ступінь автоматизації, гнучкість	Визначає гнучкість і здатність до саморегуляції

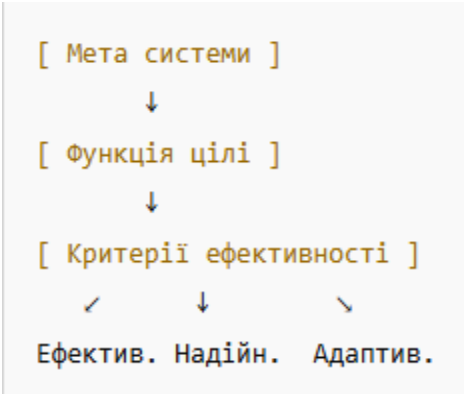

Рис. 1.5. Графічне представлення взаємозв’язку мети системи та критеріїв ефективності

Функція цілі – це абстрактна модель бажаного результату, а критерії ефективності – це способи її конкретного вимірювання. Система може бути ефективною, але ненадійною чи неадаптивною – і це вплине на прийняття рішень щодо її модернізації або реінжинірингу.

Формулювання функції цілі та визначення критеріїв ефективності є центральним етапом системного аналізу. Без чітко сформульованої функції цілі неможливо оцінити якість функціонування системи, а без критеріїв ефективності – обґрунтувати вибір технологій, архітектурних рішень чи моделей управління. Різні системи можуть вимагати пріоритетності одного або кількох критеріїв залежно від галузі застосування, умов експлуатації та ризикового середовища.

Взаємодія системи із середовищем: відкрита і закрита системи

Системи класифікуються за ступенем взаємодії із середовищем:

Закрита система – не взаємодіє із середовищем або взаємодіє обмежено. Частіше зустрічається у моделях, де необхідна повна автономія (наприклад, герметичні технічні системи).

Відкрита система – активно обмінюється ресурсами, інформацією та енергією із середовищем. Такий тип є типовим для соціальних і кіберфізичних систем.

Таблиця 1.9

Характеристики відкритої та закритої систем

Ознака	Відкрита система	Закрита система
Взаємодія з середовищем	Активна	Обмежена або відсутня
Приклади	Організація, смарт-гаджет	Механічний годинник, вакуумна камера
Гнучкість	Висока	Низька
Складність управління	Висока (через мінливість середовища)	Низька (через стабільність)

Розуміння базових категорій системного аналізу – таких як система, структура, зв’язки, цілі, типи систем та їх взаємодія з середовищем – є критичним для ефективного моделювання, прогнозування та мінімізації ризиків. Класифікація систем за типом і структурою дозволяє адаптувати методи системного аналізу до конкретних задач, особливо в умовах високої складності, невизначеності та динамізму сучасного техногенного середовища.

У подальших підрозділах будуть розглянуті принципи формалізації систем, моделювання взаємодії факторів ризику та застосування системного аналізу у реальних прикладних задачах.

1.3. Методологічні принципи системного аналізу в контексті ризиків

Методологічні принципи системного аналізу виступають фундаментом для побудови ефективних підходів до ідентифікації, аналізу та прогнозування ризиків у складних соціально-економічних, технічних і природно-техногенних системах. Ці принципи забезпечують цілісне розуміння взаємозв'язків між елементами системи, динаміку їх розвитку та вплив невизначеності на поведінку системи в умовах ризику.

1. Принцип цілісності та ієрархії

Принцип цілісності вказує на необхідність розгляду системи як єдиного організму, в якому взаємодія всіх елементів породжує властивості, не властиві окремим частинам. У контексті ризиків, це означає необхідність оцінювання не лише індивідуальних ризик-факторів, а й їхніх комплексних взаємодій.

Основні характеристики цілісності: Виявлення синергетичних ефектів; Урахування нелінійності та множинності причинно-наслідкових зв’язків; Розгляд ризику як багатовимірного явища.

Ієрархічна структура систем

Системи, що аналізуються, мають багаторівневу організацію, де кожен рівень виконує специфічні функції та має відповідну структуру. Ієрархія дозволяє диференціювати ризики за рівнями впливу та управління.

Таблиця 1.10

Ієрархічна структура ризик-орієнтованих систем

Рівень системи	Приклад	Основні ризики
Мікрорівень	Компонент обладнання	Вихід з ладу, зношування
Мезорівень	Виробничий підрозділ	Виробничі збої, людський фактор
Макрорівень	Організація/галузь	Репутаційні, фінансові ризики
Мегарівень	Економіка, держава	Геополітичні, екологічні

Рис. 1.6. Модель демонструє вертикальну ієрархію з потенційними каналами ризиків між рівнями.

2. Принцип зворотного зв'язку

Зворотний зв'язок – це механізм саморегуляції системи, що забезпечує адаптацію до змін зовнішнього середовища через корекцію власної поведінки. У контексті ризиків, позитивний зворотний зв'язок може підсилювати ризики, тоді як негативний – стримувати їх.

Типи зворотного зв'язку: Негативний (стабілізуючий): спрямований на зменшення відхилень; Позитивний (дестабілізуючий): спричиняє лавиноподібне наростання змін.

Таблиця 1.11

Приклади реалізації зворотного зв'язку в системах управління ризиками

Сфера застосування	Приклад	Тип зворотного зв'язку
Фінанси	Автоматичне коригування ставок	Негативний
Енергетика	Попереджувальні сигнали аварій	Негативний
Соціальні мережі	Поширення паніки або фейків	Позитивний
Промисловість	Аварійне відключення системи	Негативний

Рис. 1.7. Динамічна петля зворотного зв’язку, що демонструє взаємозалежність між дією та наслідком.

3. Системне моделювання: концептуальні, інформаційні, математичні моделі

Концептуальні моделі

Концептуальні моделі – це абстрактні схеми, що описують структуру та динаміку системи без точних чисельних параметрів. Вони є першим етапом формалізації знань про систему.

Переваги: Доступність для сприйняття; Швидке створення; Орієнтація на експертне мислення.

Недоліки: Суб’єктивізм; Відсутність формалізації.

Інформаційні моделі

Інформаційна модель – це структурований опис об’єктів, процесів та взаємозв’язків у формі, придатній для цифрового представлення. Часто реалізується у вигляді баз даних або інформаційно-аналітичних систем.

Таблиця 1.12

Порівняння моделей

Тип моделі	Рівень формалізації	Призначення	Інструменти реалізації
Концептуальна	Низький	Узагальнене розуміння системи	Карти знань, UML, блок-схеми
Інформаційна	Середній	Опис структур та взаємозв’язків	Бази даних, експертні системи
Математична	Високий	Кількісна оцінка ризиків	Системи моделювання, MATLAB, R

Математичні моделі

Це точні формалізовані описи системних процесів, що дозволяють аналізувати поведінку системи, прогнозувати наслідки впливів та оцінювати ефективність рішень.

Основні типи математичних моделей: Стохастичні моделі (імовірнісні): аналіз невизначеності; Детерміністичні моделі: оцінка чітких причинно-наслідкових залежностей; Системи диференціальних рівнянь: (моделювання динаміки системи); Імітаційні моделі: (дослідження поведінки за різних сценаріїв).

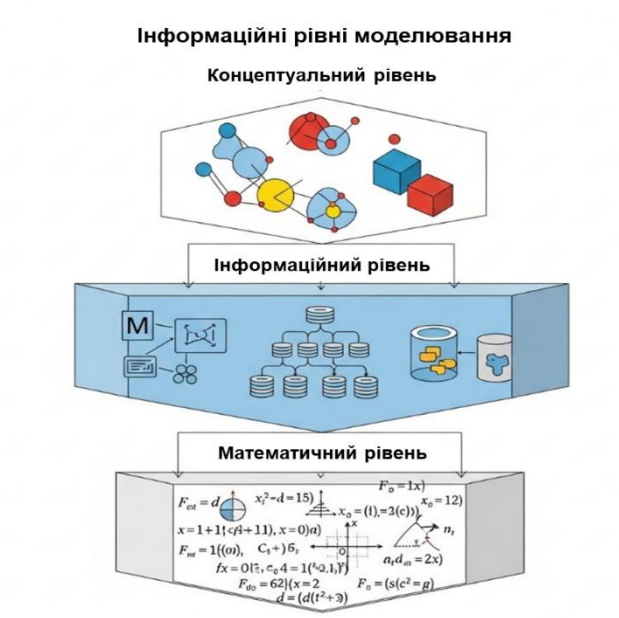

Рис. 1.8. Взаємозв'язок концептуального, інформаційного та математичного рівнів моделювання.

Методологічні принципи системного аналізу – цілісність, ієрархічність, зворотний зв’язок та моделювання – є базовими інструментами для формалізації, діагностики й управління ризиками у складних системах. Їх інтеграція у практику дозволяє створити адаптивні, динамічні й орієнтовані на майбутнє підходи до ризик-менеджменту.

Для підвищення навчального ефекту, рекомендується використання спеціалізованого програмного забезпечення типу AnyLogic, MATLAB, RiskWatch або Vensim для побудови моделей ризиків у системах із зворотним зв’язком та ієрархією.

1.4. Інструментарій системного аналізу для оцінювання ризиків

Оцінювання ризиків у сучасних складних системах вимагає багаторівневого та міждисциплінарного підходу, що враховує не лише ймовірнісні аспекти подій, але й структурно-функціональні, поведінкові та когнітивні взаємозв’язки між елементами системи. У цьому контексті

системний аналіз пропонує розгалужений інструментарій, який дозволяє якісно і кількісно досліджувати природу ризиків, моделювати сценарії їх розвитку та приймати ефективні управлінські рішення. У цьому підрозділі розглядаються ключові методи системного аналізу, які можуть бути застосовані для ідентифікації, структуризації, моделювання та ранжування ризиків.

Побудова причинно-наслідкових діаграм

Fishbone-діаграма (діаграма Ішікави)

Fishbone-діаграма (діаграма причинно-наслідкових зв’язків) використовується для ідентифікації потенційних причин конкретного ризику або проблеми. Основна перевага – систематизація знань експертів і виявлення глибинних чинників ризиків.

Основні категорії причин: Людський фактор. Матеріальні ресурси. Методологія. Менеджмент. Навколишнє середовище. Вимірювання.

Рис. 1.9. Приклад побудови Fishbone-діаграми (діаграми Ішікави) для виявлення причин виготовлення деталі неправильного розміру

Таблиця 1.13

Приклад заповнення Fishbone-діаграми для ризику кіберінциденту

Категорія	Причини
Людський фактор	Недостатня кваліфікація, нехтування правилами
Методологія	Відсутність стандартів реагування
Менеджмент	Незадовільне управління безпекою
Навколишнє середовище	Відсутність захисту зовнішніх каналів

Дерево відмов (Tree of Faults)

Дерево відмов – це логічна модель, що дозволяє визначити комбінації помилок, які можуть призвести до критичного ризику. Вузли дерева поділяються на базові події та проміжні події, об'єднані логічними операторами AND/OR.

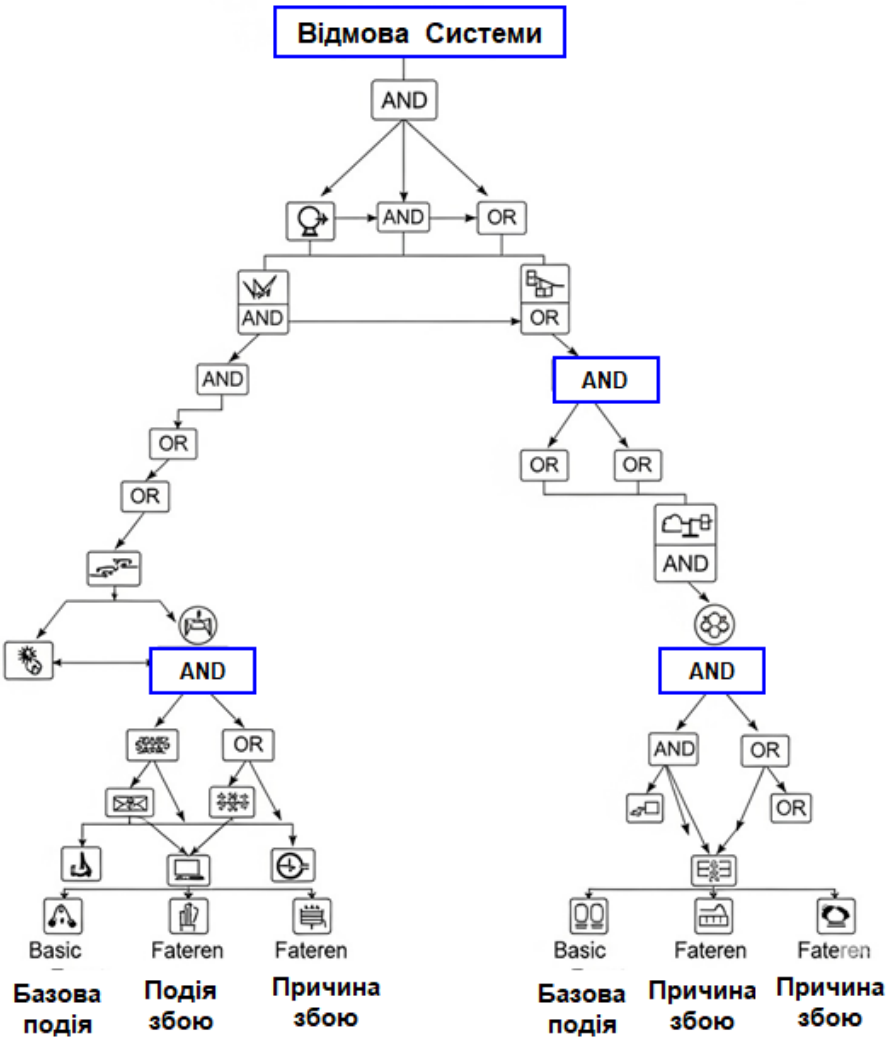

Рис. 1.10. Дерево відмов (Fault Tree Analysis) із використанням логічних операторів AND/OR для визначення причин технічного збою

Переваги методу, а саме: виявлення критичних комбінацій подій. формалізація сценаріїв розвитку відмов.

Таблиця 1.14

Приклад базових подій для ризику технічної відмови

Базова подія	Ймовірність	Примітки
Вихід з ладу джерела живлення	0.02	Пов'язано з зовнішнім впливом
Збій ПЗ	0.05	Програмна помилка
Людська помилка	0.03	Неправильна експлуатація

Використання структурної декомпозиції

Метод SADT (Structured Analysis and Design Technique)

Метод SADT (IDEF0-варіант) дозволяє описувати функціональну структуру систем, зокрема зв'язки між функціями, ресурсами та механізмами реалізації. Особливо ефективний при аналізі технологічних, логістичних та організаційних ризиків.

Рис. 1.11. Базова структура SADT-діаграми (IDEF0) з відображенням входів, керуючих сигналів, механізмів і виходів

Пояснення елементів:

1. Функція / Процес (Activity Box): Центральний елемент діаграми, що представляє конкретну дію, функцію або процес, який моделюється. Зазвичай це дієслово або дієслівна фраза, що описує виконувану роботу.

2. Вхід (Input): Елементи, що надходять до функції/процесу і необхідні для її виконання. Це можуть бути дані, матеріали, інформація, ресурси тощо. На діаграмі позначаються стрілками, що входять в ліву сторону блоку функції.

3. Вихід (Output): Результати, що генеруються функцією/процесом після її виконання. Це можуть бути оброблені дані, готові продукти, звіти, рішення тощо. На діаграмі позначаються стрілками, що виходять з правої сторони блоку функції.

4. Керування (Control): Елементи, що контролюють або регулюють виконання функції/процесу, але не є його входами або виходами. Це можуть бути правила, стандарти, політики, інструкції, умови, дозволи. На діаграмі позначаються стрілками, що входять у верхню сторону блоку функції.

5. Механізм (Mechanism): Засоби, інструменти, обладнання, програмне забезпечення, персонал або інші ресурси, що використовуються для виконання функції/процесу. На діаграмі позначаються стрілками, що входять у нижню сторону блоку функції.

Цей базовий шаблон є основою для побудови більш складних SADT-діаграм, де кожна функція може бути декомпозована на підфункції, розкриваючи деталізований опис системи

Таблиця 1.15

Приклад функціонального аналізу процесу ідентифікації ризиків

Функція	Вхід	Вихід	Керування	Механізм
Ідентифікація загроз	Дані моніторингу	Перелік загроз	Політика ІБ	Аналітик
Аналіз наслідків	Перелік загроз	Оцінка шкоди	Методологія	Програмне ПЗ

Метод IDEF

IDEF-моделювання (Integrated DEFinition for Function Modeling) є методологією, що об'єднує низку стандартів для опису, аналізу, проєктування та покращення складних систем, процесів і організаційних структур. Ці стандарти забезпечують формалізований підхід до створення моделей, які відображають логічні, функціональні та поведінкові аспекти досліджуваних об'єктів. Основною метою застосування IDEF-моделей є уніфікація способів представлення інформації для досягнення послідовності в розумінні складних систем усіма зацікавленими сторонами: від розробників до аналітиків, керівників та експертів з безпеки.

Серед багатьох варіантів IDEF-моделювання найчастіше для цілей аналізу ризиків застосовуються моделі IDEF0 та IDEF3, кожна з яких має специфічне призначення та акценти у представленні інформації.

Методологія IDEF0 базується на концепції функціонального моделювання та дозволяє детально відобразити, які функції виконує система, які ресурси вона використовує, які вхідні дані обробляє і які результати продукує. Основна одиниця моделювання в IDEF0 – це функціональний блок, який представляє окрему діяльність або процес, а також чотири типи зв’язків:

1) Входи (Inputs) – інформація або матеріали, що трансформуються функцією;

2) Виходи (Outputs) – результати функції;

3) Механізми (Mechanisms) – ресурси, які підтримують виконання функції;

4) Управління (Controls) – обмеження, правила, політики або нормативи, що регулюють виконання функції.

У контексті аналізу ризиків, IDEF0 дозволяє: Визначити критичні функції, які мають високий вплив на загальну надійність або безпеку

системи; Виявити вразливі ділянки функціонального ланцюга, де можливе порушення цілісності або збої у роботі; Встановити взаємозв’язки між функціями і ресурсами, що особливо важливо для ідентифікації потенційних точок відмови (failure points); Забезпечити візуалізацію ієрархії процесів, що дозволяє приймати обґрунтовані управлінські рішення щодо реорганізації або посилення контролю за окремими операціями.

Моделі IDEF0 широко застосовуються в аудиті інформаційної безпеки, при розробці систем управління ризиками, у процесах сертифікації відповідно до стандартів ISO/IEC (зокрема, ISO/IEC 27001).

IDEF3: Моделювання сценаріїв поведінки та часової послідовності процесів

На відміну від IDEF0, що фокусується на функціональній стороні, методологія IDEF3 орієнтована на опис послідовності подій і сценаріїв поведінки системи у часі. Це дозволяє моделювати процеси так, як вони фактично відбуваються, з урахуванням умов, гілок, альтернатив та точок прийняття рішень.

Основні компоненти IDEF3-моделей:

1) Об'єкти подій (UOB – Unit of Behavior) – елементарні операції або події;

2) Обмеження послідовності (Precedence Links) – відображають логіку виконання процесу: послідовність, розгалуження, паралельність;

3) Контексти сценаріїв – описують, у яких умовах виникає певний сценарій, які події його запускають та припиняють.

У контексті аналізу ризиків, застосування IDEF3 дозволяє: Моделювати реальні сценарії розвитку подій, включаючи ймовірні траєкторії помилок, інцидентів або вторгнень; Визначити критичні точки прийняття рішень, де можливе втручання людського фактора або автоматизованих систем контролю; Аналізувати взаємозв’язки між подіями для виявлення ланцюгових реакцій і потенційних катастрофічних наслідків; Створювати гнучкі моделі поведінки системи в умовах змінного середовища, що є особливо важливим для динамічних ризиків у сфері кібербезпеки або промислової автоматизації.

Комплексне використання IDEF0 та IDEF3 у ризик-орієнтованому підході

У практиці управління ризиками ефективним є поєднання IDEF0 та IDEF3, оскільки це дозволяє отримати цілісну картину як структурної функціональності системи (що і як виконується), так і динаміки її поведінки (у яких послідовностях і за яких умов). Такий інтегрований підхід забезпечує:

1) Високу точність і повноту ідентифікації ризиків;

2) Оптимізацію заходів реагування на ризики з урахуванням функціонального навантаження і часових сценаріїв;

3) Підвищення обґрунтованості прийняття управлінських рішень на основі формалізованої та структурованої інформації;

4) Забезпечення відповідності сучасним міжнародним підходам до моделювання процесів, зокрема BPM (Business Process Management) та системного аналізу.

Таким чином, використання IDEF0 та IDEF3 є потужним інструментарієм для моделювання складних технічних і організаційних систем у рамках процесу управління ризиками, що дозволяє не лише підвищити розуміння структури та динаміки процесів, але й забезпечити ефективну превенцію критичних відмов, зниження вразливостей і покращення загального рівня безпеки.

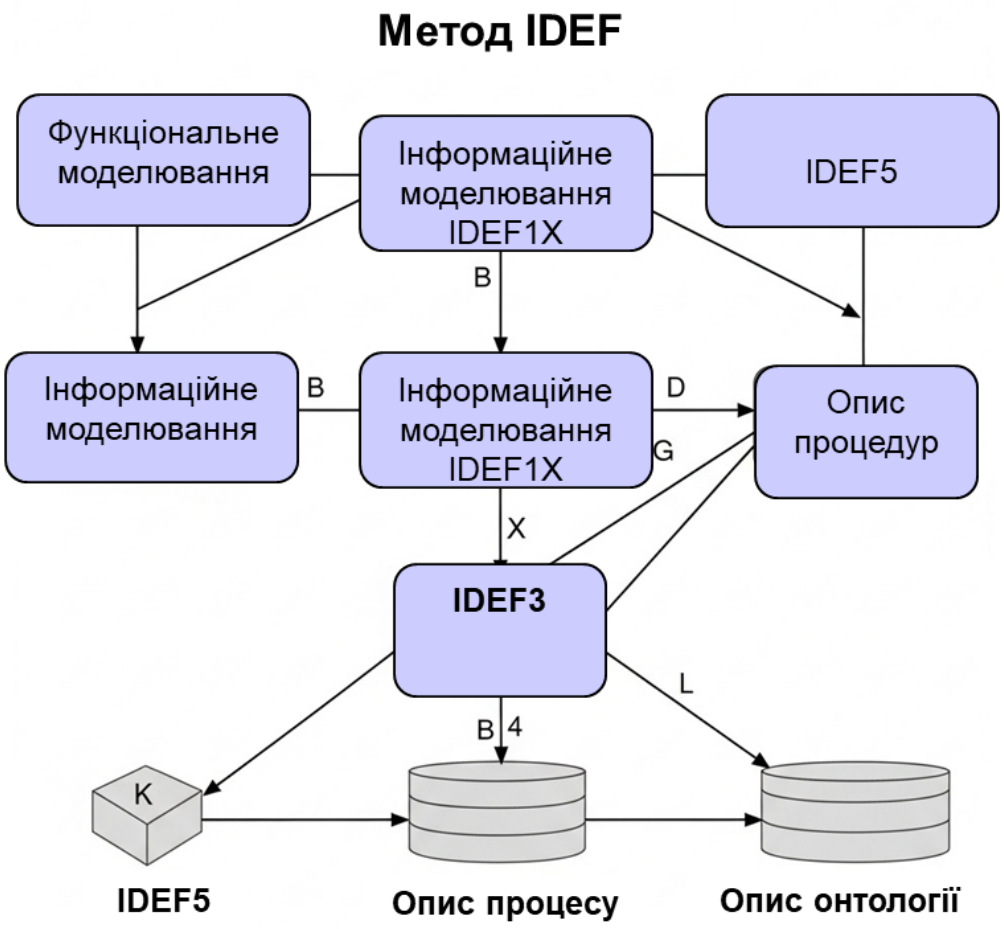

Рис. 1.12. Базовий шаблон IDEF-моделювання

Системна динаміка та когнітивне моделювання

Системна динаміка

Цей підхід дозволяє будувати моделі з часовими петлями зворотного зв'язку, що відображають нелінійну поведінку складних систем. Використовується для моделювання ризиків, пов’язаних з затримками, накопиченнями, інерційними ефектами.

Компоненти моделей:

1. Стоки і потоки
2. Зв’язки зворотного зв’язку
3. Затримки

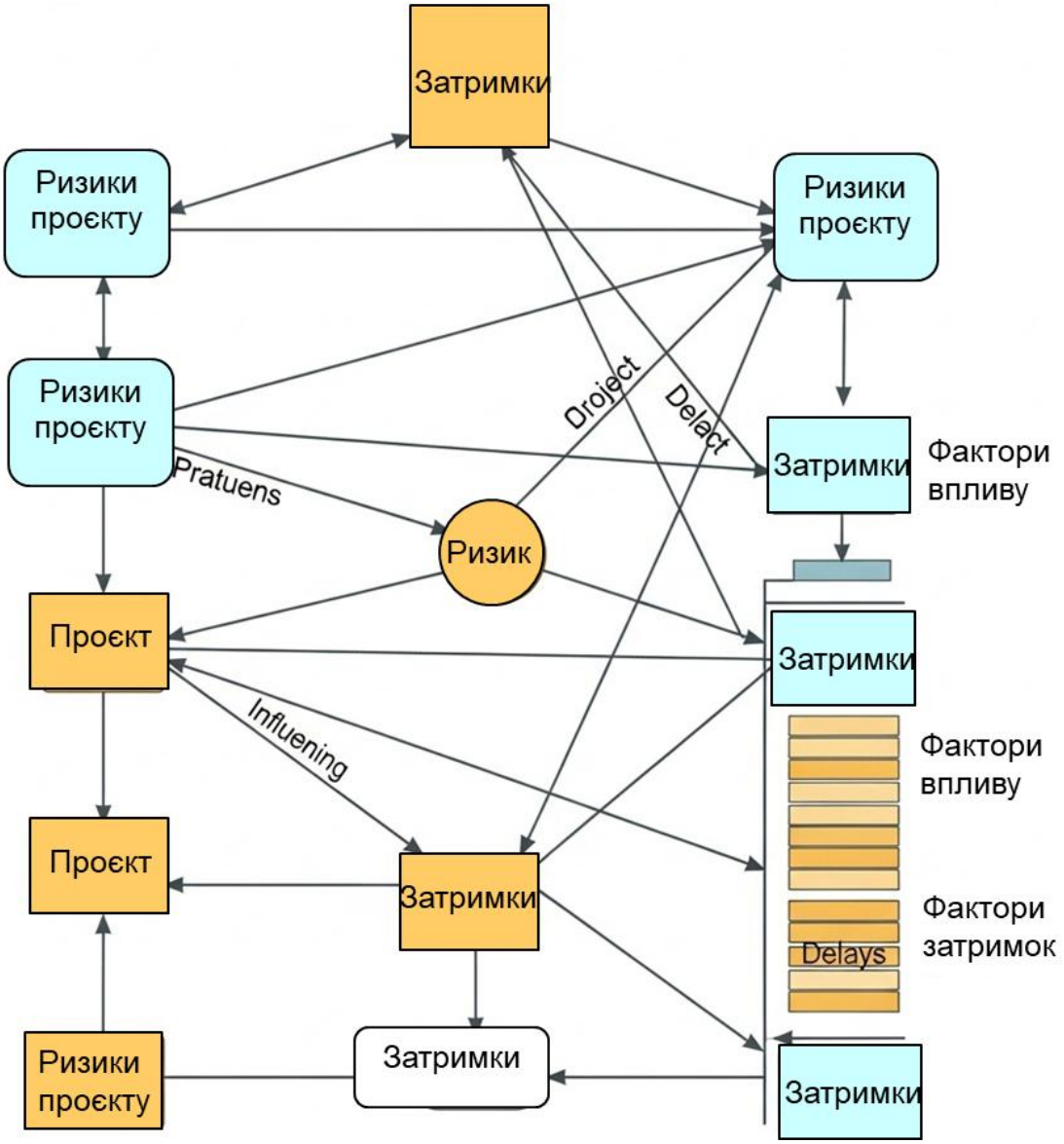

Рис. 1.13. Динамічна модель розвитку ризику проекту (діаграма із затримками та впливами)

Таблиця 1.16

Приклад впливів у моделі ризику реалізації проєкту

Елемент	Впливає на	Тип впливу	Коментар
Досвід персоналу	Швидкість виконання задач	Позитивний	Навчання зменшує затримки
Обсяг фінансування	Швидкість реалізації	Позитивний	Додаткові ресурси
Рівень ризику	Затримка	Негативний	Уповільнення рішення

Когнітивне моделювання

Когнітивна карта – граф знань, що відображає причинно-наслідкові зв'язки між концептами. Застосовується для аналізу якісних ризиків, оцінки суб'єктивних чинників, стратегічного прогнозування.

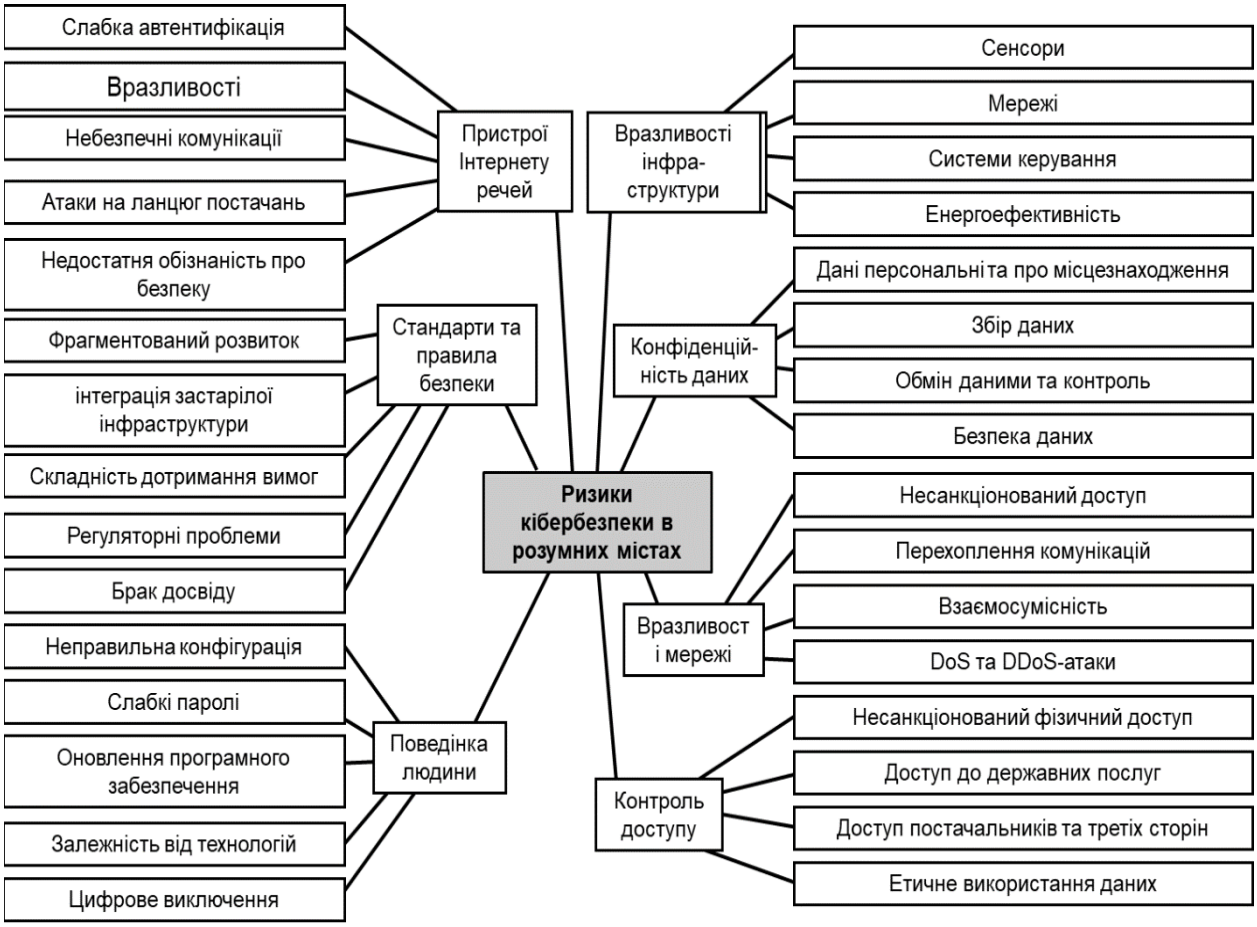

Рис. 1.14. Когнітивна карта ризиків інформаційної безпеки

Переваги: Формалізація експертних знань. Можливість сценарного аналізу. Визначення ключових факторів ризику.

Методи аналізу ієрархій (AHP) у контексті ризик-менеджменту

Метод AHP (Analytic Hierarchy Process) застосовується для ранжування ризиків, вибору пріоритетних заходів з управління або визначення вагових коефіцієнтів впливу факторів. В основі методу – побудова ієрархії цілей, критеріїв та альтернатив, а також попарне порівняння з експертним оцінюванням.

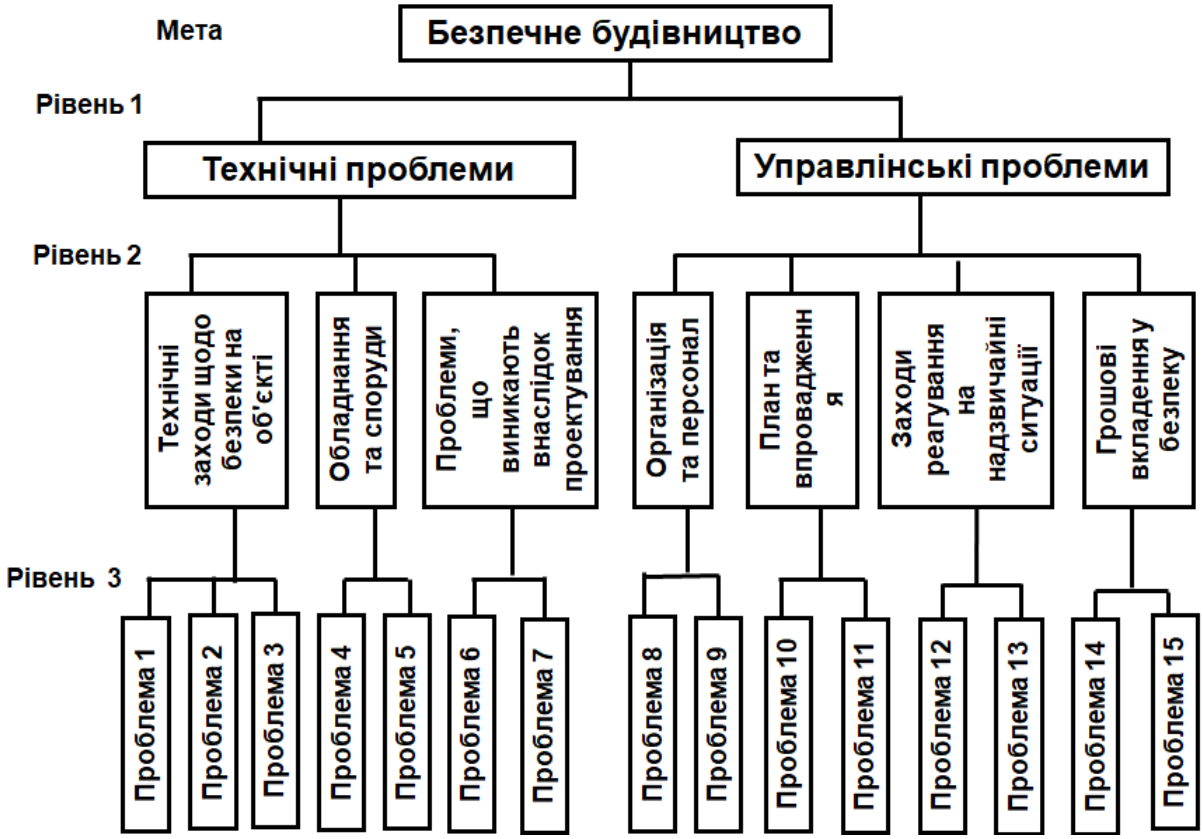

Рис. 1.15. Ієрархічна структура оцінювання ризиків із рівнями мети, критеріїв та альтернатив

Таблиця 1.17

Матриця попарного порівняння ризиків

	Ризик A	Ризик B	Ризик C
Ризик A	1	3	5
Ризик B	1/3	1	2
Ризик C	1/5	1/2	1

Результати обчислень:

1) Ризик A: 0.61
2) Ризик B: 0.27
3) Ризик C: 0.12

Переваги методу AHP:

1) Інтеграція якісних і кількісних оцінок
2) Структуризація складних проблем
3) Залучення експертних оцінок

Інструменти системного аналізу, що розглядаються у цьому підрозділі, дозволяють здійснювати повноцінну багатовимірну оцінку ризиків, адаптовану до складності сучасних технічних і соціотехнічних систем.

Поєднання причинно-наслідкових діаграм, методів декомпозиції, динамічного моделювання та багатокритеріального аналізу забезпечує

надійну методологічну базу для прийняття обґрунтованих управлінських рішень у сфері ризик-менеджменту.

Контрольні питання

1. У чому полягає сутність системного підходу та які етапи його становлення як наукового напряму?
2. Які наукові передумови виникнення системного аналізу склались у середині XX століття?
3. У чому полягає внесок Людвіга фон Берталанфі у розвиток системної теорії?
4. Яку роль у становленні системного аналізу відіграв Джей Форрестер і що таке системна динаміка?
5. Як Чарльз Черчман розвивав прикладні аспекти системного аналізу в управлінні та дослідженні операцій?
6. Якими є основні риси міждисциплінарного характеру сучасного системного аналізу?
7. Як змінювалась роль системного аналізу в дослідженнях ризиків у XXI столітті?
8. Що таке система з позиції системного аналізу, і які її основні характеристики?
9. Як класифікуються системи за природою (технічні, соціальні, кіберфізичні)?
10. Що таке структура системи та як вона впливає на функціонування системи в умовах ризику?
11. Яку роль відіграють зв’язки та взаємодії між елементами в системі?
12. Як визначаються цілі системи та яка їхня роль у ризик-орієнтованому підході?
13. Що таке середовище системи та як воно впливає на динаміку ризиків?
14. У чому відмінність між відкритими та закритими системами, з точки зору управління ризиками?
15. Що таке підсистеми та інтерфейси, і як вони застосовуються в моделюванні складних систем?
16. У чому полягає принцип цілісності в системному аналізі та як він допомагає у виявленні ризиків?
17. Як принцип ієрархії застосовується при аналізі складних систем у контексті ризиків?
18. Яке значення має принцип зворотного зв’язку для аналізу ризиків у динамічних системах?
19. Які типи моделей використовуються в системному моделюванні (концептуальні, інформаційні, математичні)?
20. Яким чином концептуальне моделювання сприяє ідентифікації потенційних ризиків у складних системах?
21. Як будується причинно-наслідкова діаграма типу «риб’ячий хребет» (Fishbone) для аналізу ризиків?

22. У чому полягає метод «дерева відмов» (Tree of Faults), і як він використовується у прогнозуванні небезпек?
23. Які переваги має структурна декомпозиція систем (SADT, IDEF) при вивченні ризикових компонентів?
24. Як системна динаміка дозволяє моделювати петлі зворотного зв’язку та затримки в поширенні ризиків?
25. У чому суть методу аналізу ієрархій (AHP) та як його застосовують для ранжування ризиків і прийняття рішень у сфері ризик-менеджменту?

Кейси до розділу 1

Кейс 1. Аналіз системної вразливості міської інфраструктури під час надзвичайної ситуації

Після сильного штормового фронту в одному з українських прибережних міст було порушено функціонування ключових елементів міської інфраструктури: енергопостачання, водопровід, зв’язок і транспорт. Через втрату електроенергії постраждали лікарні, відбулась затримка евакуації, а у соціальних мережах почали ширитися чутки, що підвищило рівень паніки.

Вам необхідно, застосовуючи системний підхід, дослідити структуру міжсистемної взаємодії, визначити тип системи (відкрита/закрита), побудувати схему зворотних зв’язків і запропонувати сценарії дій для запобігання каскадним ефектам у майбутньому.

Кейс 2. Оцінка ризиків у кіберфізичній системі логістичного управління

Підприємство логістичної галузі впровадило систему автоматичного складу, яка функціонує на базі IoT-пристроїв, машинного навчання та хмарної аналітики. Через неочікуваний збій у зв’язку з сервером управління виник ланцюг проблем: зупинка роботів, втрати даних, фізичні пошкодження товарів.

Ваше завдання – ідентифікувати тип системи, провести класифікацію ризиків (технічних, кібернетичних, організаційних), сформулювати функцію цілі цієї системи та обґрунтувати доцільність використання тієї чи іншої моделі аналізу ризиків (концептуальної, інформаційної або математичної).

Кейс 3. Ієрархічний підхід до аналізу ризиків у структурі правоохоронних органів

У контексті забезпечення правопорядку під час проведення великомасштабних публічних заходів правоохоронна система діє на кількох рівнях: від патрульного підрозділу до обласного управління. У минулому були зафіксовані випадки затримок реагування, недостатньої координації та інформаційної розбалансованості між рівнями.

На основі принципів ієрархічної організації системи побудуйте її багаторівневу модель, розподіліть типові ризики за рівнями (мікро-, мезо-, макро-) та визначте для кожного рівня відповідні цільові функції й критерії ефективності управління ризиками.

Кейс 4. Системна динаміка для прогнозування ризику аварії на хімічному підприємстві

Хімічне підприємство експлуатує реактор високого тиску, де контроль параметрів здійснюється автоматизовано. У ході обстеження виявлено тенденцію до зростання тиску вище допустимих значень. Перед вами стоїть завдання – дослідити, чи є у системі петлі зворотного зв'язку, які могли б стабілізувати ситуацію, чи навпаки – сприяють ескалації ризику.

Необхідно змоделювати систему у вигляді зворотних зв'язків (позитивних і негативних), визначити найбільш критичні точки впливу, сформулювати сценарії розвитку подій та запропонувати засоби раннього попередження й інструменти моніторингу.

Кейс 5. Формалізація ризиків у системі охорони здоров'я під час пандемії

Під час пандемії COVID-19 система охорони здоров'я в одному з регіонів зіткнулася з перенавантаженням: нестачею кисневих концентраторів, затримкою логістики ліків та браком медичного персоналу. Водночас рівень захворюваності продовжував зростати.

Застосовуючи принципи системного аналізу, побудуйте концептуальну модель взаємодії підсистем (лікарні, аптеки, логістика, органи управління). Визначте функцію цілі системи у кризовий період, оберіть релевантні критерії ефективності (наприклад, середній час реагування) та запропонуйте стратегії підвищення адаптивності системи до повторних хвиль захворювань.

Висновок по розділу 1

У межах першого розділу розкрито фундаментальні теоретико-методологічні засади системного аналізу як базової наукової платформи для дослідження та прогнозування ризиків у сфері безпеки технічних систем. Проаналізовано історичні витоки становлення системного підходу, а також внесок класиків – Людвіга фон Берталанфі, Джея Форрестера та Чарльза Черчмана – у формування міждисциплінарного наукового напряму, що став ключовим для вирішення складних інженерно-технологічних та управлінських задач.

Встановлено, що системний аналіз сьогодні є не лише прикладною дисципліною, але й методологією мислення, яка забезпечує інтеграцію знань з різних галузей – кібернетики, інформатики, інженерії, соціології – для

комплексного аналізу ризиків, пов’язаних із функціонуванням складних технічних систем.

У межах підрозділу 1.2 обґрунтовано ключові поняття системного аналізу, серед яких центральне місце займає категорія «система» – як впорядкована сукупність взаємодіючих елементів, що має визначену мету, структуру, функції та середовище існування. Проведено класифікацію систем на технічні, соціальні та кіберфізичні, що має вирішальне значення для ідентифікації специфічних типів ризиків у кожному випадку.

Розглянуто поняття підсистем, інтерфейсів, цільових функцій, а також взаємодію відкритих і закритих систем з оточенням, що створює передумови для оцінки адаптивності системи до зовнішніх впливів.

У підрозділі 1.3 було розкрито методологічні принципи системного аналізу в контексті ризиків, зокрема принцип цілісності – як необхідність розглядати систему в її повноті, з урахуванням усіх взаємозв’язків та ієрархічної структури; принцип зворотного зв’язку – як основа для моделювання динаміки ризикових процесів і їх впливу на систему. Акцентовано увагу на важливості використання різнорівневого моделювання (концептуального, інформаційного, математичного) як засобу формалізації ризиків та їхніх сценаріїв.

У підрозділі 1.4 детально охарактеризовано сучасний інструментарій системного аналізу, який використовується для виявлення, оцінювання та моделювання ризиків у складних технічних системах. До таких інструментів віднесено: причинно-наслідкові діаграми, що дозволяють ідентифікувати джерела проблем і сформувати логічну структуру причин ризиків; структурну декомпозицію процесів у межах методів SADT та IDEF, що забезпечує деталізацію функціональної архітектури систем; системну динаміку – для моделювання часових процесів із затримками, петлями зворотного зв’язку та інерційними ефектами, які є критично важливими для аналізу поведінкових аспектів ризиків; когнітивне моделювання – для виявлення експертних уявлень про причинно-наслідкові залежності між елементами системи ризиків; метод аналізу ієрархій (AHP) – як засіб кількісної оцінки пріоритетів ризиків та підтримки рішень у багатокритеріальному середовищі.

Таким чином, розділ 1 закладає науково-методологічне підґрунтя для подальшого дослідження ризиків у технічних системах, формуючи цілісне уявлення про об'єкт дослідження, методи його декомпозиції, інтерпретації взаємозв’язків і прийняття рішень в умовах невизначеності та складності.

РОЗДІЛ 2. СИСТЕМНІ МЕТОДИ ІДЕНТИФІКАЦІЇ ТА ОЦІНЮВАННЯ РИЗИКІВ

2.1. Системно орієнтовані методи виявлення ризиків у складних об’єктах

1. Характеристика складних систем та їхніх ризиків

Складні системи становлять особливий тип організації реальності, в якій взаємодія між численними компонентами призводить до формування поведінки, що не може бути повністю пояснена через вивчення окремих елементів ізольовано. На відміну від простих систем, де вихідна реакція прямо пропорційна вхідному впливу, складні системи демонструють поведінкову багатовимірність, що зумовлена численними нелінійними зв’язками, зворотними петлями впливу та часто – емерджентними властивостями, які виникають лише на рівні цілісної системи.

Ці системи можуть мати як штучну, так і природну природу, а також перебувати на межі між цими двома полюсами, утворюючи **гібридні типи**, які є характерними для сучасної доби техносоціальної еволюції. Залежно від природи елементів та характеру їх взаємодії, складні системи умовно поділяють на кілька категорій:

1) Технічні системи, до яких належать інфраструктурні комплекси, транспортні мережі, системи енергопостачання, кіберфізичні мережі. Їх головною ознакою є переважання технічних компонентів та сувора логіка функціонування, хоча сучасні технічні системи дедалі більше включають програмні, керовані штучним інтелектом компоненти, що ускладнює їхню динаміку.

2) Соціально-технічні системи, такі як організації, корпорації, державні інституції, у яких поєднуються технічні інструменти з людським фактором. У таких системах особливого значення набувають управлінські механізми, комунікаційні процеси та адаптивні стратегії.

3) Природно-технічні системи, наприклад, енергетичні об’єкти, які взаємодіють із навколишнім середовищем (гідроелектростанції, вітропарки, екосистеми із залученням технічних рішень). Тут ми спостерігаємо ускладнення через вплив зовнішнього природного середовища, яке є нестабільним і важко передбачуваним.

Незалежно від типу, складні системи характеризуються рядом фундаментальних ознак, які визначають їхню динаміку, стійкість, уразливість та потенціал розвитку:

Основні ознаки складних систем:

1. Нелінійність

Це одна з базових характеристик складних систем. Нелінійність означає, що вплив одного елемента на інший або на систему загалом не має прямо пропорційного характеру. У таких системах малі зміни в одному з компонентів можуть викликати диспропорційно великі зміни в загальній поведінці системи (ефект метелика). Це унеможливлює точне передбачення

наслідків втручання або змін і потребує застосування спеціалізованих моделей (нелінійної динаміки, теорії хаосу) для аналізу та управління.

2. Ієрархічність

Складна система зазвичай має багаторівневу структуру: її можна умовно розбити на підсистеми, кожна з яких у свою чергу також може бути складною. Така ієрархічна організація дозволяє системі зберігати функціональність навіть у разі збоїв в окремих частинах, а також ефективно адаптуватися до змін, використовуючи механізми делегування та автономії. Важливим є також те, що взаємодія між рівнями ієрархії може бути як вертикальною (зверху вниз чи знизу вгору), так і горизонтальною (між підсистемами одного рівня), що додатково ускладнює систему.

3. Інформаційна відкритість

Складні системи, як правило, не є замкнутими: вони функціонують у постійній взаємодії з зовнішнім середовищем. Це означає як можливість впливу середовища на систему (через зміни умов функціонування, появу загроз або можливостей), так і вплив самої системи на контекст (наприклад, зміна екологічного балансу, вплив на суспільні процеси). Інформаційна відкритість вимагає високого рівня чутливості до змін середовища, швидкої обробки зовнішніх сигналів, а також – механізмів зворотного зв’язку для відповідного реагування.

4. Адаптивність

Одна з ключових переваг складних систем – це їх здатність змінювати свою структуру, поведінкові моделі та пріоритети у відповідь на зовнішні виклики. Адаптивність базується на механізмах навчання, самоналаштування та самоорганізації, які особливо важливі в умовах невизначеності. У соціально-технічних системах адаптивність часто реалізується через зміну організаційної культури, внутрішніх регламентів або впровадження нових технологій. У технічних системах – через алгоритми машинного навчання, реконфігурацію мережевих маршрутів, автоматичне переналаштування обладнання тощо.

Таблиця 2.1

Класифікація складних систем за природою

Тип системи	Приклад	Основні ризики
Технічні	Енергомережі, авіаційні системи	Вихід з ладу, кібератаки
Соціально-технічні	Логістичні ланцюги, підприємства	Людський фактор, управлінські помилки
Природно-технічні	ГЕС, ЧАЕС, нафтопереробні заводи	Техногенні аварії, природні загрози

Таким чином, складні системи – це динамічні, багаторівневі утворення, які характеризуються високим ступенем взаємозалежності, мінливості та взаємодії з контекстом. Їх ефективне функціонування та безпечне існування

потребують спеціалізованих підходів до моделювання, аналізу, моніторингу та управління, що враховують як структурні, так і процесуальні аспекти їхнього існування. Системне мислення, міждисциплінарні стратегії та цифрові технології є ключовими інструментами сучасного фахівця при роботі зі складними системами.

2. Системна ідентифікація небезпек і вразливостей

Поняття системної ідентифікації

У сучасному світі, що характеризується високим ступенем взаємозалежності, цифровізації та динамізму, питання виявлення і управління ризиками набуває ключового значення для забезпечення функціональної стійкості як технічних, так і соціально-технічних систем. Системна ідентифікація небезпек виступає в цьому контексті як методологічно обґрунтований підхід до виявлення потенційних загроз і вразливостей, який базується не на інтуїції чи фрагментарному спостереженні, а на цілісному аналізі структури, процесів та взаємозв’язків у межах об'єкта дослідження.

Сутність системної ідентифікації небезпек

Під системною ідентифікацією небезпек розуміється процес глибокого й структурованого дослідження системи з метою виявлення джерел ризику, слабких ланок, конфліктних точок взаємодії та прихованих або латентних загроз. На відміну від традиційних методів, цей підхід не обмежується лише описом очевидних загроз, а прагне до виявлення системних дисфункцій, що можуть проявитися лише в певних умовах або за наявності складної взаємодії чинників.

Ключова особливість системної ідентифікації полягає в її міждисциплінарному характері. Сучасна практика вимагає залучення широкого спектру наукових підходів і технік, зокрема:

1) Системного аналізу – як методологічного каркасу для моделювання структури, ієрархії, потоків інформації та ресурсів.

2) Кібернетики – для аналізу зворотних зв’язків, регуляторних механізмів та стабільності функціонування.

3) Теорії графів – що дозволяє візуалізувати та кількісно оцінити мережеву топологію системи, виявити ключові вузли та критичні шляхи.

4) Теорії складності – для розуміння поведінки нелінійних, динамічних систем, які демонструють емерджентні властивості.

Таке інтегроване бачення дозволяє не тільки виявити існуючі загрози, а й змоделювати можливі сценарії їх розвитку, впливу на систему та механізми протидії.

Основні етапи системної ідентифікації небезпек

Процес системної ідентифікації небезпек, як правило, реалізується поетапно. Кожен етап має свою логіку, методологічне навантаження та завдання, які дозволяють послідовно перейти від загального аналізу до точкового виявлення ризиків.

1. Структурний аналіз системи

Цей етап передбачає виявлення елементного складу системи, аналіз її архітектури, внутрішніх зв'язків, потоків ресурсів (матеріальних, інформаційних, енергетичних) та логіки функціонування. За допомогою структурних схем, графів і матриць зв'язків відбувається побудова структурної моделі системи, яка виступає основою для подальшого аналізу.

На цьому етапі визначаються: Основні компоненти системи та їхні функції; Типи взаємозв'язків між компонентами (синхронні, асинхронні, жорстко або слабо пов'язані); Потенційні місця концентрації залежностей або надмірної складності (вузли з великою кількістю зв'язків, від яких залежить робота інших модулів).

Інструменти: структурно-функціональні діаграми, моделі IDEF0, UML-діаграми, графи зв'язків.

2. Оцінка контексту функціонування

Будь-яка система існує не у вакуумі, а в реальному контексті, що включає зовнішні чинники, здатні прямо чи опосередковано впливати на її стабільність. На цьому етапі здійснюється аналіз зовнішнього середовища, у якому функціонує система.

Основними напрямами контекстного аналізу є: Політичні фактори: зміни у законодавстві, регуляторна невизначеність, геополітична нестабільність. Економічні чинники: інфляція, коливання ринку, залежність від постачальників або енергетичних ресурсів. Природні фактори: кліматичні ризики, геологічні умови, природні катастрофи. Соціальні параметри: очікування користувачів, зміни в структурі попиту, поведінкові моделі персоналу.

Оцінка контексту дозволяє зв'язати внутрішні особливості системи із зовнішніми загрозами, сформувати карту можливих точок входу небезпек у систему.

Інструменти: PESTLE-аналіз, SWOT-аналіз, сценарне планування, метод Delphi.

3. Виявлення критичних елементів

Це один з найважливіших аналітичних етапів, метою якого є ідентифікація так званих «вузьких місць» або критичних точок у системі.

Такими елементами можуть бути: Вузли з високим навантаженням; Компоненти, вихід з ладу яких блокує інші частини системи; Елементи з низькою відмовостійкістю; Компоненти, для яких немає резервних або дублюючих рішень.

Оцінка критичних елементів часто супроводжується вивченням імовірності відмови та аналізом наслідків (наприклад, метод FMEA – Failure Modes and Effects Analysis), а також застосуванням мережевого аналізу для виявлення елементів із найвищим коефіцієнтом центральності в графі системи.

4. Оцінка сценаріїв розвитку подій

Останній етап передбачає побудову моделей розвитку подій у разі реалізації певних загроз або збоїв. Це дозволяє не лише передбачити можливі

наслідки, а й сформувати стратегії реагування, виявити резерви адаптивності системи.

На цьому етапі здійснюється:

1) Створення сценаріїв «що-якщо» (what-if);

2) Моделювання динаміки системи із застосуванням агентних, дискретно-подійних або системно-динамічних підходів;

3) Оцінка часу реакції, ступеня деградації функцій та ефективності протидії;

4) Визначення точок входу для впровадження контрзаходів або резервних стратегій.

Інструменти: системна динаміка (Vensim, AnyLogic), Monte Carlo моделювання, fault tree analysis (FTA), event tree analysis (ETA).

Таблиця 2.2

Порівняння традиційного та системного підходів до ідентифікації ризиків

Критерій	Традиційний підхід	Системний підхід
Фокус аналізу	Індивідуальні компоненти	Вся система в цілому
Врахування взаємодій	Обмежене	Комплексне
Оцінка впливу змін	Лінійна	Нелінійна
Інструменти	Чек-листи, експертне оцінювання	Моделювання, граф-аналіз

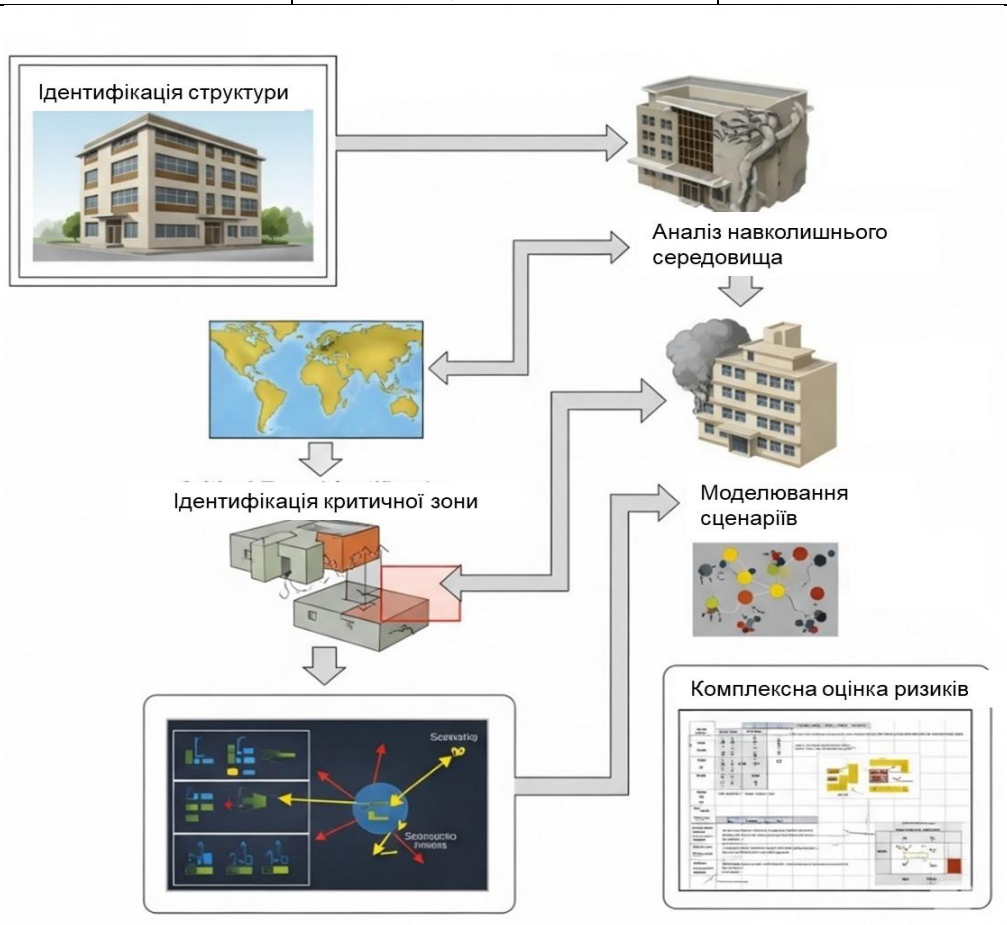

Рис. 2.1. Етапи системної ідентифікації ризиків

[Графічне зображення — блок-схема з п’ятьма етапами: ідентифікація структури → аналіз середовища → виявлення критичних зон → моделювання сценаріїв → інтегрована оцінка ризиків.]

Системна ідентифікація небезпек є необхідною умовою для побудови безпечних, надійних і адаптивних технічних або соціально-технічних систем. Завдяки міждисциплінарному підходу та багаторівневому аналізу, цей метод дозволяє не лише виявити поточні загрози, а й сформувати ґрунт для проактивного управління ризиками, адаптації системи до змін і розробки стійких архітектур.

3. Картування ризиків (Risk Mapping)

Картування ризиків (англ. *Risk Mapping*) є одним із ключових інструментів системного аналізу ризиків у технічних, інформаційних, екологічних, соціально-економічних та кіберфізичних системах. Воно передбачає візуалізацію розподілу ризиків у межах складної системи з метою кращого розуміння джерел загроз, уразливих компонентів, потенційних каналів впливу та ймовірних наслідків.

На відміну від суто описових або математичних моделей ризиків, картування забезпечує просторову, функціональну та контекстуальну інтерпретацію наявних і потенційних загроз. Це дозволяє приймати обґрунтовані рішення на основі візуальної логіки, де ризики стають "видимими" в системному полі, а не залишаються абстрактними показниками у таблицях чи звітах.

Основні цілі картування ризиків

1. Ідентифікація концентрації ризиків (кластерів загроз) Візуальне представлення дозволяє виявити області або компоненти системи, де спостерігається висока щільність ризиків, тобто так звані *гарячі зони*. Це можуть бути як фізичні об’єкти (наприклад, серверні центри, транспортні вузли, хімічні склади), так і функціональні елементи (наприклад, критично навантажені мережеві вузли або інформаційні шлюзи в кіберсистемі). Виявлення таких кластерів дозволяє сконцентрувати ресурси безпеки саме на тих ділянках, де потенційні збитки будуть найбільшими.

2. Визначення слабких місць системи (вразливостей) Через графічне зображення взаємозв’язків між загрозами та елементами системи можна виявити вузькі місця або *білі плями* – ті області, які є недостатньо захищеними або мають надто багато залежностей від інших підсистем. Зазвичай це компоненти, які виконують критичні функції, але мають обмежені резерви, слабку ізоляцію, застаріле обладнання чи низький рівень контролю.

3. Підтримка процесу ухвалення рішень щодо пріоритетів безпеки Картування слугує не лише аналітичним, а й комунікаційним інструментом, який полегшує сприйняття складної інформації керівниками, інженерами, фахівцями з безпеки та іншими зацікавленими сторонами. Воно дає змогу візуально оцінити взаємозв’язки, пріоритети та сценарії розвитку ризиків,

що, у свою чергу, полегшує розробку стратегічних планів, бюджетування та прийняття тактичних рішень.

Види карт ризиків

1. Просторові карти ризиків

Це найпоширеніший тип карт, який застосовується у фізичних системах (промислові об’єкти, транспорт, міська інфраструктура) та географічному контексті. На таких картах ризики позначаються на фізичній або цифровій топографії простору, з урахуванням локації потенційних джерел загроз. Наприклад, карта сейсмічних ризиків або розподіл кіберзагроз у глобальній комп’ютерній мережі. Цей тип карт дозволяє здійснювати геопросторовий аналіз, враховувати навколишнє середовище, кліматичні умови, доступність ресурсів та логістичні маршрути.

2. Функціональні карти ризиків

Цей тип відображає взаємозв’язки між функціональними модулями або процесами системи та ризиками, що на них впливають. Він є особливо корисним для аналізу складних технологічних, бізнесових або інформаційних систем, де ключове значення мають саме взаємодії, а не географічне розташування. Наприклад, карта, яка показує, як ризик кіберзлому впливає на функцію управління логістикою, фінансовий облік або зв’язок з партнерами. Такі карти допомагають виявити ланцюгові реакції загроз, де відмова одного модуля призводить до каскадних наслідків у суміжних елементах системи.

3. Інтегровані карти ризиків

Ці карти об'єднують просторові, функціональні та часові аспекти ризиків, створюючи багатовимірну структуру. Такий підхід застосовується для динамічного моделювання сценаріїв розвитку ризиків у просторі й часі. Інтегровані карти дозволяють відслідковувати, як ризики змінюються залежно від сезонів, змін зовнішніх умов, технічного стану об’єктів або з урахуванням людського фактору. Наприклад, на інтегрованій карті можна одночасно відобразити: зони впливу повені (просторовий вимір), вплив на функції водопостачання, енергопостачання (функціональний вимір), динаміку розвитку подій протягом 24 годин (часовий вимір).

Значення картування ризиків у сучасному управлінні безпекою

У сучасних умовах постійно зростаючої складності технічних і соціотехнічних систем, картування ризиків набуває стратегічного значення. Завдяки візуалізації можливо: здійснювати проактивне управління ризиками, передбачаючи їхню появу; забезпечити прозорість процесів прийняття рішень для всіх стейкхолдерів; інтегрувати методи інтелектуального аналізу даних, включаючи машинне навчання та штучний інтелект для автоматичного оновлення карт у реальному часі; створити цифрові двійники систем безпеки, які інтерактивно моделюють поведінку ризиків і допомагають тестувати сценарії реагування.

Таблиця 2.3

Приклад функціонального картування ризиків для енергетичної системи

Функція системи	Потенційні ризики	Критичність	Імовірність	Рівень ризику
Генерація	Вихід з ладу турбіни	Висока	Середня	Високий
Передача	Пошкодження ЛЕП	Висока	Висока	Дуже високий
Розподіл	Аварія на підстанції	Середня	Низька	Середній
Контроль	Збій SCADA-системи	Висока	Середня	Високий

Рис.2.2. Матриця ризиків (Risk Heat Map)

[Графічне зображення – матриця 5х5, де по горизонталі – ймовірність (від «дуже низька» до «дуже висока»), по вертикалі – Вплив (від «незначного» до «катастрофічного»). Клітини заповнені кольорами: зелений (низький ризик), жовтий (середній), червоний (високий).]

Системно орієнтовані методи дозволяють глибше зрозуміти природу ризиків у складних об’єктах, особливо з урахуванням нелінійної динаміки та високої взаємозалежності компонентів. Системна ідентифікація небезпек та методи картування ризиків виступають ефективним інструментарієм у стратегічному управлінні безпекою та формуванні адаптивних механізмів захисту. Інтеграція візуалізаційних засобів (heat maps, граф-структур, діаграм ризиків) значно підвищує ефективність аналітичного процесу та сприяє ухваленню обґрунтованих управлінських рішень.

2.2. Мультикритеріальні методи оцінювання ризиків

Мультикритеріальні методи оцінювання ризиків (МКМОР) використовуються для врахування кількох суперечливих критеріїв при прийнятті рішень у складних системах із високим рівнем невизначеності. Ці методи дозволяють оцінити альтернативи за сукупністю параметрів, що мають різну вагомість, та обрати найоптимальніше рішення з урахуванням системного підходу.

Метод аналізу ієрархій (AHP)

Метод аналізу ієрархій (англ. *Analytic Hierarchy Process, AHP*), розроблений американським вченим Томасом Сааті у 1970-х роках, є одним із найпотужніших інструментів багатокритеріального прийняття рішень. Його сутність полягає у структуризації складної проблеми у вигляді ієрархії та подальшому кількісному порівнянні пріоритетів через експертну оцінку парних співвідношень між елементами.

Цей метод широко використовується в галузях стратегічного планування, інженерного проєктування, управління ризиками, логістики, оборонного аналізу, медицини, кібербезпеки та державного управління. Його універсальність дозволяє адаптувати AHP як до кількісних, так і до якісних критеріїв, що робить його незамінним у складних, слабо формалізованих умовах.

Основна ідея методу

У методі AHP складна задача розбивається на менші, взаємопов’язані компоненти, які організовуються в ієрархічну структуру. Це дозволяє послідовно проаналізувати всі рівні впливу: від стратегічної мети до конкретних альтернатив, при цьому враховуючи як об’єктивні дані, так і експертні судження. Важливим аспектом AHP є використання шкали Сааті, що перетворює суб’єктивні оцінки на числові значення з можливістю подальшого агрегування.

Етапи реалізації AHP

1. Формування ієрархії: від мети до альтернатив

На цьому етапі відбувається декомпозиція проблеми у вигляді багаторівневої структури:

1) Перший рівень (мета) – загальна ціль аналізу (наприклад, вибір найефективнішої стратегії зниження ризику).

2) Другий рівень (критерії) – основні фактори, що впливають на досягнення мети (вартість, надійність, час реалізації, екологічність тощо).

3) Третій рівень (субкритерії, за потреби) – деталізація критеріїв.

4) Четвертий рівень (альтернативи) – можливі варіанти рішень або дій (наприклад, впровадження технічного засобу, зміна організаційної моделі, використання зовнішнього аудиту).

Ієрархія забезпечує прозорість структури проблеми, що є критично важливим у ситуаціях з високим рівнем складності або невизначеності, наприклад, при аналізі техногенних ризиків чи оцінці кіберзагроз.

2. Попарне порівняння критеріїв та альтернатив за шкалою Сааті

На цьому етапі експерти проводять парні порівняння елементів одного рівня відносно кожного елементу вищого рівня. Порівняння здійснюється за дев'ятибальною шкалою Сааті, яка відображає ступінь переваги одного елемента над іншим:

Таблиця 2.4

Шкала Сааті для попарного порівняння

Оцінка	**Значення**	**Інтерпретація**
1	Рівнозначно	Елементи однаково важливі
3	Помірна перевага	Один елемент трохи важливіший
5	Сильна перевага	Явна перевага одного елемента
7	Дуже сильна	Один значно важливіший
9	Абсолютна перевага	Один безумовно переважає
2,4,6,8	Проміжні значення	Для уточнення між основними балами

Результати таких порівнянь фіксуються у матрицях парних порівнянь, які слугують основою для розрахунку ваг.

3. Обчислення ваг критеріїв та альтернатив

З матриці парних порівнянь обчислюються власні вектори пріоритетів, які й відображають відносні ваги елементів. Найпоширенішим методом є нормалізація стовпців та обчислення середнього значення по рядках, хоча для точнішого результату використовується розв'язання задачі на власні вектори.

На цьому етапі також розраховується коефіцієнт узгодженості (Consistency Ratio, CR), який показує, наскільки логічно узгоджені експертні оцінки. Якщо CR перевищує 0.1, необхідно переглянути порівняння.

4. Узагальнення результатів і вибір альтернативи

Останній етап полягає в агрегуванні ваг критеріїв і відповідних альтернатив для отримання глобального пріоритету кожної альтернативи. Альтернатива з найвищим пріоритетом вважається найоптимальнішою з урахуванням заданої мети та структури критеріїв.

Цей процес забезпечує прозоре, аргументоване та обґрунтоване прийняття рішення навіть в умовах неповної інформації або при наявності конфліктних цілей.

AHP у контексті системного аналізу ризиків

Метод AHP виявляється особливо ефективним у сфері управління ризиками технічних систем, де необхідно: узгодити різноспрямовані фактори (технічні, економічні, людські); обґрунтувати вибір контрзаходів або стратегій реагування; системно підходити до проблеми, яка не має єдиного правильного рішення.

У цьому контексті AHP дозволяє:

1) формалізувати оцінку ризиків за низкою критеріїв;

2) врахувати експертну думку в умовах дефіциту статистичних даних;

3) забезпечити трасованість прийняття рішення (зрозуміло, як отриманий результат);

4) реалізувати гнучкий інструмент аналізу сценаріїв із подальшою адаптацією до нових умов.

Приклад застосування

У рамках оцінки ризику аварій на об’єктах критичної інфраструктури (наприклад, електростанція), ієрархія може мати такий вигляд:

1) Мета: Вибір найбільш ефективного заходу для зменшення техногенного ризику.

2) Критерії: Ефективність зниження ризику, економічні витрати, час впровадження, вплив на навколишнє середовище.

3) Альтернативи: Встановлення автоматичної системи моніторингу, модернізація обладнання, впровадження додаткових протоколів безпеки.

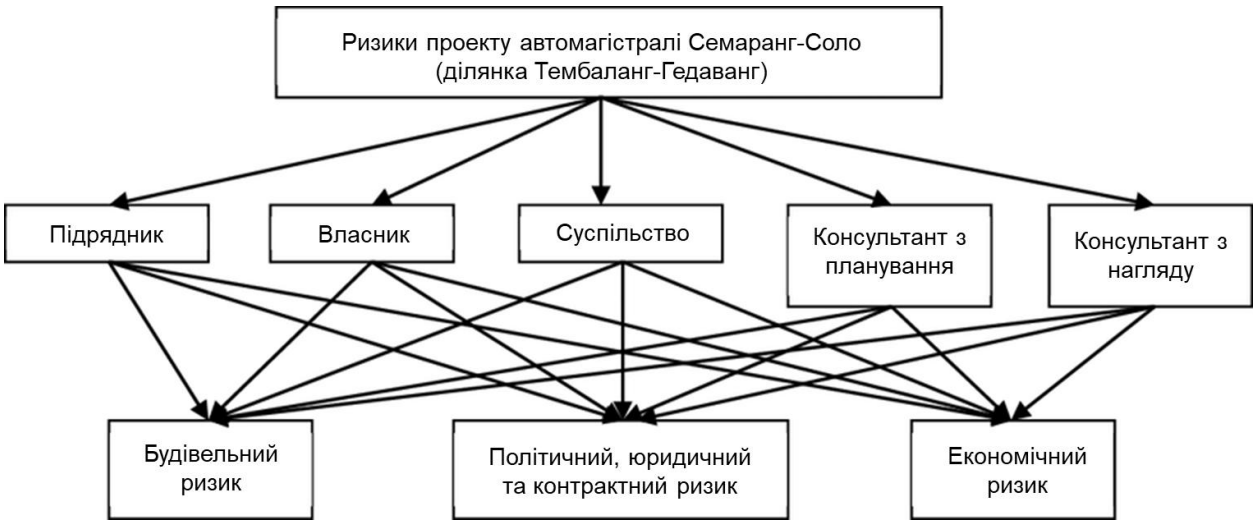

Рис. 2.3. Приклад ієрархічної структури ризику в інфраструктурному проєкті

Метод TOPSIS

Метод подібності до ідеального рішення (TOPSIS) (англ. *Technique for Order Preference by Similarity to Ideal Solution*) є одним із найпоширеніших методів багатокритеріального прийняття рішень.

Його основна ідея полягає у виборі такої альтернативи, яка одночасно є найближчою до умовно найкращого (ідеального) рішення та найдальшою від умовно найгіршого (антиідеального) рішення. TOPSIS заснований на простій, але ефективній логіці: найкраще рішення повинно бути якнайближче до позитивного ідеалу та якнайдалі від негативного ідеалу.

Основні етапи реалізації методу TOPSIS

1. Побудова матриці рішень

На першому етапі формується матриця, що відображає оцінки всіх альтернатив за кожним критерієм.

Позначимо матрицю рішень як $\boldsymbol{X = [x_{ij}]}$, де:

x_{ij} – значення критерію **j** для альтернативи **i**;

$i = 1, 2, ..., m$ – кількість альтернатив;

$j = 1, 2, ..., n$ – кількість критеріїв.

Кожен рядок у матриці відповідає окремій альтернативі, а кожен стовпчик — конкретному критерію, який використовується для оцінки.

Наприклад, якщо потрібно оцінити 4 технічні системи за 3 критеріями ефективності, вартості й надійності, то матриця рішень буде розміром 4×3.

2. Нормалізація значень

Оскільки критерії можуть мати різні одиниці вимірювання (наприклад, гривні, години, відсотки), їх слід привести до уніфікованого масштабу. Найчастіше застосовується **векторна нормалізація**, за формулою:

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}}$$

Цей етап дозволяє уникнути домінування будь-якого критерію в процесі аналізу через великі числові значення.

3. Зважування критеріїв

Оскільки не всі критерії мають однакову важливість, до кожного з них застосовують ваговий коефіцієнт $\mathbf{w_j}$, який може бути визначений експертним шляхом або за допомогою формалізованих методів (наприклад, метод аналізу ієрархій AHP, метод ентропії тощо).

Після визначення ваг розраховується зважена нормалізована матриця:

$$v_{ij} = w_j \cdot r_{ij}$$

Це дає змогу врахувати реальний внесок кожного критерію у загальну оцінку альтернатив.

4. Обчислення відстаней до ідеального та антиідеального рішення

На цьому етапі визначаються:

1) Позитивне ідеальне рішення (PIS) – набір найкращих можливих значень критеріїв;

2) Негативне ідеальне рішення (NIS) – набір найгірших можливих значень.

$$S_i^+ = \sqrt{\sum_{j=1}^{n}(v_{ij} - A_j^+)^2}$$

$$S_i^- = \sqrt{\sum_{j=1}^{n}(v_{ij} - A_j^-)^2}$$

Для кожної альтернативи обчислюється евклідова відстань до ідеального та антиідеального рішеня.

Ці ідстані дозволяють оцінити, наскільки близькою або далекою є конкретна альтернатива від уявних ідеалів.

5. Обчислення індексу близькості

Індекс близькості дозволяє отримати агреговану оцінку кожної альтернативи. Формула:n

$$C_i = \frac{S_i^-}{S_i^+ + S_i^-}$$

де: $\mathbf{C_i}$ – індекс близькості альтернативи **i** до ідеального рішення ($0 \le C_i \le 1$).

Чим ближче значення $\mathbf{C_i}$ до 1, тим кращою є альтернатива з погляду компромісного рішення. У підсумку альтернативи впорядковуються за спаданням $\mathbf{C_i}$, і вибирається та, що має найбільший індекс.

Переваги методу TOPSIS

1) Інтуїтивна логіка, що базується на концепціях відстані до ідеалу.
2) Простота реалізації й можливість автоматизації.
3) Гнучкість у врахуванні різних типів критеріїв: вигоди, витрати тощо.
4) Придатність до широкого кола задач – від технічної експертизи до стратегічного планування.

Метод TOPSIS є потужним інструментом у сфері аналізу складних альтернатив, що дозволяє формалізувати процес прийняття рішень за допомогою математичних підходів. Його адаптивність до різних предметних галузей робить його актуальним у сфері управління ризиками, стратегічного аналізу, оцінки проектів, технічного аудиту та інших дисциплін.

Таблиця 2.5

Результати нормалізованої матриці TOPSIS

Альтернатива	C1	C2	C3	...	Індекс близькості
A	0,5	0,7	0,6	...	0,82
B	0,3	0,9	0,5	...	0,75
C	0,8	0,6	0,7	...	0,91

Просторове відображення альтернатив у TOPSIS

Ось візуалізація позиції альтернатив, а також ідеального (A+) та антиідеального (A−) рішень у методі TOPSIS. Це допомагає наочно оцінити, наскільки кожна альтернатива близька до ідеалу та далека від найгіршого варіанта.

Python

```
import matplotlib.pyplot as plt
import numpy as np

# --- Приклад даних (замініть на ваші власні результати TOPSIS) ---
# D_plus: відстані до ідеального рішення для кожної альтернативи
D_plus = np.array([0.15, 0.25, 0.08, 0.30, 0.12, 0.18, 0.22, 0.05])
# D_minus: відстані до антиідеального рішення для кожної альтернативи
D_minus = np.array([0.80, 0.65, 0.92, 0.55, 0.88, 0.70, 0.60, 0.95])
# Назви альтернатив
alternatives = ['A1', 'A2', 'A3', 'A4', 'A5', 'A6', 'A7', 'A8']

# --- Обчислення координат для ідеального та антиідеального рішень для
візуалізації ---
# Ідеальне рішення (A+): мінімальна відстань до себе (D_plus = 0) і
максимальна до антиідеального.
# Для візуалізації ми розміщуємо A+ трохи вище максимального D_minus
ideal_D_plus = 0.0
ideal_D_minus = D_minus.max() * 1.05 # Додаємо невеликий відступ для кращої
візуалізації

# Антиідеальне рішення (A-): максимальна відстань до ідеального і мінімальна
відстань до себе (D_minus = 0).
# Для візуалізації ми розміщуємо A- трохи правіше максимального D_plus
anti_ideal_D_plus = D_plus.max() * 1.05 # Додаємо невеликий відступ
anti_ideal_D_minus = 0.0

# --- Створення Графіка 2 ---
plt.figure(figsize=(10, 8))

# Відображення альтернатив як точок
plt.scatter(D_plus, D_minus, s=150, zorder=5, label='Альтернативи',
alpha=0.8, edgecolors='w', linewidth=0.8)

# Додавання назв до точок альтернатив
for i, txt in enumerate(alternatives):
    plt.annotate(txt, (D_plus[i], D_minus[i]), textcoords="offset points",
xytext=(0,10), ha='center', fontsize=9, weight='bold')

# Відображення ідеального рішення (A+)
plt.scatter(ideal_D_plus, ideal_D_minus, s=300, marker='*', color='green',
label='Ідеальне рішення ($A^+$)', zorder=10)
plt.annotate('$A^+$', (ideal_D_plus, ideal_D_minus), textcoords="offset
points", xytext=(0,15), ha='center', color='green', fontsize=14,
fontweight='bold')

# Відображення антиідеального рішення (A-)
plt.scatter(anti_ideal_D_plus, anti_ideal_D_minus, s=300, marker='X',
color='red', label='Антиідеальне рішення ($A^-$)', zorder=10)
plt.annotate('$A^-$', (anti_ideal_D_plus, anti_ideal_D_minus),
textcoords="offset points", xytext=(0,15), ha='center', color='red',
fontsize=14, fontweight='bold')
# Налаштування осей та заголовка
plt.xlabel('Відстань до ідеального рішення ($D^+$)', fontsize=12,
weight='bold')
```

```
plt.ylabel('Відстань до антиідеального рішення ($D^-$)', fontsize=12,
weight='bold')
plt.title('Просторове відображення альтернатив у TOPSIS', fontsize=16,
weight='bold')
plt.grid(True, linestyle='--', alpha=0.6)

# Додавання легенди
plt.legend(fontsize=10, loc='lower left')

# Обмеження осей для кращої візуалізації (з невеликим запасом)
plt.xlim(min(0, D_plus.min() * 0.9), max(anti_ideal_D_plus * 1.1,
D_plus.max() * 1.1))
plt.ylim(min(0, D_minus.min() * 0.9), max(ideal_D_minus * 1.1, D_minus.max()
* 1.1))

# Показати графік
plt.tight_layout()
plt.show()
```

Метод ELECTRE

ELECTRE (ELimination Et Choice Translating REality) – це один із ключових методів багатокритеріального прийняття рішень, розроблений у Франції в 1960-х роках. Назва перекладається як «Елімінація та вибір, що відображає реальність», що добре ілюструє його головну ідею: використання парних порівнянь між альтернативами для поступового відсівання слабших варіантів, які не відповідають заданим критеріям або порогам.

На відміну від методів ранжування на основі агрегованих оцінок (наприклад, TOPSIS чи AHP), ELECTRE ґрунтується на відношенні переваги – він не намагається знайти одну «найкращу» альтернативу, а будує множину рішень, які не поступаються іншим у більшості критеріїв.

Основні етапи реалізації методу ELECTRE

1. Побудова матриці переваг (concordance matrix)

На цьому етапі будується матриця порівнянь альтернатив між собою за всіма критеріями. Для кожної пари альтернатив (A, B) оцінюється, наскільки сильними є підстави вважати A кращою за B.

Для цього визначається множина погодження (concordance set), яка включає всі ті критерії, за якими альтернатива A є не гіршою за B. Потім розраховується індекс узгодженості – відношення суми ваг критеріїв, за якими A переважає B, до загальної суми всіх ваг.

Таким чином формується матриця узгодження, яка відображає відносні переваги альтернатив одна над одною з урахуванням ваг критеріїв.

2. Обрахунок суперечності (discordance) та побудова порогів

Паралельно з узгодженістю розраховується індекс суперечності (discordance index) – він показує, наскільки сильно одна альтернатива поступається іншій за будь-яким критерієм. Якщо така суперечність є надто великою (тобто перевищує певний допустимий поріг), то альтернатива не може вважатися кращою в парному порівнянні.

Таким чином, враховується не лише перевага в більшості критеріїв, а й відсутність критичних відставань.

3. Формування надійного підмножини альтернатив (kernel set)

Після аналізу парних переваг та встановлення домінування формується так звана ядерна множина (kernel) – підмножина альтернатив, які не домінуються жодною іншою альтернативою згідно з введеними порогами.

Ця множина є результатом фільтрації: слабші альтернативи поступово «елімінуються» з аналізу, оскільки вони мають недостатній рівень узгодженості або перевищують пороги суперечності.

У деяких варіантах методології ELECTRE може бути застосовано багаторівневе фільтрування, тобто формування кількох рівнів пріоритетності або ранжування альтернатив на групи.

Переваги методу ELECTRE

1) Гнучкість у прийнятті складних рішень: ELECTRE не потребує повного ранжування всіх альтернатив, а дозволяє працювати з множинами допустимих рішень – що особливо цінно при нечітких або конфліктних критеріях.

2) Ефективність при великій кількості альтернатив і критеріїв: завдяки парному порівнянню метод зберігає високу точність навіть у багатовимірному просторі рішень.

3) Можливість врахування порогових значень (cut-off thresholds): це дозволяє моделювати реальні ситуації, де певні рівні відмінностей не вважаються значущими, тобто впроваджується принцип «нечутливості» до незначних варіацій.

Застосування ELECTRE

Метод ELECTRE широко застосовується в таких сферах, як: екологічне планування (оцінка впливу альтернатив на довкілля), управління проектами, вибір технічного обладнання, транспортне планування, енергетичні дослідження, стратегічне управління в умовах невизначеності.

Метод ELECTRE є потужним інструментом багатокритеріального аналізу, особливо корисним у ситуаціях, коли оцінювання альтернатив є суперечливим, а точне ранжування складним або навіть неможливим. Його здатність враховувати не лише переваги, але й конфлікти, порогові рівні та нечіткість у даних робить його актуальним для сучасних задач, пов’язаних з прийняттям складних управлінських або інженерних рішень.

Таблиця 2.6

Приклад матриці узгодженості (concordance matrix)

	A	B	C
A	–	0,7	0,5
B	0,3	–	0,8
C	0,5	0,2	–

Інтеграція суб’єктивних і об’єктивних оцінок

У сучасному аналізі складних систем і процесів часто виникає необхідність приймати рішення за умов невизначеності, обмеженої інформації або недостатньої формалізації знань. У таких ситуаціях важливо

поєднувати суб’єктивні оцінки експертів (що ґрунтуються на досвіді, інтуїції, професійному баченні) з об’єктивними даними, отриманими з емпіричних, статистичних або технологічних джерел. Такий підхід забезпечує більш повну, гнучку і стійку систему підтримки прийняття рішень.

Суть інтеграції суб’єктивних та об’єктивних даних

Інтеграція полягає у системному поєднанні кількісних (об’єктивних) і якісних (суб’єктивних) оцінок для формування комплексного критерію, що враховує як формалізовані метрики (час, вартість, ризик), так і нефіналізовані параметри (довіра, безпека, політична доцільність, стратегічна значущість).

Це особливо важливо в таких сферах, як управління ризиками, прогнозування подій або загроз, безпека технічних систем, оборонне планування, стратегічний аналіз і політика.

Ключові методи інтеграції оцінок

1. Баєсівські мережі впевненості (Bayesian Belief Networks, BBNs)

Баєсівські мережі – це графові моделі, які дозволяють моделювати причинно-наслідкові зв’язки між подіями та змінними в умовах невизначеності. Кожна вершина (вузол) у мережі представляє змінну, а ребра – ймовірнісні залежності.

Особливості:

1) Можна поєднувати об’єктивні статистичні дані (наприклад, частоти настання подій) з експертними оцінками ймовірностей.

2) Дає можливість оновлювати оцінки на основі нових даних за допомогою Баєсівського виводу.

3) Надзвичайно ефективна для оцінки ризиків, діагностики системних відмов, прогнозування подій.

Переваги:

1) Побудова динамічної моделі знань з урахуванням неповноти.

2) Можливість візуального представлення складних залежностей.

3) Інтеграція «м’якої» (експертної) інформації з «твердими» фактами.

2. Метод згортки (aggregation)

Метод згортки – це математична або евристична процедура об'єднання множини оцінок в єдиний узагальнений показник, що використовується для ранжування або вибору альтернатив.

Варіанти реалізації:

1) Лінійна згортка з використанням вагових коефіцієнтів.

2) Нелінійна згортка, що враховує неадитивні взаємозв’язки між критеріями.

3) Ієрархічна згортка, коли агрегування відбувається на різних рівнях (наприклад, спочатку для підкритеріїв, потім – для загальних критеріїв).

Метод дозволяє:

1) Об’єднувати експертні оцінки (ваги) з емпіричними даними (значення критеріїв).

2) Здійснювати чітке ранжування альтернатив.

3) Варіювати ступінь суб’єктивності через зміну ваг.

3. Fuzzy AHP і Fuzzy TOPSIS

Ці методи поєднують нечітку логіку (fuzzy logic) з класичними процедурами багатокритеріального аналізу, що дозволяє моделювати невизначеність, розпливчастість або лінгвістичні оцінки, характерні для суб'єктивних суджень.

Fuzzy AHP (Analytic Hierarchy Process): Побудова ієрархічної структури критеріїв. Параметри оцінюються експертами за допомогою нечітких чисел (наприклад, трикутних або трапецеїдальних). Визначаються нечіткі ваги кожного критерію. Забезпечується врахування експертної невизначеності без втрати математичної строгості.

Fuzzy TOPSIS: Альтернативи оцінюються за критеріями, де значення є нечіткими величинами. Визначаються ідеальні та антиідеальні рішення в нечіткому просторі. Обчислюються відстані альтернатив до цих еталонів з урахуванням нечіткої природи оцінок.

Переваги:

1) Висока адаптивність до мовних оцінок (наприклад, «високий ризик», «помірна загроза»).

2) Підвищення стійкості результатів до експертної розбіжності.

3) Застосування в умовах нечіткої, фрагментарної або лінгвістичної інформації.

Переваги комплексного підходу

Інтеграція суб'єктивних і об'єктивних оцінок дозволяє досягти , а саме: Більшої точності та гнучкості в умовах невизначеності; Можливості моделювання людських суджень у формалізованих системах підтримки рішень; Врахування як раціонального, так і евристичного аспекту вибору; Підвищення довіри до рішень завдяки залученню експертів до формування моделі.

Таблиця 2.7

Порівняння методів інтеграції оцінок

Метод	Точність	Гнучкість	Придатність до системного аналізу
Баєсівська мережа	Висока	Середня	Висока
Fuzzy AHP	Висока	Висока	Висока
Метод згортки	Середня	Висока	Середня

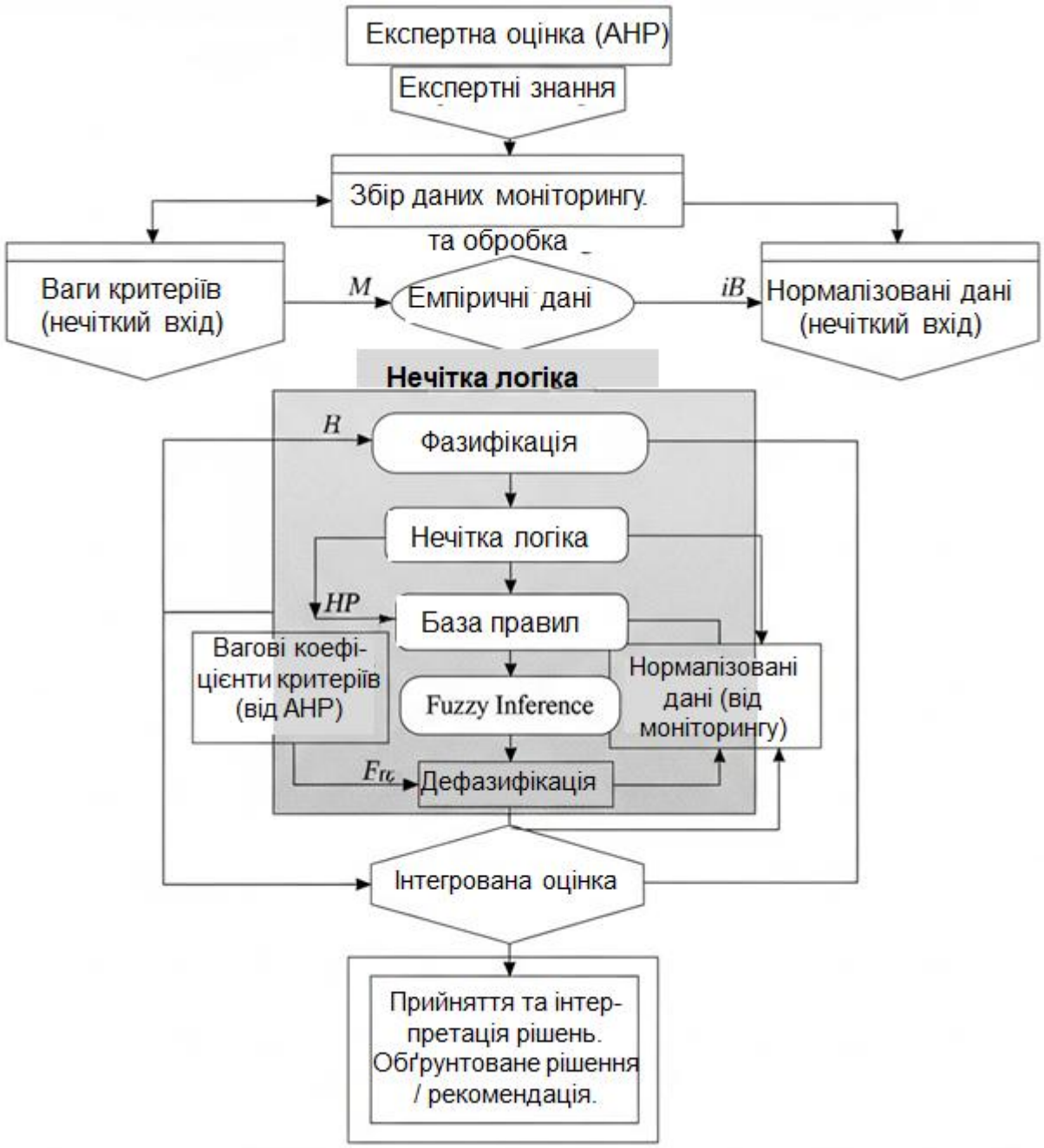

Рис. 2.4. Схема інтеграції експертної оцінки та даних моніторингу
(Об’єднання результатів AHP з емпіричними даними
у структурі нечіткої логіки)

Інтеграція суб’єктивних (експертних) та об’єктивних (статистичних, емпіричних) оцінок – це стратегічно важливий напрям у сучасних системах підтримки прийняття рішень. Її ефективне впровадження дозволяє не лише компенсувати брак даних, а й адаптувати рішення до складних соціотехнічних середовищ, де повна інформація недоступна або дорого коштує. Методи на кшталт Баєсівських мереж, згортки та нечітких MCDM-моделей (Fuzzy AHP, Fuzzy TOPSIS) створюють основу для інтелектуальних гібридних систем, що поєднують аналітичну строгість з людською інтуїцією.

Експертні оцінки з урахуванням системної взаємодії

У системному аналізі безпеки технічних систем ключову роль відіграє не лише ідентифікація та оцінювання ризиків за ступенем їхньої небезпеки, а й глибоке розуміння взаємозв'язків між елементами системи. Сучасні технічні системи є багатокомпонентними, динамічними утвореннями з нелінійною структурою, в якій зміни в одному елементі можуть спричиняти ланцюгові реакції або каскадні ефекти. Такий характер взаємодій вимагає врахування не тільки ймовірнісної природи загроз, а й здатності елементів системи реагувати на зовнішні й внутрішні збурення, передавати впливи та генерувати нові ризикові сценарії.

Важливою складовою системного підходу є поєднання якісного аналізу (експертного судження) з кількісним моделюванням. Експертні оцінки, що базуються на знаннях та досвіді фахівців у галузі технічної безпеки, значно збагачуються, коли вони враховують не лише окремі загрози, а й причинно-наслідкові зв'язки між ними. Саме цей підхід створює передумови для побудови когнітивних моделей – концептуальних схем, що відображають впливи одних компонентів на інші, враховуючи прямі, зворотні та латентні зв'язки в межах системи. Когнітивні моделі дозволяють візуалізувати складні процеси, прогнозувати можливі ризики на основі моделювання поведінки системи в умовах зміни параметрів і розробляти ефективні управлінські рішення.

Основні методи:

Когнітивне моделювання ризиків

Когнітивне моделювання – це метод побудови структурно-функціональних моделей складних систем, у яких важко чітко виокремити формалізовані зв'язки. У контексті аналізу ризиків це означає побудову когнітивної карти (графа), де вузли представляють ключові фактори ризику (технічні збої, людські помилки, зовнішні загрози тощо), а ребра – взаємозв'язки між ними, що мають певну силу та напрямок впливу (позитивний або негативний). Когнітивна модель дозволяє проводити сценарний аналіз впливу одного або кількох факторів на інші, виявляти критичні компоненти, які генерують найбільше негативних наслідків, а також вивчати ефекти посилення або компенсації впливів у системі.

Ключова перевага когнітивного моделювання полягає в його здатності працювати з неповними або нечіткими даними, що типово для реальних ситуацій, де повна інформація про всі ризики часто відсутня. Такий підхід широко використовується у безпекових дослідженнях, кризовому менеджменті, стратегічному плануванні та аналізі складних соціотехнічних систем.

Метод DELPHI з урахуванням зворотних впливів

Метод DELPHI – це багатоетапна процедура анонімного опитування групи експертів з метою досягнення консенсусу у складних або невизначених ситуаціях. Традиційний підхід передбачає поступове уточнення оцінок шляхом обробки результатів кількох раундів опитування, надання експертам зведених відповідей попереднього раунду та повторної оцінки.

Удосконалений варіант цього методу, що застосовується у системному аналізі ризиків, передбачає включення механізму зворотного впливу, коли враховується не лише прямий вплив ризикових факторів, а й можливість зворотної реакції системи на ці впливи. Наприклад, підвищення ризику в одному компоненті може спричинити підсилення активності в інших частинах системи, які своєю чергою здатні послабити або нейтралізувати початкову загрозу. У цьому сенсі DELPHI виступає не лише як метод отримання зваженої думки, а як засіб моделювання багатофакторної взаємодії в умовах невизначеності.

Залучення механізму зворотних зв'язків суттєво підвищує точність та адекватність експертних моделей, дозволяючи враховувати адаптивність, саморегуляцію або деструктивну резонансну поведінку технічних систем.

Морфологічний аналіз сценаріїв

Морфологічний аналіз – це метод формального структурного дослідження проблеми шляхом побудови морфологічної матриці, що відображає всі можливі комбінації параметрів, які впливають на функціонування системи. Він ґрунтується на логічному комбінуванні варіантів розвитку подій, що дозволяє сформувати простір можливих сценаріїв майбутнього.

У сфері аналізу технічних ризиків морфологічний аналіз використовується для формування сценаріїв розвитку ситуацій з урахуванням множини чинників: технічних характеристик, організаційних рішень, людського чинника, нормативних обмежень тощо. У ході аналізу визначаються ключові параметри (наприклад, рівень навантаження, режим експлуатації, тип зовнішніх впливів) і варіанти їхніх значень. Комбінування цих варіантів дозволяє виявити як бажані (оптимальні), так і критичні сценарії, які слід враховувати при побудові систем захисту.

Морфологічний підхід особливо цінний на етапі попереднього проектування або оцінювання альтернатив, коли потрібно розглянути широкий спектр гіпотетичних варіантів і обґрунтувати вибір найбільш стійкої конфігурації системи.

Узагальнюючи, зазначені методи не лише доповнюють один одного, а й створюють потужний інструментарій для глибокого системного аналізу ризиків, побудови наочних моделей взаємодій і формування сценарного простору для прийняття оптимальних управлінських рішень у сфері технічної безпеки. Їх застосування значно підвищує якість прогнозування, дозволяє виявляти приховані зв'язки між елементами системи, а також адаптувати стратегії захисту до змін у зовнішньому середовищі.

Якщо потрібно, я можу також доповнити цей текст прикладом побудови когнітивної моделі або морфологічної таблиці для конкретної технічної системи.

Мультикритеріальні методи дають змогу системно підходити до оцінювання ризиків, інтегруючи різні типи інформації, що особливо важливо у високотехнологічних, динамічних сферах діяльності

Рис. 2.5. Когнітивна карта взаємозв’язку ризиків у технічній системі (Узагальнення причинно-наслідкових зв’язків між ризиками: R1 → R2 → R3)

Таблиця 2.8

Матриця взаємозв’язків між ризиками

	R1	R2	R3
R1	–	1	0
R2	0	–	1
R3	1	0	–

Комбінація AHP, TOPSIS, ELECTRE, когнітивного моделювання та інтеграції експертних оцінок дозволяє забезпечити комплексну оцінку ризиків навіть у найскладніших об’єктах. Надалі ці методи можуть бути поєднані з машинним навчанням та штучним інтелектом для автоматизації аналізу ризиків.

2.3. Невизначеність у системах та аналіз чутливості

У складних соціотехнічних, техногенних та інформаційних системах невизначеність є інтегральною характеристикою, що суттєво впливає на процеси прийняття рішень. У контексті системного аналізу й прогнозування ризиків, ефективна обробка невизначеності дозволяє підвищити точність оцінювання ризиків та ідентифікацію потенційних загроз. У цьому підрозділі розглядаються ключові підходи до моделювання невизначеності, зокрема: нечітка логіка та теорія нечітких множин, аналіз сценаріїв, інтервальний підхід і байєсівські мережі.

1. Моделі нечіткої логіки та нечіткі множини

Нечітка логіка (fuzzy logic), розроблена американським математиком азербайджанського походження Лотфі Заде у 1965 році, є потужним математичним апаратом, що дозволяє працювати з невизначеністю та неточністю, які часто присутні в реальних системах. На відміну від класичної булевої логіки, де твердження можуть бути лише "істинними" (1) або "хибними" (0), нечітка логіка вводить поняття ступеня істинності, що варіюється в діапазоні від 0 до 1. Це дозволяє моделювати нечіткі, неточні або неповні дані, які не можуть бути адекватно описані бінарними значеннями.

Основна ідея нечіткої логіки полягає у використанні нечітких множин. У класичній теорії множин, елемент або належить до множини, або ні. Наприклад, людина або «висока», або «не висока». У нечіткій логіці елемент може належати до множини з певним ступенем.

Наприклад, людина може бути «трохи високою», «досить високою» або «дуже високою». Цей ступінь належності вимірюється функцією належності, яка присвоює кожному елементу універсальної множини значення від 0 до 1, що відображає його ступінь належності до нечіткої множини.

Наприклад, якщо ми маємо нечітку множину «температура гаряча», температура 30°C може мати ступінь належності 0.2, тоді як температура 80°C може мати ступінь належності 0.9.

Ця можливість працювати з частковою істинністю робить нечітку логіку надзвичайно гнучкою та дозволяє їй ефективно обробляти лінгвістичні змінні (наприклад, «низький», «середній», «високий»), які є природними для людського мислення, але складними для формалізації в класичній логіці.

Застосування нечіткої логіки в аналізі ризиків

Нечітка логіка та нечіткі множини є незамінним інструментом для аналізу ризиків, особливо коли мова йде про оцінку якісних факторів ризику, які за своєю природою є суб'єктивними, неточними та важко піддаються прямому кількісному вимірюванню. У традиційних методах аналізу ризиків часто виникають проблеми з присвоєнням точних числових значень таким параметрам, що може призвести до спрощених або нереалістичних моделей. Нечітка логіка ж дозволяє включити ці невизначеності безпосередньо в модель, роблячи її більш реалістичною та надійною.

Ось кілька прикладів якісних факторів ризику, де нечіткі множини знаходять широке застосування:

Рівень безпеки: Оцінка рівня безпеки системи або об'єкта часто вимагає врахування безлічі факторів, багато з яких не мають чітких метрик. Наприклад, "достатня" безпека може залежати від комплексу умов, таких як рівень підготовки персоналу, якість обладнання, ефективність протоколів та потенційні загрози. Нечітка логіка дозволяє агрегувати експертні судження щодо цих факторів, присвоюючи їм ступені належності до нечітких множин типу «низький рівень безпеки», «середній рівень безпеки» або «високий рівень безпеки». Це дозволяє отримати більш нюансовану та комплексну оцінку загального рівня безпеки.

Надійність системи: Надійність системи – це її здатність виконувати визначені функції за заданих умов протягом певного періоду часу. Оцінка надійності може бути складною, особливо для складних систем, де відсутні повні статистичні дані про відмови. Нечітка логіка дає змогу моделювати такі лінгвістичні поняття, як «висока надійність», «помірна надійність» або «низька надійність», на основі якісних оцінок компонентів системи, умов експлуатації та потенційних збоїв. Наприклад, експерти можуть оцінювати надійність окремих вузлів, використовуючи нечіткі терміни, а потім нечітка

система може агрегувати ці оцінки для визначення загальної надійності системи.

Експертні судження: У багатьох сферах аналізу ризиків, особливо там, де даних обмаль або вони неповні, **експертні судження** відіграють вирішальну роль. Однак експерти часто висловлюють свої оцінки в нечітких термінах, таких як «імовірно», «можливо», «рідко», «часто». Нечітка логіка надає фреймворк для формалізації цих суб'єктивних суджень. Замість того, щоб змушувати експертів давати точні числові оцінки, які можуть бути необґрунтованими, нечітка логіка дозволяє їм використовувати лінгвістичні змінні, які потім перетворюються на нечіткі множини. Це дозволяє більш точно відобразити невизначеність, притаманну людським оцінкам, і інтегрувати їх у математичну модель ризику. Наприклад, експерт може оцінити ймовірність події як «дуже низьку», що відповідатиме певній функції належності в нечіткій множині «низька ймовірність».

Використання нечітких множин в аналізі ризиків не тільки дозволяє ефективно обробляти якісні та нечіткі дані, але й робить моделі більш зрозумілими та інтерпретованими для осіб, які приймають рішення, оскільки вони працюють з концепціями, близькими до природної мови. Це значно підвищує якість та обґрунтованість рішень щодо управління ризиками.

Таблиця 2.9

Порівняння класичних і нечітких моделей у ризик-менеджменті

Параметр	Класична модель	Нечітка модель
Тип даних	Точні	Неточні, лінгвістичні
Форма входу	Цифрова	Вербальна
Результат	Чіткий	Діапазон, ступінь належності

Архітектура нечіткої системи оцінки ризику

Нижче наведено графічну схему, яка ілюструє архітектуру FIS, застосовану до оцінки ризику:

Пояснення компонентів схеми

1. Вхідні дані (Чіткі значення ризику): На цьому етапі система отримує чіткі, точні числові значення, які характеризують різні аспекти ризику. Це можуть бути, наприклад, ймовірність події, потенційні збитки, швидкість виникнення проблеми тощо.

2. Фаззифікація (Fuzzification): Призначення: Перетворення чітких вхідних даних на нечіткі множини. Процес: Чіткі значення відображаються на функції належності (membership functions), які визначають ступінь належності (membership degree) цих значень до різних нечітких термів (наприклад, «низький ризик», «середній ризик», «високий ризик»). Це дозволяє системі працювати з лінгвістичними змінними.

3. База нечітких правил (Fuzzy Rule Base): Призначення: Зберігання знань про систему у вигляді «ЯКЩО-ТО» правил.

Приклад: ЯКЩО (Ймовірність = Висока) І (Наслідки = Катастрофічні) ТО (Ризик = Дуже Високий). ЯКЩО (Ймовірність = Низька) І (Наслідки = Незначні) ТО (Ризик = Дуже Низький). Ці правила формулюються експертами або генеруються за допомогою машинного навчання.

4. Блок логічного висновку (Inference Engine): Призначення: Застосування нечітких правил до фаззифікованих вхідних даних для отримання нечітких вихідних даних. Процес: Використовуються методи нечіткої логіки (наприклад, Мамдані або Сугено) для агрегації результатів правил і формування нечіткого вихідного значення, яке є нечіткою множиною.

5. Дефаззифікація (Defuzzification): Призначення: Перетворення нечіткого вихідного значення назад у чітке числове значення. Процес: Існує кілька методів дефаззифікації, наприклад, метод центру ваги (centroid), середнього максимуму (mean of maxima) тощо. Метою є отримання одного, інтерпретованого числового значення, яке представляє остаточну оцінку ризику.

6. Вихідні дані (Чітке значення оцінки ризику): Остаточне числове значення, яке є результатом оцінки ризику нечіткою системою. Це значення може бути використане для прийняття рішень (наприклад, «ризик 7.5 з 10»).

Ця графічна схема чітко демонструє послідовність етапів у нечіткій системі оцінки ризику, від отримання сирих даних до отримання чіткого вихідного результату, що є ключовим для розуміння функціонування таких систем.

Фрагмент кода

```
graph TD
    A[Вхідні дані (Чіткі значення ризику)] --> B{Фаззифікація};
    B --> C{База нечітких правил};
    C --> D{Блок логічного висновку};
    D --> E{Дефаззифікація};
    E --> F[Вихідні дані (Чітке значення оцінки ризику)];

    subgraph Fuzzy Inference System (FIS)
        B
        C
        D
        E
    end

    style A fill:#aaffaa,stroke:#333,stroke-width:2px;
    style F fill:#aaffaa,stroke:#333,stroke-width:2px;
    style B fill:#add8e6,stroke:#333,stroke-width:2px;
    style C fill:#fffacd,stroke:#333,stroke-width:2px;
    style D fill:#add8e6,stroke:#333,stroke-width:2px;
    style E fill:#add8e6,stroke:#333,stroke-width:2px;
```

Рис. 2.6. Графічна схема: Побудова нечіткої системи оцінки ризику [Архітектура Fuzzy Inference System (FIS): fuzzification – inference – defuzzification]

2. Аналіз сценаріїв і варіантів розвитку подій

Сценарій у контексті аналізу ризиків, стратегічного планування або управління складними системами – це якісно-кількісна модель потенційного майбутнього, що дозволяє унаочнити, осмислити та прогнозувати можливі

варіанти розвитку подій. Цей інструмент є незамінним у ситуаціях високої невизначеності, коли традиційні методи прогнозування втрачають ефективність.

На відміну від одномірного прогнозу, сценарій дозволяє враховувати широкий спектр невизначених чинників – політичних, економічних, соціальних, технологічних та екологічних – і передбачити декілька альтернативних траєкторій розвитку. Таким чином, сценарій є *не фіксованим прогнозом*, а *моделюванням кількох можливих картин майбутнього*, кожна з яких базується на зміні ключових детермінант.

Основу сценарного підходу складає розробка альтернативних варіантів розвитку ситуації з урахуванням критичних факторів впливу. Ці варіанти не обов'язково відображають найімовірніші події – натомість, вони показують крайні або репрезентативні комбінації факторів, які допомагають виявити вразливі місця, нові можливості або критичні ризики у системі прийняття рішень.

Алгоритм сценарного аналізу

Сценарний аналіз є структурованим методом, який реалізується у кілька послідовних етапів. Кожен із них має своє функціональне навантаження та значущість для загального результату.

1. Ідентифікація ключових факторів впливу

Цей етап передбачає всебічне вивчення середовища, у якому функціонує об'єкт аналізу. Основна мета – виявити критичні фактори, які можуть істотно вплинути на перебіг подій у майбутньому. Такі фактори можуть бути як внутрішні (організаційні, технологічні, управлінські), так і зовнішні (макроекономічні тенденції, зміни у нормативно-правовому полі, поведінка конкурентів тощо).

На цьому етапі широко застосовуються методи експертного опитування, SWOT-аналіз, PESTLE-аналіз, аналіз зацікавлених сторін (stakeholder analysis), побудова дерева впливів тощо. Головне – сформувати повний список релевантних чинників, що формують майбутні ризики або можливості.

2. Класифікація факторів за ступенем невизначеності та впливу

Після ідентифікації чинників необхідно здійснити їх систематизацію за двома критеріями:

а) Ступінь впливу на систему: наскільки той чи інший фактор здатен трансформувати ситуацію.

б) Рівень невизначеності: чи є цей чинник передбачуваним, чи він може змінюватися хаотично та непередбачувано.

Для цього використовують матрицю впливу-невизначеності (impact-uncertainty matrix), де на осі X розміщують рівень невизначеності, а на осі Y - силу впливу. У результаті отримують чотири квадранти, з яких найважливішими є ті чинники, що мають високий вплив та високу невизначеність. Саме вони формуватимуть основу сценарного дерева.

3. Побудова базових сценаріїв

На цьому етапі конструюються основні моделі майбутнього, які ілюструють альтернативні варіанти розвитку подій. Як правило, створюють 3-5 сценаріїв:

1) Оптимістичний – реалізація найсприятливіших припущень.
2) Песимістичний – розвиток подій за найгірших обставин.
3) Інерційний (базовий) – майбутнє, в якому поточні тренди зберігаються.
4) Дисраптивний – різка зміна внаслідок зовнішнього шоку чи технологічного прориву.

Сценарії будуються на основі комбінування ключових чинників (високої невизначеності) у різних варіантах їх прояву. Наприклад, у сценарії технологічного прориву передбачається різке зниження витрат виробництва через штучний інтелект, що трансформує всю галузь.

4. Моделювання наслідків

Кожен побудований сценарій має бути ретельно проаналізований з точки зору його наслідків для об’єкта аналізу.

Це включає: економічні наслідки (витрати, доходи, інвестиції); соціальні наслідки (зміни в поведінці споживачів, потреби в кадрах); правові наслідки (можливі регуляторні зміни); технологічні наслідки (адаптація інфраструктури, потреба в нових рішеннях); екологічні наслідки (вплив на довкілля).

На цьому етапі використовуються аналітичні та симуляційні моделі, зокрема імітаційне моделювання, системна динаміка, агентне моделювання тощо. Мета – прогнозувати, як кожен сценарій вплине на ключові параметри системи.

5. Оцінка ймовірностей та чутливості

Останній етап полягає в кількісному або якісному оцінюванні ймовірності реалізації кожного сценарію. Зазвичай використовуються експертні методи (метод Делфі, парне порівняння) або байєсівський підхід для формалізації невизначеностей.

Паралельно виконується чутливісний аналіз (sensitivity analysis) – оцінка того, як зміни одного чи кількох факторів впливають на результати. Це дозволяє з’ясувати, які змінні є критично важливими та потребують постійного моніторингу.

Сценарний підхід є ефективним інструментом управління невизначеністю в складних системах. Його застосування дозволяє не лише краще розуміти можливі траєкторії розвитку ситуації, але й підвищувати адаптивність управлінських рішень, завчасно готуючи організацію або систему до дій в умовах радикальних змін. В умовах сучасного динамічного світу сценарний аналіз стає не просто методом прогнозування, а невід’ємною складовою стратегічного мислення.

Таблиця 2.10

Типи сценаріїв

Тип сценарію	Опис
Базовий	Найбільш імовірний перебіг подій
Песимістичний	Найгірший сценарій із високим рівнем ризику
Оптимістичний	Сценарій із найсприятливішими умовами
Криза	Аномальна подія з руйнівними наслідками

Приклад: Сценарії розвитку кіберзагроз у промислових системах

1) Сценарій 1: Атака через SCADA – часткове порушення керування
2) Сценарій 2: Масштабний DDoS – зупинка виробництва
3) Сценарій 3: Впровадження адаптивної системи безпеки – мінімізація впливу атак

3. Інтервальний аналіз та байєсівські мережі

Інтервальний аналіз

Цей підхід застосовується у випадках, коли параметри ризику невідомі з точністю, а задані як інтервали.

Формалізація: Нехай. Тоді ризикова оцінка.

Переваги: Облік неповної інформації. Побудова обмежувальних оцінок.

Таблиця 2.11

Приклад інтервального оцінювання ризику

Параметр	Мінімальне значення	Максимальне значення	Інтервал ризику
Температура, °C	60	90	[0,2, 0,8]
Вологість, %	30	70	[0,1, 0,6]

Байєсівські мережі (Bayesian Networks)

Байєсівські мережі – це графові моделі ймовірнісного умовного зв’язку між змінними, які дозволяють враховувати причинно-наслідкові залежності в умовах невизначеності.

Основні компоненти: Вузли: випадкові змінні (події, параметри). Дуги: напрям причинного впливу. Таблиці ймовірностей (Conditional Probability Tables, CPT).

Побудова байєсівської мережі: Ідентифікація змінних. Побудова графа залежностей. Наповнення CPT на основі даних або експертної оцінки. Проведення інференції (оновлення оцінок при надходженні нових даних)

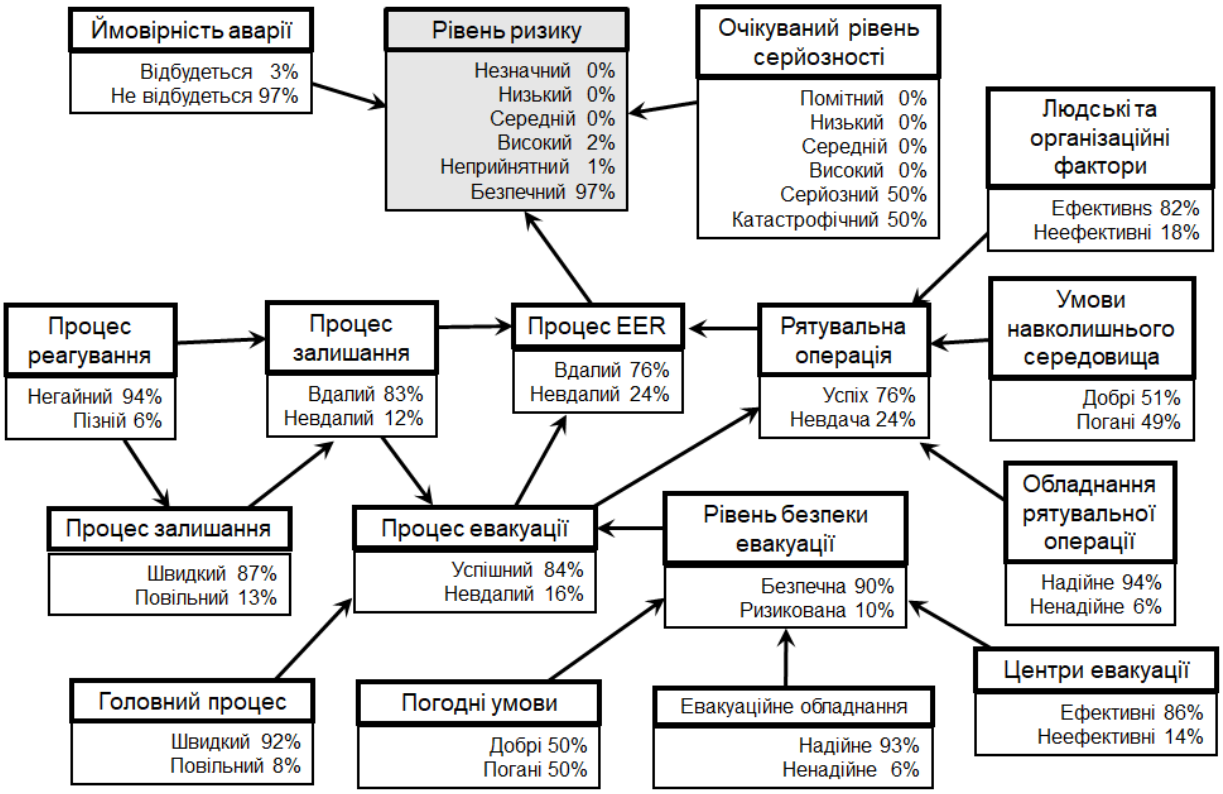

Рис. 2.7. На основі мереж Баєса аналіз відмов бар'єрів безпеки на плавучій СПГ-установці.

4. Інтеграція методів у єдину систему аналізу

Гібридні моделі

Можлива інтеграція нечіткої логіки, байєсівських мереж та сценарного аналізу у вигляді гібридних інтелектуальних систем для комплексного аналізу ризиків.

Таблиця 2.12

Порівняльна характеристика методів обробки невизначеності

Метод	Тип невизначеності	Основна перевага	Обмеження
Нечітка логіка	Лінгвістична	Гнучкість	Суб'єктивність
Сценарії	Комбінована	Врахування варіантів	Складність моделювання
Інтервали	Кількісна	Простота реалізації	Недостатня точність
Байєсівські мережі	Ймовірнісна	Врахування причинності	Потреба в даних

Сучасні методи аналізу невизначеності та чутливості в системному аналізі ризиків дозволяють ефективно ідентифікувати, класифікувати та оцінювати ризики в складних об’єктах. Застосування моделей нечіткої

логіки, сценарного аналізу, інтервального підходу та байєсівських мереж підвищує надійність прогнозування та прийняття рішень, знижуючи ймовірність системних збоїв у критично важливих системах.

2.4. Когнітивне моделювання ризиків у складних соціально-технічних системах

Когнітивне моделювання являє собою сучасний системно-аналітичний підхід до ідентифікації, аналізу та прогнозування ризиків у складних соціально-технічних системах. Воно ґрунтується на формалізації експертних знань, концептуалізації факторів ризику та побудові причинно-наслідкових зв’язків між ними у вигляді когнітивних карт.

Соціально-технічні системи (СТС), зокрема критичні інфраструктури, енергетичні мережі, системи національної безпеки або великі виробничо-логістичні комплекси, відзначаються динамічністю, неоднорідністю компонентів, мультиагентною природою та високим рівнем невизначеності. У таких умовах традиційні кількісні методи аналізу ризиків не завжди є придатними, що й обґрунтовує застосування когнітивних підходів.

Побудова когнітивних карт ризику

Когнітивна карта ризику – це орієнтований граф, у якому вузли відображають фактори ризику або ключові змінні, а дуги – причинно-наслідкові впливи між ними.

Формування когнітивної моделі включає кілька етапів, а саме: Ідентифікація релевантних факторів – з використанням експертних опитувань, аналізу літератури, статистичних даних тощо. Формалізація зв’язків – визначення позитивного або негативного характеру впливів між змінними. Встановлення сили впливів – за допомогою шкал оцінювання (наприклад, від -1 до +1). Побудова матриці суміжності – числового представлення когнітивної карти. Графічна візуалізація – побудова когнітивного графа (див. Рис. 2.8.).

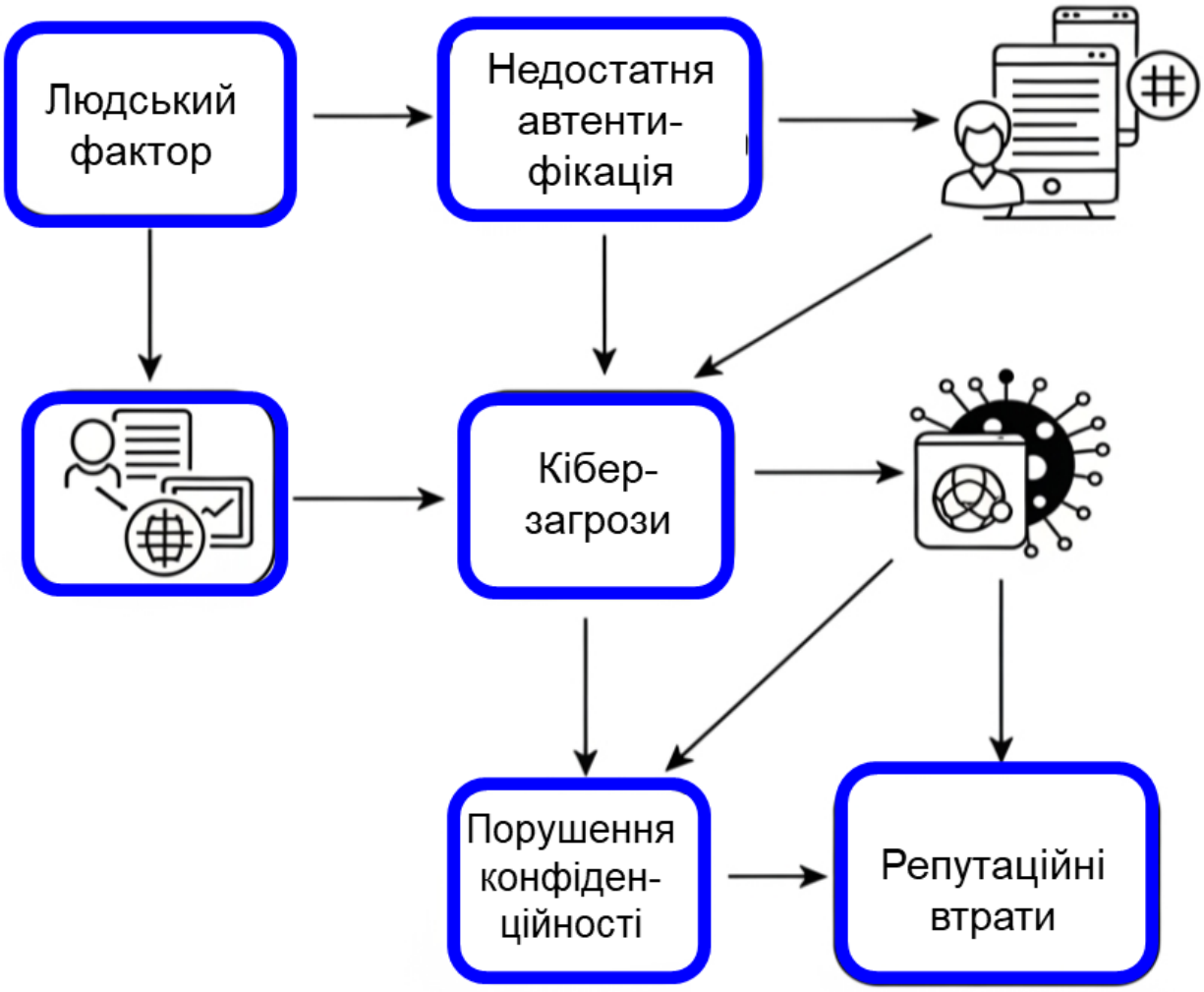

Рис. 2.8. Приклад когнітивної карти ризиків у сфері кібербезпеки
Графічне зображення когнітивної карти з вузлами: «Людський фактор», «Недостатня автентифікація», «Кіберзагроза», «Порушення конфіденційності», «Репутаційні втрати», зі стрілками впливів між ними.

Таблиця 2.13

Приклад фрагмента матриці вагових коефіцієнтів впливів

Фактор \ Вплив	F1: Людський фактор	F2: Недостатня автентифікація	F3: Кіберзагроза
F1	0	0.8	0.4
F2	0	0	0.6
F3	0	0	0

Аналіз сценаріїв на основі когнітивної моделі

Аналіз сценаріїв із застосуванням когнітивних карт базується на обчисленні ефектів розповсюдження впливів у системі.

Основні інструменти включають до себе: Імпульсний аналіз (Impulse Analysis) – оцінювання змін у системі після введення одиничного імпульсу в

певний вузол. Аналіз стабільності моделі – за допомогою спектрального радіуса матриці ваг. Визначення ключових вузлів – факторів з найбільшим індексом впливовості (influence index).

Таблиця 2.14

Сценарне моделювання наслідків впливу на «Недостатню автентифікацію»

Крок	Людський фактор	Недостатня автентифікація	Кіберзагроза	Конфіденційність
0	0	1	0	0
1	0	1	0,6	0,3
2	0	1	0,84	0,51

Застосування когнітивного моделювання у прийнятті управлінських рішень

Когнітивні моделі є цінним інструментом у стратегічному управлінні ризиками.

Вони дозволяють здійснювати наступні напрями: Підтримувати ухвалення рішень – ідентифікувати критичні точки впливу та пропонувати інтервенції. Формувати політику управління – на основі моделювання сценаріїв і оцінки наслідків. Використовувати в мультиагентних середовищах – як інструмент координації рішень між суб’єктами.

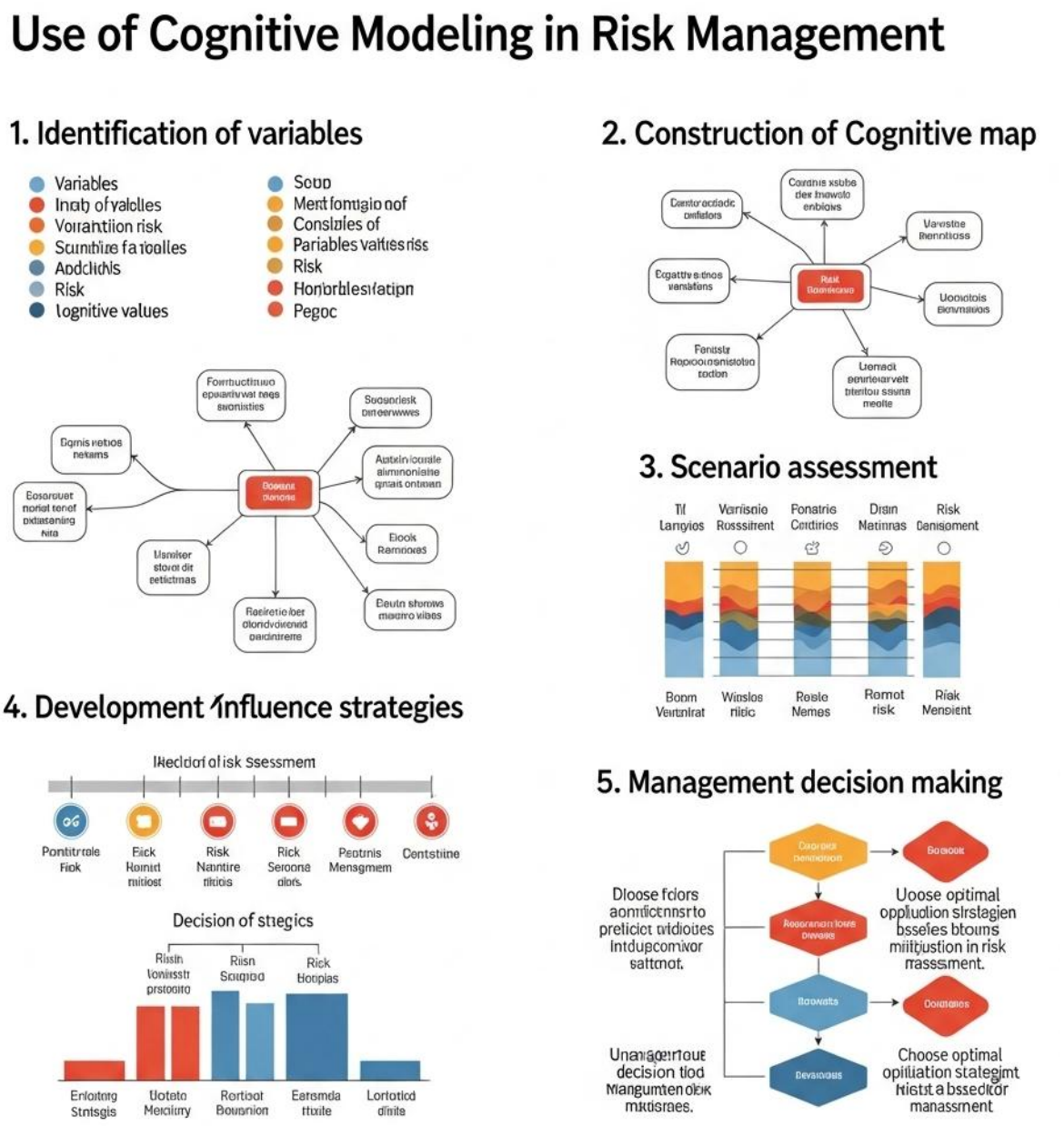

Рис. 2.9. Алгоритм використання когнітивного моделювання в управлінні ризиками: Ідентифікація змінних → 2. Побудова когнітивної карти → 3. Оцінка сценаріїв → 4. Розробка стратегій впливу → 5. Прийняття управлінських рішень.

Таблиця 2.15

Приклади управлінських інтервенцій на основі аналізу

Ключовий вузол	Потенційна дія	Очікуваний ефект
Недостатня автентифікація	Впровадження двофакторної авторизації	Зниження ризику витоку даних
Людський фактор	Навчання персоналу	Зменшення ймовірності інцидентів

Програмне забезпечення для когнітивного моделювання

Існує низка інструментів для реалізації когнітивного аналізу, основні із них включають до себе наступні програмні продукти: Cognitive Map Toolkits (CMAP). Decision Explorer. FCMapper. Vensim / AnyLogic (у поєднанні зі структурним моделюванням)

Таблиця 2.16

Порівняння програмних інструментів

Інструмент	Підтримка сценаріїв	Інтерфейс	Експорт у графові формати
CMAP	Так	Середній	GraphML
Decision Explorer	Так	Високий	CSV, XML
FCMapper	Так (через R)	Низький	Graphviz

Когнітивне моделювання в умовах складних соціально-технічних систем є ефективним інструментом аналізу ризиків, який поєднує якісні експертні знання з формальними алгоритмами оцінювання. Завдяки побудові когнітивних карт і аналізу сценаріїв можливо не лише виявляти потенційні загрози, а й ефективно планувати дії з управління ними. Це робить когнітивне моделювання важливим компонентом у системному аналізі ризиків та забезпеченні стійкості складних систем.

Контрольні питання

1. У чому полягає специфіка ризиків у складних системах у порівнянні з простими?
2. Які основні ознаки складної системи важливо враховувати при ідентифікації ризиків?
3. Що таке системна ідентифікація небезпек і як вона відрізняється від класичного підходу?
4. Які методи можна застосовувати для виявлення вразливостей у складних об’єктах?
5. Які етапи включає процес картування ризиків (Risk Mapping)?
6. Які переваги та обмеження картування ризиків у складних соціально-технічних системах?
7. Як можна візуалізувати взаємозв’язки між небезпеками, загрозами та вразливостями у складній системі?
8. У чому полягає суть методу аналізу ієрархій (AHP) для оцінювання ризиків?
9. Як працює метод TOPSIS та які типи рішень він дозволяє підтримувати?
10. Які особливості має метод ELECTRE при аналізі ризиків?
11. Яким чином мультикритеріальні методи враховують конфліктність критеріїв у системному аналізі?

12. Як здійснюється інтеграція суб’єктивних та об’єктивних оцінок у ризик-менеджменті?
13. У чому полягає роль експертного оцінювання в умовах системної взаємодії елементів?
14. Як можна перевірити надійність і узгодженість експертних оцінок при багатокритеріальному аналізі?
15. Яким чином нечітка логіка допомагає врахувати невизначеність у моделюванні ризиків?
16. У чому полягає відмінність між нечіткими множинами та класичними множинами в контексті ризик-аналізу?
17. Які типи сценаріїв застосовуються в аналізі варіантів розвитку подій у ризик-орієнтованому системному аналізі?
18. Що таке інтервальний аналіз та як він використовується для оцінювання ризику в умовах невизначеності?
19. Які можливості надає використання байєсівських мереж у моделюванні ризиків?
20. Як можна оцінити чутливість системної моделі до змін вхідних параметрів?
21. Що таке когнітивна карта ризиків та які етапи її побудови?
22. Які переваги когнітивного моделювання в аналізі взаємозалежних ризиків?
23. Як аналіз сценаріїв на основі когнітивної моделі допомагає приймати обґрунтовані рішення?
24. Які інструменти можуть бути використані для створення та аналізу когнітивних моделей ризику?
25. Як когнітивні моделі підтримують процес прийняття управлінських рішень у складних соціально-технічних умовах?

Кейси до розділу 2

Кейс 1. Системно орієнтоване виявлення ризиків у виробничій системі з високим рівнем автоматизації

На заводі з виготовлення електроніки було виявлено, що зростає кількість інцидентів, пов’язаних із зупинкою роботизованих ліній. Попередній аудит не виявив критичних технічних відмов, однак проблеми продовжують виникати.

Здійсніть системну ідентифікацію потенційних ризиків за допомогою методу структуризації (наприклад, діаграми Ісікави або дерева причин). Визначте, які елементи системи можуть бути прихованими джерелами ризику, та сформулюйте рекомендації щодо інтеграції методів виявлення слабких сигналів у процес управління виробництвом.

Кейс 2. Мультикритеріальний аналіз ризиків у муніципальній інфраструктурі

Міська влада розглядає варіанти оновлення водопровідної системи, яка зазнала кількох аварій. Для обґрунтування інвестицій необхідно провести оцінювання ризиків з урахуванням таких факторів: ймовірність прориву труб, вартість ремонту, соціальний ефект, екологічні наслідки.

Побудуйте мультикритеріальну модель оцінювання ризиків (наприклад, за методом AHP або аналізом зважених балів). Поясніть, як визначались ваги критеріїв, та обґрунтуйте обраний варіант модернізації з урахуванням найвищого інтегрального ризику.

Кейс 3. Аналіз чутливості ризиків у критичній інформаційній системі

У структурі МВС експлуатується інформаційна система моніторингу правопорушень. Через модернізацію компонентів (сервери, канали передачі даних, оновлення бази даних) з'явилась потреба проаналізувати, які з параметрів системи найбільше впливають на загальний рівень ризику збоїв.

Використовуючи метод аналізу чутливості, оцініть залежність вихідного ризику від зміни окремих вхідних параметрів. Визначте критичні змінні та побудуйте таблицю/графік впливу. Сформулюйте висновки щодо доцільності коригування найбільш вразливих елементів.

Кейс 4. Когнітивне моделювання ризиків у системі управління громадським транспортом

Після впровадження нової системи електронного квитка в міському транспорті спостерігалися періодичні збої валідації, зростання конфліктів між пасажирами та водіями, а також перевантаження серверів у години пік.

Побудуйте когнітивну карту, що відображає причинно-наслідкові зв'язки між ризик-факторами (технічними, поведінковими, організаційними). Позначте тип зв'язку (позитивний/негативний) і силу впливу. На основі моделі запропонуйте точки втручання для зменшення ризику системного збою.

Кейс 5. Ідентифікація системних ризиків у міжвідомчому проекті цифровізації

У ході реалізації пілотного проєкту цифрової інтеграції даних між судами, поліцією та медичними закладами виявлено низку труднощів: різні формати даних, неузгоджені протоколи безпеки, інституційна конкуренція.

Використайте принципи системного підходу до виявлення міжорганізаційних ризиків. Проведіть структуризацію проблем за методикою «What-if Analysis», визначте основні конфліктні зони, запропонуйте сценарії

гармонізації взаємодії суб'єктів у рамках міждисциплінарного ризик-менеджменту.

Висновок по розділу 2

Розділ 2 навчального посібника присвячено комплексному аналізу системних підходів до виявлення, ідентифікації, моделювання та оцінювання ризиків у контексті складних технічних, соціотехнічних і інформаційних систем. Запропонований матеріал демонструє актуальність і необхідність системного бачення ризиків, що виникають у процесах проектування, експлуатації та модернізації технічних об'єктів у сучасних умовах високої складності та невизначеності. Кожен із підрозділів 2.1-2.4 розкриває специфічні методологічні засади та інструментарій, що можуть бути використані у практиці безпечного управління технічними системами.

У підрозділі 2.1 проаналізовано природу складних систем, що є ієрархічними, відкритими, адаптивними структурами з множинною взаємодією елементів. Така системна складність генерує специфічні типи ризиків: як технічного, так і організаційного, людського або інформаційного характеру. Особливу увагу приділено системній ідентифікації небезпек і вразливостей, що передбачає цілісне розуміння структури об'єкта, його функціональних зв'язків, вхідних і вихідних потоків інформації, ресурсів, енергії. Методологія картування ризиків (Risk Mapping) розглядається як потужний візуалізаційний інструмент, що забезпечує формування комплексної картини потенційних загроз і взаємозв'язків між ними. Завдяки цьому інструменту значно підвищується ефективність стратегічного аналізу та формування пріоритетів безпеки.

Підрозділ 2.2 присвячено мультикритеріальним методам оцінювання ризиків, серед яких найбільшу увагу приділено методам AHP (Analytic Hierarchy Process), TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) та ELECTRE (Elimination and Choice Expressing the Reality). Ці методи дозволяють ефективно обробляти ризики з урахуванням множинності критеріїв, що відображають різні аспекти безпеки – від технічної надійності до вартості впровадження захисних заходів. Особливо актуальним є підхід, який передбачає поєднання суб'єктивних (експертних) і об'єктивних (кількісних, статистичних) оцінок. Системна взаємодія між критеріями, альтернативами та експертними судженнями дозволяє досягти збалансованих рішень, що враховують різноманітні сценарії розвитку подій і багаторівневий характер ризику. Мультикритеріальні підходи, розглянуті у підрозділі, демонструють високу адаптивність до складних умов прийняття рішень в умовах обмеженої інформації.

Підрозділ 2.3 висвітлює феномен невизначеності, який є невід'ємним атрибутом аналізу ризиків у складних системах. Застосування моделей нечіткої логіки та теорії нечітких множин дає змогу подолати обмеження класичних детермінованих підходів, надаючи аналітичну основу для врахування нечітких, суб'єктивних, неповних або суперечливих даних.

Аналіз сценаріїв і варіантів розвитку подій дозволяє змоделювати широкий спектр потенційних станів системи та оцінити їхню ймовірність і наслідки. Інтервальний аналіз і байєсівські мережі дають змогу кількісно опрацьовувати варіативні оцінки параметрів і зв'язків між елементами системи, формуючи гнучкі, адаптивні моделі ризику. У сукупності, ці підходи дозволяють зменшити невизначеність, підвищити обґрунтованість управлінських рішень та забезпечити стійкість систем у змінному середовищі.

У підрозділі 2.4 особливу увагу приділено когнітивному моделюванню як потужному методу аналізу ризиків у соціотехнічних системах, де домінують складні людські фактори, інформаційні впливи та багаторівнева взаємодія. Когнітивні карти ризику дають змогу моделювати не лише об'єктивні взаємозв'язки, але й суб'єктивні уявлення, переконання, очікування, які впливають на прийняття рішень. Вивчення сценаріїв на основі когнітивних моделей дає змогу виявити критичні точки ризику, конфліктні зони та системні парадокси. Когнітивний підхід є особливо ефективним у підтримці прийняття управлінських рішень, оскільки дозволяє візуалізувати складні причинно-наслідкові зв'язки та моделювати поведінку системи в умовах змін.

Таким чином, у Розділі 2 представлено цілісну методологічну рамку системного аналізу ризиків, яка поєднує якісні та кількісні підходи, враховує взаємозв'язок між структурними елементами, динаміку змін, невизначеність та багаторівневість сучасних технічних і соціотехнічних систем. Застосування системно орієнтованих, мультикритеріальних, когнітивних та нечіткісних методів дозволяє не лише адекватно ідентифікувати й оцінювати ризики, але й формувати обґрунтовані стратегії їхнього зниження, адаптації або компенсації. Результати, викладені в розділі, можуть бути безпосередньо використані в інженерній практиці, технічному аудиті, державному управлінні, аналітичних службах та під час проектування складних систем із вбудованими механізмами забезпечення безпеки.

У підсумку, системний підхід до аналізу ризиків у технічних системах, як його подано у Розділі 2, є не лише теоретично обґрунтованим, але й методологічно ефективним та практично значущим. Його використання сприяє формуванню нового стандарту мислення у сфері технічної безпеки, який базується на інтеграції міждисциплінарних знань, інструментальної точності та стратегічного бачення.

РОЗДІЛ 3. ПРОГНОЗУВАННЯ РИЗИКІВ У СИСТЕМНОМУ СЕРЕДОВИЩІ

3.1. Моделювання ризиків в умовах динаміки та невизначеності

У сучасному системному середовищі ризики не є сталими чи ізольованими явищами, натомість вони постійно виникають, розвиваються та трансформуються під впливом широкого спектра чинників. Характерною рисою цього середовища є висока динаміка змін – як внутрішніх (технологічних, економічних, організаційних), так і зовнішніх (соціальних, політичних, екологічних). Усе це відбувається в умовах багатовимірної невизначеності, де не лише початкові умови, але й самі правила взаємодії між елементами системи можуть змінюватися з плином часу. Невизначеність проявляється не лише в нестабільності вхідних параметрів, а й у непередбачуваності поведінки учасників системи, змінних середовища та збоїв у комунікаційних каналах.

У таких умовах традиційні статичні підходи до аналізу ризиків виявляються недостатніми, оскільки вони не враховують тимчасові аспекти розвитку подій, зворотні впливи дій на саму систему, а також складну взаємодію між суб'єктами, що приймають рішення. Тому виникає нагальна потреба у використанні адаптивних і прогностичних моделей, які здатні враховувати часові лаги (відкладені ефекти рішень), петлі зворотного зв’язку (як позитивного, так і негативного типу), стохастичні збурення (випадкові флуктуації параметрів), а також поведінкові чинники (очікування, індивідуальна раціональність, емоції) та агентні фактори (взаємодія автономних суб'єктів системи з різними цілями та стратегіями).

Часові лаги є критичним елементом моделювання, оскільки між прийняттям рішення і його наслідками може проходити значний проміжок часу. Це особливо важливо в контексті стратегічного управління ризиками, де короткострокові дії можуть мати довгострокові ефекти, часто непередбачуваного характеру.

Зворотні зв’язки формують основу саморегуляції або самопідсилення систем, що може як стабілізувати, так і дестабілізувати її. Наприклад, в економічній системі зростання ризику може спричинити зменшення інвестицій, що, своєю чергою, ще більше підсилить нестабільність.

Стохастичні впливи охоплюють випадкові події, які неможливо передбачити із повною точністю, але їхню ймовірність можна оцінити на основі статистичних даних. Такі впливи вимагають включення у моделі елементів ймовірнісного прогнозування та сценарного аналізу.

Поведінкові чинники відображають когнітивні та психологічні особливості суб'єктів прийняття рішень – наприклад, ефект упередженості у ризик-оцінках, ефект втрати або надмірний оптимізм. Залучення таких чинників забезпечує вищу точність і реалістичність моделювання складних соціотехнічних систем.

Агентні фактори розглядають систему як сукупність взаємодіючих агентів, кожен із яких має власну мету, обмежену інформацію, адаптивну поведінку і здатність до навчання. Це дозволяє моделювати емерджентні властивості систем, які виникають не з окремих елементів, а з їхніх взаємодій (наприклад, панічні настрої на фінансових ринках чи колективну реакцію на загрозу).

Усі ці елементи вимагають застосування сучасного інструментарію моделювання, здатного репрезентувати складну динаміку змін системних параметрів. Динамічні системи у поєднанні з методами системної динаміки дозволяють будувати причинно-наслідкові петлі, визначати критичні точки системи, моделювати ланцюгові реакції та оцінювати довгострокові наслідки управлінських рішень. Наприклад, системна динаміка дає змогу аналізувати баланс між витратами на безпеку і рівнем ризику в організації з урахуванням відкладеного ефекту інвестицій.

Імітаційне моделювання дає змогу проводити віртуальні експерименти у безпечному середовищі, змінюючи параметри моделі, структуру системи або початкові умови для виявлення можливих сценаріїв розвитку подій. Це особливо корисно для аналізу рідкісних, але катастрофічних подій (low-probability, high-impact events), які складно дослідити емпірично.

Агентне моделювання дає змогу враховувати мікрорівень взаємодії між суб'єктами системи з різними характеристиками, моделюючи як їхню індивідуальну, так і колективну поведінку. Цей підхід особливо цінний у дослідженні соціотехнічних, інформаційних та організаційних систем, де люди, алгоритми та інфраструктурні елементи взаємодіють у складній мережі.

Отже, ефективне управління ризиками в умовах сучасної складної та динамічної реальності потребує міждисциплінарного підходу, що поєднує математичне моделювання, системний аналіз, кібернетику, психологію, економіку та інформатику. Такий підхід забезпечує глибше розуміння поведінки складних систем, дозволяє здійснювати обґрунтоване прогнозування ризиків і формулювати адаптивні стратегії управління, що здатні зберігати ефективність навіть в умовах турбулентності та постійних змін.

Динамічні системи та моделі з часовими лагами

У сучасному аналізі складних технічних, соціотехнічних та організаційних систем дедалі більшої значущості набуває використання динамічних моделей, які відображають зміну стану системи у часі. Динамічні системи – це системи, в яких поведінка змінюється під впливом внутрішніх процесів і зовнішніх чинників, причому ці зміни мають послідовний і взаємозалежний характер. У порівнянні з традиційними статичними підходами, динамічні системи дозволяють враховувати тимчасові аспекти розвитку, ефекти накопичення, затримки реакцій (так звані часові лаги), інерційність поведінки системи, а також взаємозв’язки між змінними, які розгортаються у часі.

У контексті моделювання ризиків, динамічний підхід є критично важливим, оскільки багато ризикових факторів не проявляються миттєво. Наприклад, невдала управлінська стратегія може призвести до зростання ризиків лише через певний час; так само недооцінка змін у зовнішньому середовищі (економічному, політичному, екологічному) може мати відтерміновані, але серйозні наслідки. Відповідно, динамічні моделі забезпечують можливість прогнозування розвитку подій у часі та тестування реакцій системи на зміни у вхідних параметрах.

Основні компоненти динамічної моделі

1. Станові змінні (state variables). Це ключові показники, що описують поточний стан системи. Вони змінюються з часом залежно від внутрішніх механізмів функціонування системи та впливу зовнішнього середовища. Наприклад, у фінансовій системі становими змінними можуть бути рівень прибутковості, рівень заборгованості або ліквідність активів. У моделюванні безпеки – рівень захищеності інфраструктури, кількість активних загроз або стан ресурсного забезпечення.

Важливою характеристикою станових змінних є їх здатність акумулювати інформацію про попередні стани системи, що дозволяє враховувати історичні дані при формуванні прогнозу.

2. Вхідні параметри (inputs). Це змінні, які надходять до системи ззовні і є екзогенними по відношенню до моделі. Вони не змінюються самою моделлю, але суттєво впливають на динаміку внутрішніх процесів. Наприклад, у моделюванні ризиків такими параметрами можуть бути рівень інфляції, частота кібератак, соціальні зміни, політична нестабільність тощо.

Вхідні параметри часто задаються як функції часу або сценаріїв, що дозволяє змінювати умови зовнішнього середовища під час віртуального експериментування.

3. Часові лаги (time lags).Часовий лаг – це затримка між впливом певної причини і моментом, коли проявляється її наслідок. У реальних системах такі затримки є типовим явищем: наприклад, впровадження нової технології може призвести до зменшення витрат лише через декілька місяців або навіть років. Аналогічно, порушення в роботі системи безпеки можуть проявитися не одразу, а після накопичення критичного рівня вразливостей.

Моделювання часових лагів дозволяє уникнути хибного уявлення про миттєву ефективність чи загрозу, натомість формуючи реалістичну картину інерційних процесів. Існують різні типи лагів: постійні, змінні, стохастичні; а також прямі й зворотні лаги, які можуть враховуватись у формальних рівняннях моделі.

4. Механізми перетворення (transformation mechanisms). Це правила, за якими змінюється стан системи. Вони можуть бути представлені у вигляді диференціальних або різницевих рівнянь, логічних конструкцій, стохастичних функцій або агентних алгоритмів. Механізми перетворення визначають, як саме вплив одного або кількох факторів викликає зміну певної станової змінної.

Наприклад, механізм перетворення в економічній моделі може описувати, як зміна відсоткової ставки впливає на рівень інвестицій, або як зростання кількості інцидентів у сфері безпеки впливає на загальний рівень загроз. У складних системах такі механізми часто мають нелінійний характер, тобто один і той самий вплив за різних умов може викликати зовсім іншу реакцію системи.

Завдяки використанню таких моделей, фахівці з ризик-менеджменту, системного аналізу чи інформаційної безпеки можуть: виявляти точки затримки або накопичення ризиків; проводити сценарне планування з урахуванням відкладених ефектів; оптимізувати керування ресурсами з урахуванням часових інтервалів реакції; моделювати системні наслідки управлінських рішень у середньо- та довгостроковій перспективі.

Таким чином, динамічні моделі з часовими лагами є потужним інструментом для аналізу ризиків у складних адаптивних системах. Вони дозволяють поєднати формальну точність математичного апарату з гнучкістю сценарного аналізу, що особливо важливо в умовах сучасного мінливого та нестабільного середовища.

Таблиця 3.1

Приклади часових лагів у ризикових процесах

Сфера	Приклад	Тип лагу
Економіка	Реакція ринку на зміну облікової ставки	Лінійний лаг
Безпека	Впровадження політики захисту даних	Інституційний лаг
Технічні системи	Вихід з ладу після впливу перевантаження	Фізичний лаг

Системна динаміка* Джеєм В. *Форрестера: петлі зворотного зв'язку

Метод системної динаміки, розроблений американським вченим Джеєм В. Форрестером у середині XX століття, став ключовим інструментом для моделювання та аналізу поведінки складних систем, що змінюються в часі. Цей підхід спочатку застосовувався в галузі управління промисловими підприємствами, однак згодом знайшов широке застосування в економіці, екології, соціальних науках, урбаністиці, інформаційних технологіях і, зокрема, в управлінні ризиками та безпекою технічних систем.

Системна динаміка базується на ідеї, що поведінка складних систем виникає з їхньої структури, тобто конфігурації внутрішніх змінних, з'єднань між ними, типів впливів, зворотних зв'язків і затримок. Це дозволяє будувати імітаційні моделі, які демонструють, як система змінюється під впливом внутрішніх та зовнішніх факторів.

Ключові елементи системної динаміки:

1. Рівня (Stocks): Це накопичувачі – змінні, які репрезентують ресурси, що зберігаються або акумулюються в системі з часом. Вони можуть бути

фізичними (наприклад, кількість матеріалу на складі, об’єм води у резервуарі), фінансовими (накопичений прибуток), інформаційними (база знань) або навіть соціальними (довіра, репутація). Рівня відображають стан системи на певний момент часу та є інерційними – вони не змінюються миттєво, а накопичують ефект від потоків.

2. Потоки (Flows): Потоки – це швидкість, з якою змінюються рівня. Вони можуть бути притоком або відтоком. Наприклад, притік води до резервуару чи відтік фінансів зі звітного рахунку. Потоки завжди пов’язані з рівнями і визначають, як швидко та в якому напрямку змінюється накопичення. Вони є руховою силою динаміки системи.

3. Зв’язки (Links): Це причинно-наслідкові взаємозв’язки між змінними системи. Через ці зв’язки визначаються впливи одного елементу системи на інший. Вони можуть мати часові затримки (наприклад, вплив впровадження нової політики на рівень споживання енергії проявляється через кілька місяців), бути прямими або опосередкованими. Зв’язки – це структурні елементи, які формують логіку взаємодії.

4. Петлі зворотного зв’язку (Feedback loops): Це один з найважливіших і водночас найхарактерніших компонентів системної динаміки. Вони описують циклічну взаємодію між елементами системи, коли вихід однієї змінної з часом починає впливати на саму себе через ланцюжок взаємозв’язків.

Така петля може: Стабілізувати систему (негативна петля зворотного зв’язку): Негативні зворотні зв’язки (balancing or negative feedback loops) виконують регулюючу або гомеостатичну функцію. Вони зменшують відхилення, повертаючи систему до стану рівноваги. Прикладом є термостат у системі опалення: коли температура підвищується вище заданої межі, система зменшує нагрів, і навпаки. Такі петлі важливі в системах управління ризиками, де необхідно уникнути коливань або кризових ситуацій.

Підсилювати процеси (позитивна петля зворотного зв’язку): Позитивні зворотні зв’язки (reinforcing or positive feedback loops) навпаки, підсилюють початкові зміни, спричиняючи експоненціальне зростання або падіння. Наприклад, в економіці – ефект «накопичення капіталу»: чим більше інвестується, тим більше прибутку, і тим більше можна інвестувати. Проте без належного контролю позитивні петлі можуть дестабілізувати систему, приводячи до краху або вибухових зростань.

Типові приклади застосування зворотних зв’язків:

1) Безпека технічних систем: Позитивні петлі можуть сприяти накопиченню вразливостей, якщо не реагувати на сигнали тривоги. Негативні петлі – це системи моніторингу й автоматичного втручання, які знижують ризик, коли рівень загрози перевищує поріг.

2) Соціальні системи: У моделях, які описують поширення чуток або довіри, позитивні петлі підсилюють вірусний ефект, а негативні – стабілізують ситуацію через втому або насичення інформацією.

3) Екологічні моделі: Наприклад, процес глобального потепління може мати позитивну петлю через танення льодовиків: менше льоду – менше відбивання сонячного світла – більше тепла – ще менше льоду.

Графічне представлення та моделювання:

Петлі зворотного зв’язку у системній динаміці часто позначаються за допомогою каузальних діаграм впливу (causal loop diagrams, CLD). На цих діаграмах: Стрілки позначають напрямок впливу; Знаки «+» та «–» вказують на тип впливу (прямий або зворотний); Замкнені контури позначають наявність петлі.

Такі діаграми дають змогу визначати потенційно критичні елементи, виявляти джерела нестабільності, аналізувати поведінкові патерни системи у довгостроковій перспективі.

Метод Форрестера та, зокрема, концепція петель зворотного зв’язку є фундаментом для розуміння та управління складними технічними системами, особливо в умовах динамічних ризиків. Вони дозволяють побачити більше, ніж просто лінійні причинно-наслідкові зв’язки, а саме – поведінкові закономірності, які розгортаються в часі та залежать від структури самої системи. Завдяки цьому системна динаміка забезпечує потужний інструментарій для передбачення, оцінки та проектування стійких і адаптивних систем, зокрема в галузях безпеки, управління технологіями та соціо-технічного розвитку.

Рис. 3.1. Приклад схеми зворотного зв’язку у моделі ризику
Рисунок: Петля «Інциденти – Контроль – Довіра – Інциденти»

Таблиця 3.2

Порівняння позитивного та негативного зворотного зв’язку

Характеристика	Позитивний зворотний зв’язок	Негативний зворотний зв’язок
Ефект	Підсилює зміну	Стабілізує систему
Приклад	Поширення паніки	Регуляторний механізм
Ризик	Ескалація загроз	Затухання небезпеки

Імітаційне та агентне моделювання

Імітаційне моделювання є потужним інструментом дослідження складних систем, який дозволяє вивчати поведінку об'єктів, процесів і явищ шляхом створення цифрових моделей, що відтворюють ключові елементи та динаміку реального світу. На відміну від аналітичних методів, які часто передбачають спрощення структури системи до формалізованих математичних рівнянь, імітаційне моделювання дозволяє зберігати її складність, варіювати параметри та аналізувати реакцію системи на різні сценарії розвитку.

Основна ідея методу полягає у створенні комп’ютерної моделі, яка відображає структурні характеристики та поведінкові закономірності реальної системи. Така модель може включати в себе як детерміновані, так і стохастичні елементи, враховувати часові затримки, зовнішні збурення, нелінійності й зворотні зв’язки. Це робить імітаційне моделювання незамінним інструментом для аналізу технічних, економічних, соціальних і екологічних систем, де експериментування з реальними об’єктами є небезпечним, дорогим або просто неможливим.

Ключові переваги імітаційного моделювання:

1) Безпечне експериментування: дозволяє проводити численні експерименти в умовах віртуального середовища без ризику для реальних об’єктів. Наприклад, моделювання поведінки ядерного реактора в екстремальних умовах можливе лише на симуляційному рівні.

2) Виявлення критичних точок і вузьких місць: моделі дають змогу виявити елементи або фази процесу, які мають найбільший вплив на загальну ефективність чи безпеку системи.

3) Підвищення обґрунтованості управлінських рішень: симуляція сценаріїв прийняття рішень дозволяє оцінити наслідки варіативних стратегій у контрольованому середовищі, що сприяє мінімізації ризиків і оптимізації ресурсів.

4) Гнучкість і адаптивність: моделі легко оновлюються у відповідь на зміну зовнішніх умов або структурних параметрів системи.

Агентне моделювання (agent-based modeling, ABM) – це один із сучасних підходів до симуляції складних адаптивних систем, в якому увага зосереджена не на макроскопічній поведінці системи в цілому, а на мікрорівні – через моделювання автономних агентів, що діють за певними правилами. Агент може бути будь-яким самостійним елементом системи –

людиною, підприємством, транспортним засобом, програмним ботом або навіть біологічною клітиною.

Головною перевагою АВМ є його здатність відображати складну, емерджентну (виникаючу з взаємодії елементів) поведінку систем, яка не завжди може бути передбачена класичними методами аналізу. Агентне моделювання особливо корисне там, де системи характеризуються високим ступенем гетерогенності, непередбачуваності, адаптивності та децентралізованості.

Ключові характеристики агентів:

1) Автономність – кожен агент функціонує незалежно, приймає рішення на основі власних правил, інформації та цілей.

2) Адаптивність – агенти мають здатність змінювати свою поведінку залежно від змін середовища або досвіду.

3) Гетерогенність – агенти можуть мати різні характеристики, що дозволяє моделювати соціальне різноманіття, різні типи споживачів, стратегії поведінки тощо.

4) Локальна взаємодія – більшість змін у моделі виникає внаслідок локальних взаємодій між агентами, що може породжувати глобальні ефекти (ефект мурашника, ринкові кризи, соціальні рухи тощо).

Приклади застосування агентного моделювання:

1) Соціальні науки: моделювання динаміки громадської думки, міграції, поширення інфекційних захворювань.

2) Економіка і ринки: симуляція поведінки споживачів, оцінка впливу ринкових стратегій на ціноутворення.

3) Кібербезпека: моделювання поведінки ботнетів або адаптивних систем захисту.

4) Транспорт: моделювання трафіку з урахуванням індивідуальної поведінки водіїв або автономних транспортних засобів.

5) Екологія: взаємодія популяцій у біосистемах або оцінка впливу діяльності людини на довкілля.

Агентне моделювання відрізняється від традиційних моделей тим, що не потребує глобального алгоритму управління всією системою. Поведінка системи є результатом взаємодії численних мікроагентів, що значно підвищує реалістичність та аналітичну гнучкість моделі.

Таблиця 3.3

Порівняння АВМ та системної динаміки

Критерій	Системна динаміка	Агентне моделювання
Рівень аналізу	Макрорівень	Мікро/мезорівень
Тип змінних	Сукупності	Індивідуальні агенти
Гнучкість поведінки	Обмежена	Висока
Модель взаємодії	Зумовлена структурою	Динамічна та емерджентна

Застосування агентного моделювання в ризик-менеджменті

Агентне моделювання (Agent-Based Modeling, ABM) дедалі активніше використовується в галузі управління ризиками завдяки своїй здатності відображати складні системи, у яких ключову роль відіграє людський фактор, автономна поведінка учасників системи та нелінійні сценарії розвитку подій. Особливу цінність ABM має для аналізу ризиків у складних соціотехнічних, інформаційних та фінансових системах, де динаміка процесів формується не централізованим управлінням, а численними локальними взаємодіями між агентами з різними мотиваціями, знаннями та можливостями.

Нижче розглянуто три ключові приклади застосування агентного моделювання в контексті ризик-менеджменту.

1. Моделювання поширення інформації / пліток у соціальних мережах

Одним із найактуальніших напрямів застосування ABM у сфері ризик-менеджменту є моделювання поширення інформації, дезінформації або пліток у цифрових соціальних середовищах. У таких моделях агенти виступають користувачами соціальних мереж, які обмінюються інформацією залежно від своїх уподобань, рівня довіри до джерела, попереднього досвіду та емоційного стану.

Особливості моделювання:

1) Гетерогенність агентів: користувачі мають різну чутливість до інформації, схильність до репостів або коментування.

2) Соціальні мережі як середовище взаємодії: мережа зв’язків (графи) моделює структуру взаємин, через які поширюється інформація.

3) Динаміка впливу: враховується зміна переконань або ставлення агентів до тієї чи іншої інформації залежно від її кількості та авторитетності джерела.

Значення для ризик-менеджменту:

1) Виявлення умов, за яких інформація стає вірусною або зупиняється.

2) Аналіз сценаріїв інформаційних атак (наприклад, у контексті кібергігієни чи гібридної війни).

3) Визначення ключових «інфлюенсерів», від поведінки яких залежить подальше поширення контенту.

4) Оцінка ризиків репутаційних втрат для організацій або державних структур.

2. Вивчення поведінки шахраїв у фінансових системах

Іншим надзвичайно важливим напрямом є агентне моделювання поведінки шахраїв (fraudsters) у фінансових системах, що дозволяє досліджувати механізми виникнення і розгортання шахрайських схем у банківській сфері, на фінансових біржах, у платіжних системах тощо.

Особливості моделювання:

1) Ролі агентів: система включає не лише звичайних користувачів, але й потенційних шахраїв, аналітиків безпеки, регуляторів.

2) Поведінкові стратегії: шахраї можуть змінювати тактики залежно від контрзаходів системи (реалізується принцип адаптивності).

3) Навчання агентів: моделі можуть включати елементи машинного навчання для моделювання еволюції шахрайських дій (наприклад, підбір шаблонів фішингу чи виведення коштів через ботоферми).

Значення для ризик-менеджменту:

1) Прогнозування сценаріїв реалізації шахрайських атак.

2) Визначення слабких місць у правилах верифікації транзакцій.

3) Тестування політик фінансової безпеки (наприклад, введення затримок, додаткових етапів перевірки).

4) Формування адаптивних алгоритмів виявлення шахрайської активності в реальному часі.

3. Аналіз реакцій користувачів на технічні інциденти

У критично важливих інфраструктурах, таких як енергетика, транспорт, IT-системи або охорона здоров'я, поведінка користувачів або операторів у разі технічних інцидентів (відмова системи, атака, катастрофа) може мати вирішальне значення для розвитку або локалізації кризи. Агентне моделювання дає змогу дослідити, як індивідуальні рішення й соціальні взаємодії впливають на загальну динаміку системи в умовах стресу, обмеженої інформації або паніки.

Особливості моделювання:

1) Роль часу: моделювання динаміки реакцій у режимі реального часу (секунди, хвилини).

2) Емоційна модель поведінки: агенти можуть реагувати емоційно – демонструвати страх, агресію, нерішучість.

3) Комунікаційні стратегії: вивчення впливу офіційних повідомлень, чуток або відсутності інформації на поведінку користувачів.

Значення для ризик-менеджменту:

1) Планування дій при надзвичайних ситуаціях, формування сценаріїв евакуації.

2) Оцінка ефективності стратегій кризових комунікацій.

3) Розробка рекомендацій щодо дизайну інтерфейсів і повідомлень, що зменшують паніку.

4) Аналіз потенційного ефекту доміно, коли нераціональна поведінка однієї групи агентів призводить до масштабної дестабілізації.

Агентне моделювання в ризик-менеджменті відкриває нові можливості для передбачення, ідентифікації та управління складними ризиками, які пов'язані не лише з технічними факторами, але й із соціальною поведінкою, інформаційними процесами та зловмисною активністю. Завдяки гнучкості АВМ можна моделювати як локальні сценарії, так і масштабні системні кризи, що робить цей підхід незамінним у стратегічному плануванні, кібербезпеці, кризовому управлінні та розробці політик стійкості систем.

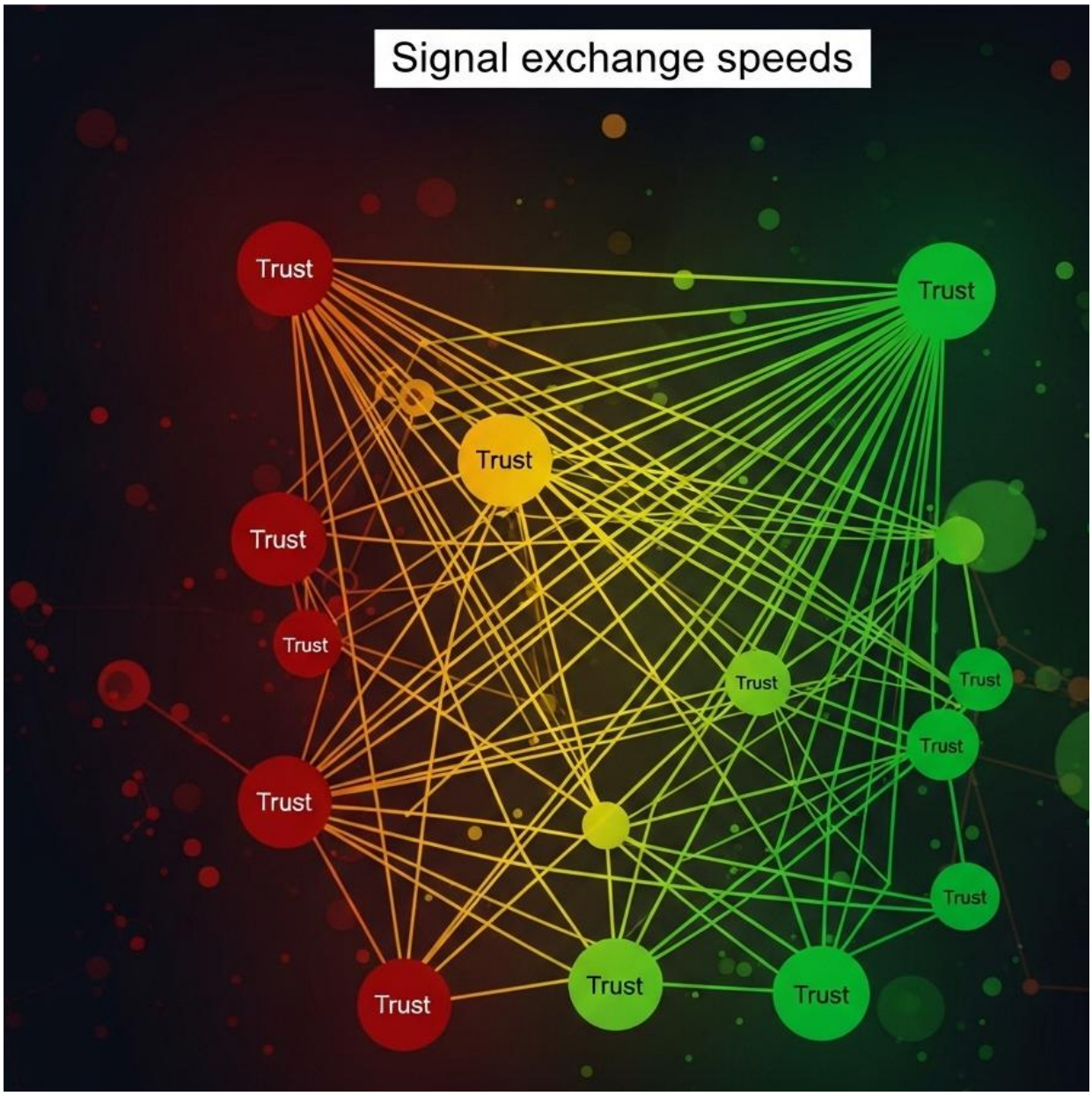

Рис.3.2. Агентна модель реагування на загрозу у розподіленій мережі
Ілюстрація: Агенти з різними рівнями довіри та швидкістю обміну сигналами

Моделювання ризиків в умовах динаміки та невизначеності потребує застосування міждисциплінарного підходу, який поєднує елементи математичного, системного, і поведінкового аналізу. У поєднанні, динамічні моделі, системна динаміка Форрестера, імітаційне та агентне моделювання дають змогу створити гнучкі інструменти для прогнозування, аналізу сценаріїв та підтримки прийняття рішень в умовах невизначеності.

У наступному підрозділі буде розглянуто практичне застосування цих підходів у моделюванні ризиків для критичної інфраструктури, фінансових систем та кібербезпеки.

3.2. Прогнозування за допомогою експертних та статистичних моделей

Прогнозування ризиків у сучасному системному середовищі є складним міждисциплінарним процесом, що потребує не лише аналізу поточних станів, але й глибокого розуміння прихованих змінних, трендів, поведінкових моделей і потенційних сценаріїв розвитку. Ризик у таких умовах розглядається як багатофакторна категорія, яка формується під впливом як зовнішніх умов, так і внутрішніх закономірностей функціонування системи. З огляду на це, для ефективного прогнозування небажаних подій застосовуються як **статистичні** (формальні) методи, так і **експертні** (неформальні, якісні) підходи, що в сукупності дозволяють створити адаптивну й обґрунтовану систему попередження ризиків.

Урахування динаміки змін та прихованих трендів

У системному аналізі ризиків важливо не лише фіксувати поточні значення параметрів, а й розуміти темп, напрямок і взаємозалежність їх змін у часі. Динаміка змін може містити латентні закономірності, які не проявляються у статичних зрізах, але відіграють критичну роль у виникненні системних збоїв чи катастроф.

Приховані тренди, наприклад, можуть виявляти накопичення відхилень у поведінці користувачів, технологічне старіння компонентів системи, деградацію продуктивності, зростання інформаційного навантаження тощо. Такі тенденції потребують інструментів математичного аналізу часових рядів та моделей, що враховують стохастичний характер змін.

Регресійні моделі як основа кількісного аналізу ризиків

Одним із базових підходів до прогнозування є регресійне моделювання, яке дозволяє встановити функціональні залежності між змінними – наприклад, між рівнем фінансової стабільності підприємства та кількістю виявлених технічних інцидентів, між навантаженням на систему та часом відповіді, між числом користувачів і ймовірністю збоїв.

Основні типи регресійних моделей:

– Лінійна регресія: проста оцінка ризиків за лінійною залежністю між фактором і результатом.

– Множинна регресія: одночасний аналіз кількох змінних для визначення їхнього спільного впливу.

– Логістична регресія: особливо корисна для прогнозування дискретних подій – наприклад, чи настане збій системи (1) чи ні (0).

Регресійні моделі дозволяють не лише робити кількісні прогнози, але й проводити чутливісний аналіз – виявляти, які змінні мають найбільший вплив на рівень ризику.

ARIMA та методи аналізу часових рядів

Іншим потужним інструментом прогнозування є моделі часових рядів, серед яких особливу увагу заслуговує модель ARIMA (AutoRegressive Integrated Moving Average).

Вона дозволяє враховувати: Автокореляції в даних (AR-компонент), Інтеграцію трендів (I-компонент), Рухомі середні (MA-компонент), що фіксують випадкові збурення у попередніх періодах.

Моделі ARIMA широко використовуються для прогнозування системного навантаження, динаміки виявлення загроз, витрат на обслуговування, частоти технічних інцидентів тощо. Їх перевага полягає в здатності працювати зі складними, нелінійними й сезонними рядами, особливо коли важливо передбачити часову динаміку ймовірності виникнення ризику.

Метод Делфі як інструмент експертного передбачення

У випадках, коли статистичних даних недостатньо, або ситуація характеризується високою невизначеністю, доцільним є застосування методу Делфі – структурованого методу збору думок від групи експертів. Цей метод дозволяє:

1) Отримати якісну оцінку ризиків, коли математичні моделі не можуть бути побудовані.

2) Врахувати думки фахівців із різних галузей, що забезпечує міждисциплінарний підхід.

3) Досягти консенсусу за допомогою кількох ітерацій опитування, з наданням анонімного зворотного зв’язку.

Метод Делфі ефективно застосовується в проектному управлінні, стратегічному прогнозуванні, розробці політик у сфері безпеки, особливо коли необхідно оцінити потенційні ризики впровадження інновацій або зміни зовнішніх регуляторних умов.

Системна оцінка достовірності побудованих моделей

Незалежно від використаного підходу (статистичного чи експертного), важливою складовою прогнозування є оцінка достовірності та валідації моделей. У системному середовищі це означає перевірку:

1) Адекватності моделі до реальних процесів (структурна відповідність).

2) Прогностичної точності (точність передбачень у різних часових інтервалах).

3) Стійкості до шуму (робастність при зміні вхідних параметрів).

4) Універсальності – чи можна модель застосувати до інших ситуацій або систем.

Серед методів валідації: Крос-валідація; Порівняння з історичними даними; Аналіз залишків (residual analysis); Використання індексу довіри до прогнозу, що комбінує математичну та експертну оцінку.

Комплексне прогнозування ризиків у складному системному середовищі потребує інтеграції формальних математичних методів (регресія, ARIMA, часові ряди) із неформальними експертними оцінками (метод Делфі). Такий підхід дозволяє не лише виявити ймовірність виникнення загроз, але й зрозуміти приховані механізми їх формування, адаптивно реагувати на нові ризики та будувати сценарії стратегічної стійкості. Важливим є не лише створення моделі, але й її регулярна перевірка,

уточнення та узгодження з поведінковими, економічними та технологічними характеристиками системи.

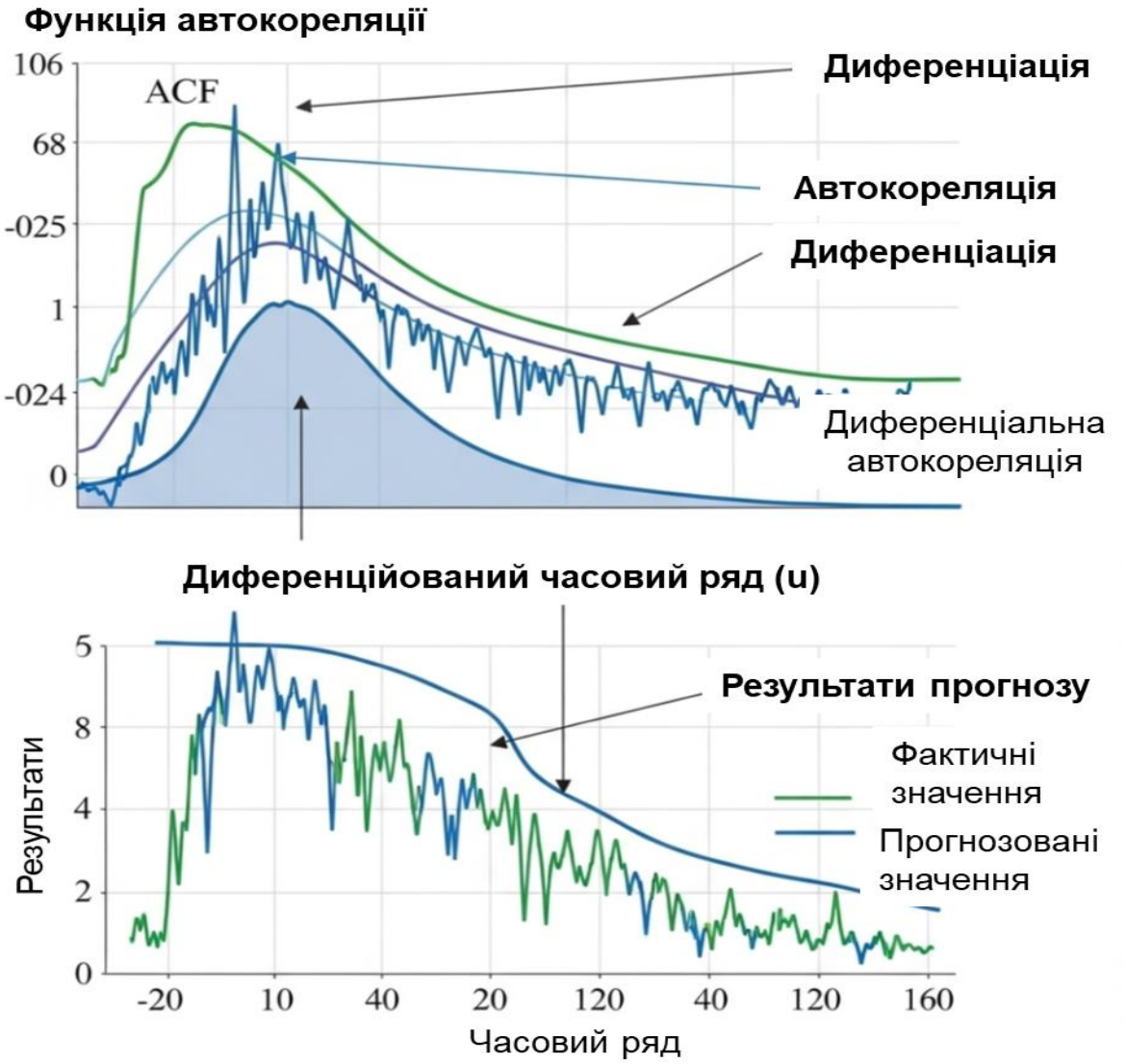

Рис. 3.3. Схема побудови ARIMA-моделі прогнозування ризику інцидентів
Графік: автокореляція, диференціювання, залишки прогнозу

Таблиця 3.4

Порівняння підходів

Метод	Основна перевага	Недоліки
Лінійна регресія	Простота і швидкість реалізації	Лінійність обмежує гнучкість
ARIMA	Підходить для нестаціонарних рядів	Складність калібрування параметрів
Часові тренди	Інтуїтивна інтерпретація	Схильність до сезонних збурень

Приклад застосування

Прогнозування кількості збоїв у мережі передачі даних за ARIMA(2,1,1) з урахуванням попередніх інцидентів та технічних оновлень. Отримані результати дозволяють розрахувати імовірність критичного навантаження на систему через 30 днів із точністю 85%.

Таблиця 3.5

Порівняння традиційного та модифікованого Делфі

Ознака	Класичний Делфі	Модифікований Делфі
Анонімність	Так	Так
Використання цифрових платформ	Ні	Так
Кількість раундів	3-4	Залежно від динаміки

Приклад

У дослідженні загроз для критичних інформаційних систем методом Делфі були залучені 25 експертів. У результаті трьох раундів було визначено 12 найбільш імовірних ризиків з пріоритетом за шкалою впливу.

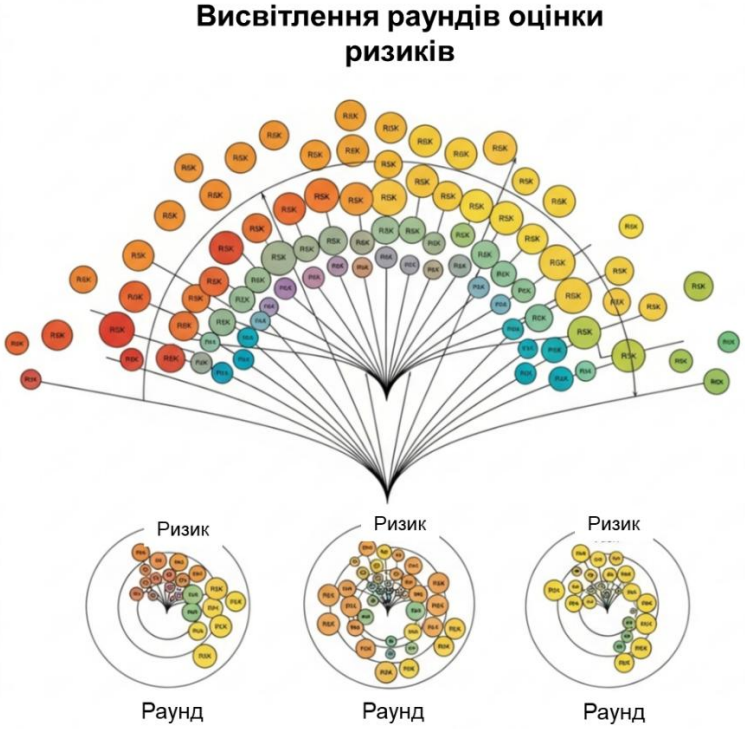

Рис. 3.4. Модель консенсусу в експертному середовищі
Діаграма: конвергенція оцінок ризиків протягом раундів

Оцінка достовірності моделей на основі системного підходу

У процесі побудови моделей прогнозування ризиків, подій чи станів у технічних, економічних або соціально-організаційних системах ключове значення має оцінка достовірності моделей. Недостатньо лише побудувати

модель, яка демонструє високу точність на навчальних даних – необхідно впевнитися, що вона надійно функціонує в умовах реального, змінного середовища та не призводить до хибних висновків або помилкових управлінських рішень. У цьому контексті системний підхід до оцінювання достовірності моделей стає основою для формування ефективної, надійної та адаптивної аналітичної інфраструктури.

Системний підхід передбачає розгляд моделі як компонента ширшої системи, в якій вона взаємодіє з різними елементами – даними, зовнішнім середовищем, користувачами, управлінськими цілями тощо. У такій парадигмі перевірка достовірності моделі включає не лише математичну валідацію, а й оцінку її поведінки в динаміці, гнучкість до змін, інтерпретованість результатів та здатність до адаптації. Лише такий всебічний аналіз дозволяє зменшити ризик помилкових інтерпретацій прогнозів та неефективних рішень.

Метрики точності: кількісні показники якості прогнозування

Для початкової, формальної оцінки точності моделей широко застосовуються метрики похибки, які відображають, наскільки прогнозовані значення відрізняються від фактичних. Серед них найпоширенішими є:

- MAE (Mean Absolute Error) – середня абсолютна похибка, яка вимірює середнє відхилення прогнозованих значень від фактичних незалежно від напрямку.

Формула: $MAE = (1/n) \sum |y_i - \hat{y}_i|$

Інтерпретація: Чим менше значення, тим точніша модель. Добре підходить для систем із помірною варіативністю.

- RMSE (Root Mean Square Error) – корінь із середньоквадратичної похибки, що акцентує увагу на великих відхиленнях через зведення похибки до квадрата.

Формула: $RMSE = \sqrt{(1/n) \sum (y_i - \hat{y}_i)^2}$

Інтерпретація: Більш чутлива до «викидів» і допомагає виявляти нестабільні або непридатні моделі в умовах зростання складності даних.

- MAPE (Mean Absolute Percentage Error) – середня абсолютна процентна похибка, яка виражає відхилення у відсотках, що особливо зручно для оцінки моделей у фінансах, логістиці та ресурсному плануванні.

Формула: $MAPE = (1/n) \sum (|y_i - \hat{y}_i| / y_i) \times 100\%$

Інтерпретація: Визначає, на скільки відсотків у середньому прогноз відрізняється від фактичного значення. Менше 10% – зазвичай вважається прийнятним рівнем для практики.

Ці метрики забезпечують базовий рівень валідації, однак вони не враховують динамічні та структурні аспекти функціонування моделей, особливо у складних системах із багатьма взаємозалежними параметрами.

Системні критерії оцінки достовірності: міжфункціональний аналіз моделей

Для забезпечення реальної надійності та застосовності моделей у складному середовищі, потрібне доповнення формальних метрик

системними критеріями, що дозволяють оцінити модель у контексті її стійкості, адаптивності та прозорості для користувача.

1. Адаптивність

Цей критерій відображає здатність моделі:

1) Оновлювати свої параметри в умовах зміни даних чи зовнішнього середовища;

2) Інтегрувати нові змінні або фактори, не порушуючи цілісності структури;

3) Автоматично перетреновуватись у відповідь на нові вхідні дані, що критично для систем реального часу.

Приклад: у фінансових системах ризику вартість активів змінюється щогодини, тому адаптивна модель повинна враховувати ці коливання автоматично, не вимагаючи ручного втручання.

2. Стійкість

Стійкість означає здатність моделі:

1) Зберігати адекватну точність навіть при незначних збуреннях у даних;

2) Не «переобучуватись» (overfitting) – тобто не втрачати загальну узагальнювальну здатність через надмірну чутливість до окремих патернів;

3) Функціонувати в умовах неповних або неточних даних.

Приклад: аналітична модель у кібербезпеці повинна залишатися ефективною, навіть якщо частина телеметричних даних тимчасово недоступна.

3. Інтерпретованість

Інтерпретованість передбачає:

1) Можливість логічно пояснити, як і чому модель зробила певний прогноз;

2) Надання візуалізованих причинно-наслідкових зв'язків або вагових коефіцієнтів;

3) Доступність для нефахівців – щоб управлінці або аналітики могли приймати рішення, розуміючи підґрунтя прогнозу.

Приклад: у медицині модель прогнозування діагнозу має не просто дати ймовірність захворювання, а й пояснити, які саме симптоми або фактори вплинули на таку оцінку.

Інтеграція метрик і системних критеріїв: комплексна схема оцінки

Для досягнення надійної, ефективної та застосовної у практиці моделі слід поєднувати формальні метрики точності з системними критеріями. Це дозволяє перейти від локальної оцінки математичної правильності до глобальної системної валідації, яка охоплює життєвий цикл моделі та її взаємодію з навколишнім середовищем.

Таблиця 3.6

Системні критерії оцінки достовірності

Критерій оцінки	Тип оцінки	Опис
MAE, RMSE, MAPE	Статистичний	Визначають середній ступінь похибки між прогнозом і фактом
Адаптивність	Системний	Відповідь моделі на зміну умов
Стійкість	Системний	Збереження ефективності при збуреннях
Інтерпретованість	Системний	Здатність пояснити прогноз користувачу

Оцінка достовірності моделей у системному підході – це не ізольований етап, а невід'ємна частина процесу побудови моделей, яка забезпечує їхню ефективність, адаптивність і практичну застосовність. Поєднання формальних метрик точності з системними критеріями дозволяє створювати моделі, стійкі до реальних викликів, зрозумілі для користувачів та здатні до самооновлення. Такий підхід формує основу для прийняття інформаційно обґрунтованих, а не евристичних управлінських рішень у складному, динамічному середовищі.

Таблиця 3.7

Комплексна оцінка моделей

Модель	MAE	RMSE	MAPE	Адаптивність	Інтерпретованість
Лінійна	12,4	15,6	9,2%	Середня	Висока
ARIMA	9,1	11,3	6,8%	Висока	Середня
Делфі	–	–	–	Залежить від оновлень	Висока

Рис. 3.5. Місце статистичної моделі у системному контурі прийняття рішень
Інфографіка: Модель → Оцінка → Вплив на політику управління ризиками → Зворотний зв'язок

Прогнозування ризиків у системному середовищі вимагає гармонійного поєднання кількісних і якісних моделей. Статистичні підходи, зокрема ARIMA та регресійні моделі, дозволяють формалізувати історичні закономірності, тоді як метод Делфі забезпечує інтеграцію експертних оцінок. Системна валідація моделей забезпечує їхню практичну цінність і стабільність у реальних умовах. У наступному підрозділі буде розглянуто поєднання гібридних підходів до прогнозування в умовах багатофакторної невизначеності.

3.3. Прогнозування ризиків з використанням штучного інтелекту

Сучасні методи прогнозування ризиків у складних системних середовищах дедалі активніше використовують потенціал штучного інтелекту (ШІ). Інтелектуальні алгоритми дозволяють моделювати, аналізувати та передбачати потенційні загрози, ґрунтуючись на історичних даних, виявлених патернах та адаптивних механізмах навчання. Цей підрозділ присвячений дослідженню ключових напрямів використання ШІ у прогнозуванні ризиків, а саме нейронним мережам і глибокому навчанню, машинному навчанню для розпізнавання ризикових патернів, а також інтеграції AI у системи підтримки прийняття рішень (СППР).

Нейронні мережі та глибоке навчання

Нейронні мережі – це клас моделей машинного навчання, натхненний структурою та функціонуванням біологічного мозку. У контексті прогнозування ризиків, вони демонструють високу ефективність у виявленні складних закономірностей та латентних залежностей у великих масивах даних.

Таблиця 3.7

Архітектури нейронних мереж

Тип мережі	Сфера застосування	Особливості
Feedforward Neural Networks (FNN)	Класичне прогнозування	Пряма передача сигналу між шарами
Recurrent Neural Networks (RNN)	Аналіз часових рядів	Зворотні зв'язки дозволяють враховувати попередні стани
Long Short-Term Memory (LSTM)	Прогнозування з довготривалими залежностями	Ефективна робота з великими часовими послідовностями
Convolutional Neural Networks (CNN)	Просторовий аналіз ризиків	Часто використовуються для обробки структурованих даних

Приклад: Застосування LSTM у кібербезпеці

LSTM-мережі використовуються для виявлення аномальної поведінки в мережевих логах. Навчаючись на нормальному трафіку, модель може передбачати нормальні послідовності дій, а відхилення сигналізують про можливу загрозу.

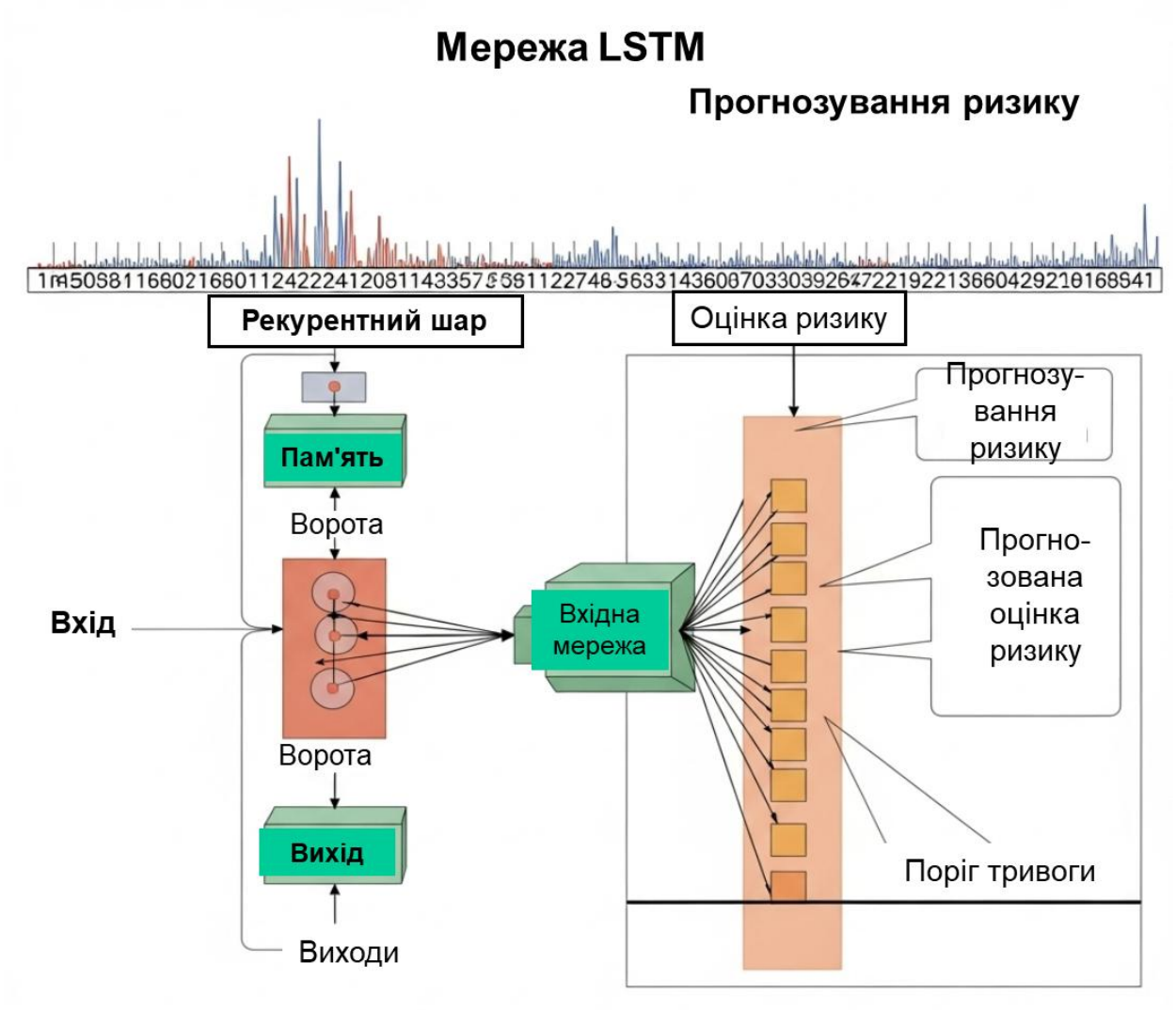

Рис. 3.6. Архітектура LSTM для прогнозування мережевих загроз
[Графік: Структура мережі LSTM з входами на часовій шкалі, передбаченням ризику та порогом тривоги.]

Машинне навчання для розпізнавання ризикових патернів

Машинне навчання (ML) – це підхід до ШІ, який дозволяє системам автоматично навчатися з даних та вдосконалювати свої прогнози без жорстко запрограмованих інструкцій. У системному аналізі ML забезпечує автоматичну класифікацію, кластеризацію та регресійне моделювання ризиків.

Таблиця 3.8

Класифікація методів машинного навчання

Тип ML	Алгоритми	Використання у прогнозуванні ризиків
Навчання з учителем	Decision Trees, SVM, Random Forest	Прогнозування фінансових та технічних ризиків
Навчання без учителя	K-Means, DBSCAN	Виявлення нових типів загроз, кластеризація інцидентів
Напівкероване навчання	Self-training, Co-training	Аналіз даних з обмеженим маркуванням
Підкріплювальне навчання	Q-learning, Deep Q Networks	Динамічне управління ризиками в реальному часі

Приклад: Виявлення шахрайства в банківській системі

Моделі Random Forest або Gradient Boosting навчаються на історичних транзакціях, класифікуючи їх як «нормальні» чи «ризикові». Навчання моделі враховує десятки ознак – геолокацію, час, суму, тип транзакції.

Таблиця 3.9

Порівняння точності алгоритмів ML для виявлення фінансового шахрайства

Алгоритм	Точність	Повнота	F-міра
Logistic Regression	84%	76%	0,79
Random Forest	92%	89%	0,90
Gradient Boosting	94%	91%	0,92

Інтеграція AI у системи підтримки прийняття рішень: концепція, архітектура та перспективи застосування

У сучасному світі, де обсяги даних зростають експоненційно, а системи управління функціонують в умовах високої складності й невизначеності, системи підтримки прийняття рішень (СППР) стають незамінними інструментами для ефективного функціонування соціотехнічних структур. Зокрема, інтеграція штучного інтелекту (ШІ) до таких систем відкриває нові горизонти в управлінні ризиками, дозволяючи не лише автоматизувати обробку великої кількості даних, а й генерувати адаптивні, обґрунтовані та контекстно залежні управлінські рішення**.**

ШІ суттєво трансформує логіку функціонування СППР, переходячи від традиційного алгоритмічного мислення до інтелектуального аналізу патернів, ситуаційного прогнозування та самонавчання на основі нових вхідних даних. Це, у свою чергу, забезпечує проактивну взаємодію з динамічним середовищем, зменшуючи ймовірність помилкових рішень та посилюючи стійкість систем до непередбачуваних подій.

Моделі інтеграції ШІ у СППР: типологія і приклади реалізації

Існує кілька підходів до побудови інтегрованих СППР з компонентами штучного інтелекту, кожен з яких відповідає різному рівню складності задачі, обсягу даних і необхідного ступеня автономності системи. Найбільш поширені моделі включають:

1. Експертні системи. Ці системи базуються на заздалегідь сформульованих правилах, які розробляються експертами в певній предметній галузі. Правила представляють собою набір умов і відповідних дій («якщо–то» логіка), що дозволяє відтворити процес мислення фахівця. Хоча експертні системи не володіють адаптивністю ШІ, вони забезпечують високу інтерпретованість та прозорість логіки прийняття рішень. Вони залишаються релевантними в умовах стабільного середовища або для вирішення вузько спеціалізованих задач.

2. Гібридні СППР. Це багаторівневі системи, які поєднують нейромережеві компоненти (глибоке навчання, машинне навчання) з класичними логічними правилами. Завдяки такому підходу, гібридні СППР поєднують адаптивність і здатність до самонавчання з пояснюваністю та чіткою структурою ухвалення рішень. Наприклад, нейромережа може прогнозувати ймовірність події (наприклад, затоплення або кіберзагрози), а логічна підсистема – формувати рішення щодо подальших дій залежно від рівня загрози.

3. Автономні агенти. Це програмні інтелектуальні агенти, які здатні до автономного функціонування в динамічному середовищі, навчаючись в процесі експлуатації. Такі агенти використовують методи підкріпленого навчання (reinforcement learning), еволюційних алгоритмів та багатокритеріальної оптимізації. Вони є особливо ефективними в ситуаціях, коли середовище змінюється швидко та непередбачувано (наприклад, у фінансових ринках, під час кіберінцидентів або в умовах надзвичайних ситуацій).

Приклад інтеграції AI у системи управління надзвичайними ситуаціями

Одним із найбільш яскравих прикладів інтеграції ШІ у СППР є системи, які забезпечують прогнозування та реагування на надзвичайні ситуації, зокрема природні катастрофи. При аналізі ризику затоплень сучасні СППР можуть:

1) отримувати вхідні дані з метеорологічних сенсорів у реальному часі;
2) обробляти геоінформаційні дані (карти рельєфу, гідрологічні дані);
3) використовувати алгоритми машинного навчання для побудови моделей затоплення на основі історичних подій і сценаріїв;
4) формувати автоматизовані сценарії евакуації для населення залежно від рівня води, часу доби, щільності населення тощо.

Це не лише підвищує ефективність реагування на катастрофи, але й дозволяє приймати превентивні рішення до настання критичного моменту.

Переваги інтеграції AI у СППР: функціональна та стратегічна ефективність

Інтеграція інтелектуальних технологій у СППР забезпечує цілий спектр переваг:

1) Швидкість обробки інформації**:** сучасні алгоритми дозволяють аналізувати великі масиви даних (Big Data) у реальному часі, суттєво знижуючи час на ухвалення рішень у критичних ситуаціях.

2) Адаптивність: алгоритми машинного навчання здатні до навчання на нових патернах, що забезпечує їх актуальність і здатність до самовдосконалення без ручного втручання.

3) Контекстність: ШІ може враховувати складний набір факторів і змінних, що формують ситуацію, зокрема часові, просторові, соціальні та економічні характеристики середовища.

4) Аналітична прозорість (у разі використання explainable AI): користувач може отримати пояснення щодо обґрунтованості прийнятих рішень, що підвищує довіру до системи.

Штучний інтелект і прогнозування ризиків: синергія з системним аналізом

Застосування ШІ в рамках СППР дає змогу реалізувати нову парадигму системного аналізу ризиків, яка поєднує:

- автоматизоване виявлення трендів і відхилень;
- класифікацію та оцінку критичності сценаріїв розвитку подій;
- генерацію альтернативних рішень з урахуванням невизначеності;
- постійне уточнення моделей на основі реальних результатів.

Таке поєднання перетворює СППР з інструменту реактивного управління на проактивну інтелектуальну платформу, здатну передбачити ризики ще до їхнього виникнення.

Виклики та вектори подальших досліджень

Попри значні досягнення у сфері інтеграції ШІ в СППР, існують важливі проблеми, що потребують глибокого вивчення:

1) Етичність: необхідність створення прозорих і справедливих алгоритмів, що не дискримінують користувачів або групи населення.

2) Інтерпретованість: пояснюваність моделей є ключовою умовою довіри до ШІ, особливо у сферах, де рішення мають критичні наслідки (медицина, оборона, управління катастрофами).

3) Надійність і відмовостійкість: системи повинні демонструвати стабільну роботу у змінних, стресових умовах і мати вбудовані механізми контролю помилок.

4) Інтеграція в реальному часі**:** здатність до швидкої реакції на зміну середовища потребує оптимізації алгоритмів для обробки потокових даних з мінімальною затримкою.

Інтеграція штучного інтелекту у системи підтримки прийняття рішень є не просто технічною модернізацією, а стратегічним кроком до створення нового типу інтелектуальних управлінських систем, які здатні адаптуватися до викликів майбутнього. Уміння працювати з динамікою ризиків, швидко приймати обґрунтовані рішення та забезпечувати пояснюваність результатів стає основою стійкого розвитку складних організацій і суспільств загалом.

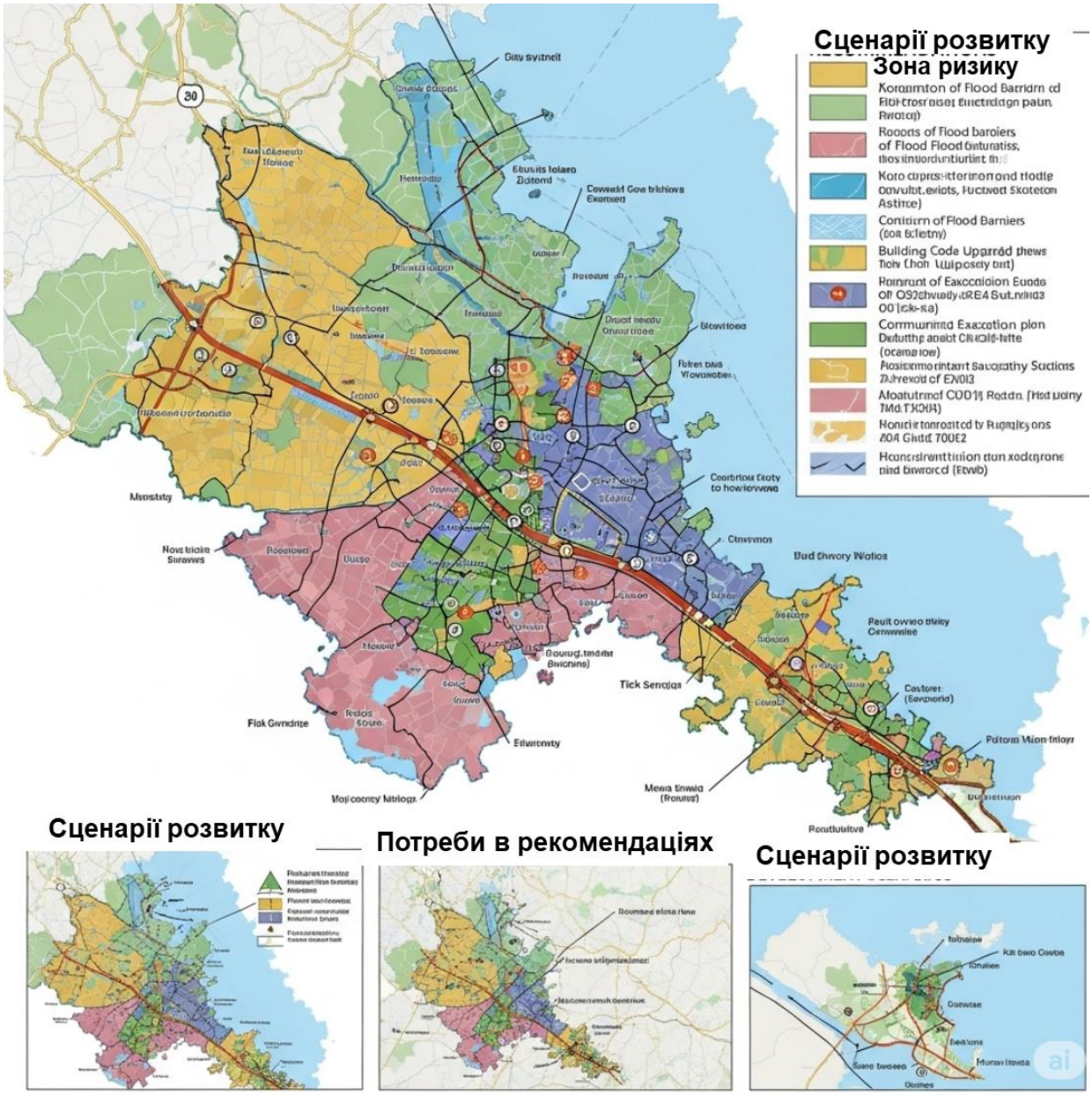

Рис. 3.7. Інтерфейс СППР із вбудованим AI-модулем прогнозування ризиків Графіка: Карта регіону з позначеними зонами ризику, рекомендаціями та сценаріями розвитку подій.]

Таблиця 3.10

Порівняння традиційних та AI-орієнтованих СППР

Характеристика	Традиційна СППР	AI-орієнтована СППР
Швидкість адаптації	Низька	Висока
Обсяг даних	Обмежений	Великі масиви
Автоматичне оновлення моделей	Ні	Так
Рівень автономності	Обмежений	Високий

3.4. Інформаційні системи та цифрові платформи моніторингу ризиків

Інформаційні системи та цифрові платформи моніторингу ризиків сьогодні відіграють ключову роль у забезпеченні стійкості організацій до внутрішніх та зовнішніх загроз. Застосування цифрових двійників (Digital Twins), сенсорного аналізу в IoT-середовищі, а також візуалізація даних через інтерактивні панелі управління (dashboards) і карти теплових зон (heatmaps) дозволяє створити гнучкі, адаптивні та прогностичні середовища прийняття рішень.

1. Цифрові двійники (Digital Twins) та ризик-інтерфейси

У сучасних умовах цифрової трансформації та зростання складності соціотехнічних систем з'являється гостра потреба у більш точних, гнучких та інтегрованих підходах до моніторингу, прогнозування і управління ризиками. Однією з ключових інноваційних технологій у цьому напрямі є концепція цифрового двійника (Digital Twin) – цифрової репрезентації фізичного об'єкта, процесу або складної системи, яка здатна не лише відображати поточний стан системи в реальному часі, а й моделювати її майбутню поведінку на основі різноманітних сценаріїв ризику.

Цифровий двійник – це динамічна комп'ютерна модель, що відображає фізичну сутність з високим ступенем точності. На відміну від традиційних моделей, цифровий двійник функціонує на базі постійно оновлюваних даних, що надходять від сенсорів, лічильників, телеметричних систем тощо. Завдяки цьому забезпечується актуалізація цифрової копії в реальному часі, що надає широкі можливості для візуалізації, аналізу та прийняття рішень у контексті ризик-менеджменту.

Ключові функції цифрових двійників включають: Моніторинг у реальному часі: постійне відстеження параметрів функціонування об'єкта. Прогнозування подій: моделювання можливих станів системи на основі аналізу даних. Імітація ризикових сценаріїв: перевірка системи на стійкість до гіпотетичних загроз. Оптимізація процесів: вдосконалення процедур та операцій на основі цифрових експериментів.

Основні характеристики цифрових двійників у контексті управління ризиками

1. Динамічне оновлення стану об'єкта на основі сенсорних даних Цифровий двійник не є статичною копією системи, а функціонує як жива модель, яка оновлюється в режимі реального часу. Завдяки використанню IoT-сенсорів та телеметрії, двійник отримує безперервний потік даних (температура, тиск, вібрації, навантаження, швидкість тощо), що дозволяє оперативно виявляти аномалії, прогнозувати відмови, виявляти приховані ризики. Такі властивості є критично важливими для систем з підвищеною складністю та високою вартістю помилок, зокрема у критичній інфраструктурі, авіації, енергетиці.

2. Можливість імітаційного моделювання ризикових сценаріїв Однією з ключових функцій цифрового двійника є здатність виконувати

імітаційні експерименти: тестування впливу різних факторів ризику, таких як вихід з ладу компонентів, зовнішні атаки, зміна параметрів середовища тощо. Це дозволяє не лише оцінити потенційні наслідки, а й підготувати ефективні стратегії реагування. Наприклад, цифровий двійник енергосистеми може змоделювати сценарій перевантаження мережі через масове використання побутової техніки в пікові години та запропонувати оптимальну схему перерозподілу навантаження.

3. Підтримка рішень через ризик-інтерфейси. Ризик-інтерфейси – це інтерактивні модулі в цифровому двійнику, які забезпечують візуалізацію, оцінювання та управління ризиками.

Вони дозволяють:

– виявляти уразливі місця в системі;

– пріоритизувати ризики за ступенем ймовірності та серйозності наслідків;

– прогнозувати ефективність превентивних заходів;

– генерувати рекомендації для управлінського персоналу у форматі інтерактивних панелей, карт ризиків або сценарних матриць.

Приклади використання цифрових двійників із ризик-інтерфейсами

1. У промисловості: У сучасному машинобудуванні та енергетиці цифрові двійники широко застосовуються для прогнозування технічного зносу компонентів обладнання. Наприклад, цифровий двійник газової турбіни збирає дані про вібрації, температуру підшипників та кількість запусків. На основі цих даних система прогнозує імовірний час відмови критичних компонентів, пропонуючи оптимальний час технічного обслуговування або заміни.

2. У логістиці: У логістичних мережах цифрові двійники дозволяють створювати динамічне віддзеркалення транспортної системи, включаючи маршрути, склади, пункти контролю, погодні умови та інші змінні. Ризик-інтерфейси в таких системах дають змогу: аналізувати ризики затримок поставок через погодні умови чи логістичні затори; моделювати альтернативні маршрути; прогнозувати вплив подій (аварії, карантинні обмеження тощо) на постачальні ланцюги; здійснювати адаптивне перепланування маршрутів у реальному часі.

Стратегічні переваги впровадження цифрових двійників з ризик-орієнтованими функціями

1) Підвищення прозорості системи: управлінці отримують чітке розуміння реального стану об’єкта та можливих загроз.

2) Покращення якості управлінських рішень: імітація дозволяє протестувати стратегії до їх фактичного впровадження.

3) Оптимізація витрат: завчасне виявлення відхилень дає змогу зменшити витрати на аварійне обслуговування.

4) Формування культури проактивного ризик-менеджменту: цифрові двійники сприяють переходу від реактивного до превентивного стилю управління.

Таблиця 3.11

Приклад реалізації

Компонент цифрового двійника	Функція	Джерело даних
Сенсорна мережа	Збір даних про стан	IoT-девайси
Аналітичне ядро	Оцінка ризиків, прогнозування	Моделі машинного навчання
Візуалізація	Інтерфейс керування та моніторингу	Dashboards/AR-інтерфейси

Рис. 3.8. Граф: Взаємодія між реальним об’єктом та цифровим двійником [СХЕМА: Digital Twin Architecture – фізична система ↔ сенсори ↔ аналітика ↔ інтерфейс управління].

Перспективи розвитку

Очікується, що подальший розвиток цифрових двійників буде тісно інтегрований з технологіями штучного інтелекту, великих даних (Big Data), edge computing та 5G, що дозволить значно розширити їх функціональність. Особливу увагу науковці та інженери приділяють розробці самонавчальних

цифрових двійників, які зможуть адаптуватися до нових умов без потреби в ручному налаштуванні моделей. Також важливим напрямом є забезпечення етичності та інтерпретованості рішень, які генеруються в рамках ризик-інтерфейсів.

2. IoT-середовище та сенсорний аналіз у прогнозуванні ризиків

У сучасному світі, де технічні системи взаємодіють з фізичним середовищем у реальному часі, ключову роль у прогнозуванні ризиків відіграє Інтернет речей (Internet of Things, IoT). IoT-середовище дозволяє формувати динамічну, інтегровану систему, яка здатна постійно здійснювати моніторинг, збір і передавання даних з різних джерел, включно з технічними об’єктами, інфраструктурними вузлами та середовищем функціонування системи.

Центральною особливістю IoT у контексті безпеки є можливість континуального (неперервного) збору даних із фізичних та кіберфізичних об’єктів, що надає підґрунтя для ідентифікації аномалій, які можуть свідчити про настання ризиків. Наприклад, навіть незначне коливання температури, вібрацій, тиску чи рівня енерговитрат може свідчити про майбутній збій у технічній системі або спробу несанкціонованого втручання.

Таким чином, IoT виступає не лише як інструмент фіксації стану системи, а й як передумова створення адаптивних систем попередження та реагування на ризики, які працюють у реальному часі.

IoT-архітектура для аналізу ризиків

Функціонування IoT у контексті аналізу ризиків базується на чітко структурованій архітектурі, яка охоплює кілька ключових етапів:

1. Збір даних (сенсори).

Перший рівень IoT-архітектури передбачає розгортання сенсорної інфраструктури, яка виконує функцію первинного збору даних. Сенсори можуть бути різних типів:

1) Фізичні: для вимірювання температури, вологості, тиску, вібрацій, рівня шуму, концентрації газів, тощо.

2) Кіберфізичні: сенсори, інтегровані в складні системи, що поєднують програмне та апаратне забезпечення (наприклад, в автоматизованих виробництвах).

3) Біометричні: у безпекових системах для моніторингу фізіологічних параметрів персоналу або доступу.

4) Сенсори руху та позиціонування: виявляють переміщення об'єктів, що важливо для охорони периметрів або логістичних систем.

Сенсори є джерелами сирих, первинних даних, які у необробленому вигляді не мають аналітичної цінності, проте забезпечують базову інформацію для формування цифрового профілю системи.

2. Передача (протоколи MQTT, CoAP)

Після фіксації параметрів середовища або технічного об’єкта, дані передаються далі за допомогою легковагових комунікаційних протоколів, адаптованих до IoT-середовищ, таких як:

1) MQTT (Message Queuing Telemetry Transport) – протокол публікації/підписки, який використовується в умовах обмежених ресурсів та нестабільного каналу зв'язку. Ідеально підходить для середовищ з великою кількістю розподілених сенсорів.

2) CoAP (Constrained Application Protocol) – орієнтований на системи з обмеженою обчислювальною потужністю. Відзначається компактністю, підтримкою REST-моделі та зручністю інтеграції у мобільні системи.

Ці протоколи забезпечують надійну, енергоефективну та масштабовану передачу інформації, що критично важливо для своєчасного аналізу та прогнозування ризиків у розподілених технічних системах.

3. Обробка (Edge/Cloud Computing)

Зібрані дані потребують оперативної обробки та аналізу, що реалізується двома основними підходами:

1) Edge Computing – обробка даних відбувається безпосередньо на пристроях або вузлах, наближених до сенсорів (edge-нодах). Це дозволяє зменшити затримки, знизити навантаження на мережу, а також підвищити рівень безпеки за рахунок локальної фільтрації даних.

2) Cloud Computing – передбачає передавання даних на хмарні сервери, де відбувається їх глибокий аналіз, зберігання, порівняння з історичними патернами, виявлення довготривалих тенденцій та формування звітів.

У складних сценаріях безпеки застосовується гібридна модель, де критично важливі сигнали обробляються на edge-рівні (для миттєвого реагування), а стратегічний аналіз виконується у хмарі.

4. Інтеграція в платформу моніторингу

Останнім етапом є інтеграція всіх процесів у єдину систему моніторингу ризиків, яка дозволяє: Візуалізувати стан систем у реальному часі. Генерувати тривожні сигнали при виявленні аномалій. Формувати прогностичні моделі на основі машинного навчання. Автоматизувати процеси реагування на ризики. Забезпечити аудит та історичний аналіз інцидентів.

Такі платформи можуть бути частиною централізованих SCADA-систем, інтелектуальних рішень безпеки або платформ кіберфізичної безпеки. Вони використовують потужні аналітичні рушії, алгоритми кореляції подій, нейронні мережі для прогнозування та оцінювання рівня ризиків у контексті конкретних ситуацій.

IoT-архітектура у поєднанні з сенсорним аналізом формує нову парадигму забезпечення технічної безпеки, де основна увага зосереджена на прогнозуванні, ранньому попередженні та адаптивному реагуванні. Впровадження таких рішень дозволяє переходити від реактивної моделі управління безпекою до проактивного, інтелектуального захисту, що забезпечує стійкість систем в умовах зростаючої складності загроз і технологічного середовища.

Таблиця 3.12

Типи сенсорів та застосування

Тип сенсора	Система	Моніторингові ризики
Температурні	Виробництво	Перегрів обладнання
Гази/Хімічні	Екологія	Забруднення повітря
Вібраційні	Механіка	Механічні пошкодження
GPS	Логістика	Втрата маршруту

Таблиця 3.13

Порівняння хмарного і крайового аналізу

Параметр	Хмарна обробка (Cloud)	Крайова обробка (Edge)
Затримка (latency)	Вища	Низька
Обсяг обробки	Масштабований	Локалізований
Безпека	Централізована	Локальна

Візуалізація системних ризиків: dashboards, heatmaps

У сучасних інформаційно-аналітичних системах управління ризиками візуалізація відіграє фундаментальну роль. Вона є не лише інструментом представлення інформації, але й ефективним засобом виявлення прихованих закономірностей, аномалій та трендів, які можуть залишитися непоміченими у вигляді табличних даних або традиційних звітів.

Особливої актуальності візуалізація набуває у сфері системного аналізу ризиків, де обсяги даних зростають експоненційно, а характер загроз ускладнюється. Завдяки сучасним інструментам візуального аналізу – інтерактивним панелям керування (dashboards) та тепловим картам (heatmaps) – аналітики, менеджери та керівники отримують можливість швидко інтерпретувати ситуацію, оцінювати динаміку змін, приймати обґрунтовані управлінські рішення в умовах невизначеності.

Узагальнено, візуалізація в аналітиці ризиків виконує декілька критичних функцій: Сприяє когнітивному сприйняттю складної інформації: Візуальні образи активують механізми обробки даних у мозку швидше, ніж текст або таблиці. Допомагає виявляти патерни та кореляції: Візуалізовані тренди, кластери та аномалії наочно ідентифікують системні загрози. Забезпечує прозорість управлінських рішень: Візуально відображені ризики дозволяють керівництву обґрунтовано визначати пріоритети реагування. Сприяє колективному розумінню: Інтерактивні панелі дозволяють різним підрозділам спільно аналізувати ризики та координувати дії.

Dashboards, або панелі моніторингу ризиків, є інтегрованими аналітичними інтерфейсами, які дозволяють в реальному часі відслідковувати стан системи безпеки, контролювати ключові індикатори ризиків та оперативно реагувати на відхилення.

Приклад структури типового risk-dashboard:

1. Основна панель з ключовими індикаторами ризиків (KRI – Key Risk Indicators)

У цій частині відображаються агреговані метрики, що вказують на рівень поточних ризиків. Це можуть бути: Індекс кіберзагроз. Частота збоїв критичних систем. Середній час реагування на інциденти. Індикатори відхилень у роботі технічної інфраструктури, візуально вони представлені у вигляді лічильників, кругових діаграм або індикаторів рівня. Динамічні графіки трендів ризиків. Цей блок демонструє часову динаміку ключових параметрів ризику, що дозволяє виявляти: Зростання чи спад активності загроз. Повторюваність аномальних подій. Вплив зовнішніх чинників на рівень ризику (наприклад, сезонні фактори, економічні події). Тут доцільно застосовувати лінійні графіки, гістограми, діаграми залежностей. Інтерактивна карта подій/аномалій.

На карті геоприв'язки або топології об’єктів відображаються: Географічне розташування інцидентів. Інтенсивність проявів ризиків. Зони концентрації критичних подій. Користувач може клікнути по області карти, щоб отримати розширену інформацію – це суттєво полегшує геопросторовий аналіз системних вразливостей.

2. Фільтри по типам ризиків, підрозділам, часовим періодам. Інтерактивні фільтри дають змогу гнучко налаштовувати подання даних, зокрема: Переглядати лише операційні, технічні або кіберризики. Оцінювати ризики конкретного підрозділу або об’єкта. Порівнювати динаміку ризиків у різні періоди часу. Така фільтрація сприяє локалізації проблем та адресному прийняттю рішень.

Heatmaps є ще одним потужним візуальним інструментом у сфері системного управління ризиками. Вони дозволяють виявляти зони підвищеного ризику завдяки кольоровому кодуванню інтенсивності проявів ризиків у тій чи іншій області системи.

Основні характеристики heatmaps у контексті ризик-аналізу:

1) Градація кольору відображає ступінь ризику: Наприклад, червоний – критичний ризик, жовтий – середній, зелений – допустимий.

2) Матричне представлення ймовірності та впливу: Найчастіше використовуються у вигляді двовимірної матриці «Імовірність × Наслідки», де кожна клітинка показує інтегральний ризик.

3) Секторна деталізація: Heatmap може бути розподілена за секторами – технічними зонами, інформаційними потоками, об’єктами інфраструктури.

4) Динамічні карти з часовою віссю: Дозволяють простежити, як змінювався рівень ризику у конкретній зоні або системі з плином часу.

Heatmaps використовуються для пріоритезації заходів управління ризиками, розробки планів реагування, а також для аудиту стану безпеки на основі історичних даних.

Інструменти dashboards та heatmaps у контексті управління ризиками забезпечують: Швидке виявлення критичних ситуацій. Підвищення оперативності реагування. Формування візуальної звітності для керівництва.

Уніфікацію даних з різних джерел в одному інтерфейсі. Підтримку стратегічного планування та прогнозування ризиків.

Інтеграція інструментів візуалізації у систему управління ризиками є не лише технологічною перевагою, а й стратегічною необхідністю. Dashboards та heatmaps трансформують великі масиви даних у зрозумілу та дієву інформацію, що дозволяє будувати ефективну модель прийняття рішень, забезпечуючи проактивний, гнучкий і адаптивний підхід до управління ризиками у складних технічних системах.

Таблиця 3.14

Таблиця типи візуалізацій

Тип інструменту	Функція	Приклад використання
Dashboards	Огляд показників у реальному часі	SCADA-системи
Heatmaps	Інтенсивність ризиків по зонах	Кібератаки в мережі
KPI-індикатори	Візуальна оцінка досягнення цілей	Ризики невиконання SLA

Інтеграція платформ моніторингу у системний аналіз

Платформи моніторингу ризиків стають невід'ємною частиною системного середовища управління організаціями. Їх інтеграція дозволяє: Створити єдиний інформаційний простір аналізу та реагування. Використовувати автоматизовані сценарії дій при виявленні ризику. Забезпечити документацію ризикових подій та навчання систем на основі історичних даних.

Таблиця 3.15

Популярні цифрові платформи

Платформа	Характеристика	Функції
Splunk	Big Data аналіз ризиків	Реальний час, алерти, ML
IBM QRadar	Кібербезпека	Аналіз логів, кореляція подій
Siemens Mindsphere	Промислова IoT	Підключення цифрових двійників
Microsoft Azure IoT Central	Хмара + аналітика	Аналітика на базі моделей ML

Інформаційні системи моніторингу ризиків трансформують процеси прогнозування, роблячи їх інтерактивними, адаптивними та стійкими. Інтеграція Digital Twins, IoT, візуальних інтерфейсів та аналітичних платформ створює нову парадигму системного аналізу ризиків. В умовах швидкоплинних ризик-орієнтованих середовищ такі технології стають незамінними інструментами стратегічного управління.

Контрольні питання

1. Що таке динамічна система та як часові лаги впливають на моделювання ризиків?
2. Яким чином використовується системна динаміка Форрестера у виявленні ризиків?
3. Поясніть поняття «петлі зворотного зв’язку» в контексті системного моделювання.
4. У чому полягає відмінність між імітаційним та агентним моделюванням ризиків?
5. Як імітаційне моделювання допомагає аналізувати поведінку системи в умовах невизначеності?
6. Наведіть приклади застосування агентного моделювання для прогнозування ризиків у складних системах.
7. Які переваги використання динамічних моделей у порівнянні з класичними підходами до оцінки ризиків?
8. Які основні особливості регресійних моделей у прогнозуванні ризиків?
9. Що таке модель ARIMA та як вона використовується для аналізу часових рядів?
10. У чому полягає сутність підходу аналізу часових рядів у прогнозуванні ризиків?
11. Охарактеризуйте метод Делфі та його значення для експертного оцінювання ризиків.
12. Які етапи включає процедура проведення опитування за методом Делфі?
13. Як оцінюється достовірність прогнозних моделей на основі системного підходу?
14. Які обмеження мають статистичні моделі у сфері прогнозування ризиків?
15. Які типи нейронних мереж використовуються у сфері прогнозування ризиків?
16. Як глибоке навчання застосовується для обробки великих обсягів ризик-орієнтованих даних?
17. Які задачі машинного навчання є найбільш релевантними для ідентифікації ризиків?
18. Наведіть приклади алгоритмів машинного навчання, які успішно застосовуються для виявлення ризикових патернів.
19. Які основні переваги використання AI у системах підтримки прийняття рішень у ризик-менеджменті?
20. Як здійснюється інтеграція систем штучного інтелекту у традиційні моделі оцінки ризиків?
21. Які ризики пов’язані із застосуванням AI у прогнозуванні ризиків?
22. Що таке цифровий двійник (Digital Twin) та яку роль він відіграє у моніторингу ризиків?
23. Які особливості має IoT-середовище для ідентифікації та передбачення технічних ризиків?

24. У чому полягає значення сенсорного аналізу в системах моніторингу ризиків?
25. Які візуальні інструменти (dashboards, heatmaps) найефективніші для представлення системних ризиків?

Кейси до розділу 3

Кейс 1. Прогнозування ризиків в умовах динамічної зміни параметрів технічної системи

В умовах експлуатації гідротехнічної споруди було зафіксовано коливання рівня води, пов’язані з кліматичними змінами. Через це виникає ризик переливу, а згодом — техногенної аварії.

Використовуючи методи моделювання в динамічному середовищі, сформуйте математичну модель змін параметрів (наприклад, рівень води, швидкість течії, навантаження). Застосуйте принципи системної динаміки для прогнозування розвитку ризику. Побудуйте діаграму зворотного зв’язку та визначте критичні часові точки для втручання.

Кейс 2. Застосування експертних методів прогнозування ризиків у сфері критичної інфраструктури

У процесі стратегічного планування безпеки об’єктів енергетики постала потреба у прогнозуванні загроз на наступні 5 років. Аналітики не мають повної статистичної бази, але залучено групу досвідчених фахівців з технічного, інформаційного й адміністративного секторів.

Використовуючи Delphi-метод або метод сценаріїв, проведіть етапи експертного опитування, узгодження прогнозів і оцінки варіантів розвитку подій. Розробіть матрицю ймовірність × наслідки та зробіть висновок щодо необхідності змін у системі реагування.

Кейс 3. Прогнозування соціального ризику з використанням штучного інтелекту

У місті було впроваджено систему цифрового моніторингу громадського середовища з використанням AI-аналітики відеопотоків, геолокації та анонімізованих соціальних даних. Метою є передбачення зон з підвищеною ймовірністю правопорушень.

Побудуйте базову модель прогнозування з використанням машинного навчання (класифікація/кластеризація). Обґрунтуйте вибір архітектури AI-моделі, поясніть, як система може адаптуватися до зміни поведінки в просторі. Визначте ризики неправильної інтерпретації даних.

Кейс 4. Цифрова платформа моніторингу ризиків у галузі охорони здоров'я

На базі міської лікарні створено цифрову панель управління ризиками (dashboard), яка щогодини агрегує дані про заповненість ліжок, рівень доступних медикаментів, навантаження на персонал. Мета – вчасно передбачати перевищення допустимих навантажень.

На основі принципів системного аналізу опишіть архітектуру цифрової платформи моніторингу. Визначте ключові показники (KPI), алгоритми оповіщення та канали візуалізації ризиків. Запропонуйте засоби інтерфейсу для прийняття управлінських рішень у режимі реального часу.

Кейс 5. Інтеграція прогнозних моделей у систему національного управління ризиками

Державна установа розробляє інтегровану систему управління ризиками, яка має поєднувати прогностичні моделі для ризиків природного, техногенного та соціального походження. Потрібно узгодити джерела даних, об'єднати різні моделі (експертні, статистичні, симуляційні) і забезпечити цифрову доступність результатів.

Побудуйте логічну структуру інтегрованої системи прогнозування. Визначте, які типи моделей будуть найбільш ефективними для кожного типу ризику. Продемонструйте механізм зворотного зв'язку та способи адаптації прогнозів до нових даних.

Висновок по розділу 3

Висновки до Розділу 3. Прогнозування ризиків у системному середовищі

У третьому розділі навчального посібника розглянуто сучасні теоретико-методологічні та практичні підходи до прогнозування ризиків у контексті складного системного середовища. Системне мислення, інструменти моделювання, а також аналітичні, обчислювальні та візуалізаційні платформи розглянуто як ключові компоненти ефективної прогностичної діяльності. Зокрема, було здійснено глибокий аналіз чотирьох напрямів: моделювання ризиків в умовах динаміки та невизначеності, використання експертних і статистичних моделей, впровадження штучного інтелекту та машинного навчання, а також застосування цифрових платформ і інформаційних систем моніторингу ризиків.

У підрозділі 3.1 розглянуто моделювання ризиків з урахуванням динамічних властивостей середовища та невизначеності, яка притаманна сучасним технічним, соціальним та економічним системам. Було наголошено на значенні динамічних систем із часовими лагами, що дозволяють моделювати вплив запізнілих ефектів на розвиток ризикових сценаріїв. Вивчення системної динаміки Форрестера з її механізмами зворотного

зв’язку дозволило сформувати уявлення про петлі посилення й стабілізації, які можуть призводити як до катастрофічних зламів, так і до системної рівноваги. Імітаційне та агентне моделювання, завдяки здатності до врахування багатофакторної взаємодії та емерджентних властивостей, виявилося ефективним інструментом відтворення складної поведінки систем під впливом ризиків. Агентно-орієнтовані моделі дозволяють виявити приховані ризикові патерни, які не фіксуються традиційними методами.

Підрозділ 3.2 було присвячено прогнозуванню на основі експертних та статистичних моделей. Регресійні моделі, моделі часових рядів (зокрема ARIMA) дозволяють здійснювати коротко- та середньострокові прогнози ризиків на основі історичних даних і виявлених трендів. Особливу увагу було приділено дельфі-методу, як інструменту групової експертної оцінки з високим ступенем адаптивності до нових умов. У межах системного підходу здійснено аналіз достовірності та валідації моделей, включаючи показники надійності, точності, чутливості та узгодженості. Була представлена концепція «моделі в моделі», коли прогнозування здійснюється з урахуванням зміни параметрів самих моделей у динамічному середовищі, що є принципово важливим у нестабільних системах.

У підрозділі 3.3 розкрито потенціал штучного інтелекту в прогнозуванні ризиків. Особлива увага приділена використанню нейронних мереж і глибокого навчання для виявлення складних нелінійних залежностей між вхідними параметрами та ризиковими наслідками. Наведено приклади використання convolutional і recurrent neural networks для аналізу часових рядів і послідовностей ризиків у кіберфізичних системах. Розглянуто застосування машинного навчання для виявлення ризикових патернів на основі класифікації, кластеризації та аномального поведінкового аналізу. Особливо цінною є інтеграція AI-рішень у системи підтримки прийняття рішень, що дозволяє забезпечити адаптивну реакцію на загрози в режимі реального часу, з урахуванням історичного досвіду та нових вхідних даних. Штучний інтелект, інтегрований у багаторівневі інформаційні середовища, виступає як динамічний інструмент ситуаційного прогнозування.

Підрозділ 3.4 присвячений інформаційним системам та цифровим платформам моніторингу ризиків. Розглянуто використання цифрових двійників (Digital Twins) як репрезентативного цифрового аналога фізичних об’єктів, що дозволяє не лише відтворювати, але й передбачати поведінку систем у складних умовах. Завдяки IoT-технологіям і сенсорним мережам забезпечується глибинний аналіз даних у режимі реального часу, що створює основу для високоточних адаптивних моделей ризику. Платформи візуалізації, такі як аналітичні dashboards, heatmaps, інтерактивні графи дозволяють ефективно відображати критичні зони, сценарії та траєкторії розвитку ризиків, що значно підвищує якість управлінських рішень. Важливою складовою цифрових платформ є їх здатність до самонавчання та еволюційної адаптації на основі нових даних і поведінкових індикаторів системи.

Загалом, у третьому розділі було доведено, що ефективне прогнозування ризиків у системному середовищі потребує поєднання кількох методологічних підходів: від класичних моделей до інноваційних обчислювальних технологій. Інтеграція системної динаміки, експертних оцінок, штучного інтелекту та цифрових інтерфейсів дозволяє створити адаптивну, багаторівневу архітектуру управління ризиками. Особливої ваги набуває міждисциплінарний підхід, який поєднує математичне моделювання, інформатику, соціотехнічні науки, кібербезпеку та інженерію рішень. У майбутньому подальший розвиток прогнозування ризиків передбачає використання когнітивних обчислень, квантових алгоритмів, генеративного AI та розширених симуляційних платформ у цифрових екосистемах.

Таким чином, Розділ 3 створює основу для формування цілісного бачення сучасного ризик-менеджменту, орієнтованого на динамічну адаптацію, високоточне прогнозування та гнучке прийняття рішень у складних системних умовах.

РОЗДІЛ 4. УПРАВЛІННЯ РИЗИКАМИ ЯК ЕЛЕМЕНТ СИСТЕМНОГО УПРАВЛІННЯ

4.1. Системне прийняття рішень в умовах ризику

Управління ризиками є складовою частиною системного управління, що передбачає використання структурованих, методологічно обґрунтованих підходів до ідентифікації, оцінки, аналізу та мінімізації небажаних впливів. Особливу роль у цьому процесі відіграє системне прийняття рішень в умовах невизначеності й ризику, яке потребує застосування міждисциплінарних методів з акцентом на формалізоване моделювання та прогнозування.

Теорія корисності, дерево рішень, матриця наслідків

Теорія корисності (Expected Utility Theory – EUT) є фундаментальною концепцією в теорії прийняття рішень, особливо в контексті ситуацій, що характеризуються невизначеністю або ризиком. Вона була сформульована та математично обґрунтована у роботах Джона фон Неймана та Оскара Моргенштерна у середині XX століття і відтоді набула широкого застосування у таких галузях, як економіка, психологія, поведінкові науки, теорія ігор, а також кримінальний аналіз, менеджмент ризиків і стратегічне планування.

У центрі цієї теорії перебуває суб’єкт прийняття рішення, або Decision Maker (DM) – індивід, група або автоматизована система, що має здійснити вибір між альтернативами, кожна з яких пов’язана з певними ймовірностями настання подій і відповідними наслідками.

Теорія очікуваної корисності базується на раціоналістичній парадигмі, згідно з якою особа, що приймає рішення, діє логічно, послідовно та прагматично, маючи на меті максимізацію суб’єктивної корисності результату. Згідно з цим підходом:

1. Кожна можлива дія або стратегія (альтернатива) призводить до одного з кількох можливих результатів (наслідків), кожен з яких має свою ймовірність.

2. Особисті уподобання особи, що приймає рішення, можуть бути представлені у вигляді числових оцінок (корисностей), що відображають суб’єктивну цінність кожного результату.

3. Очікувана корисність альтернативи обчислюється як сума добутків корисності кожного можливого наслідку на ймовірність його настання.

Розглянемо ситуацію вибору між двома стратегіями у кримінальному аналізі:

Стратегія А: Інвестувати ресурси в аналітичну розвідку, що з ймовірністю 0,7 призведе до запобігання злочину (корисність – 80 одиниць), але з ймовірністю 0,3 не дасть результату (корисність – 10 одиниць).

Стратегія В: Використати ресурси на посилення патрулювання, що з ймовірністю 0,6 дозволить знизити кількість злочинів (корисність – 60), але з ймовірністю 0,4 – не вплине суттєво (корисність – 20).

Розрахунок очікуваної корисності:

1. EU(A) = 0.7 × 80 + 0.3 × 10 = 56 + 3 = 59
2. EU(B) = 0.6 × 60 + 0.4 × 20 = 36 + 8 = 44

Отже, за критерієм очікуваної корисності, раціональний Decision Maker має обрати Стратегію A, як таку, що має вищу очікувану вигоду.

Поведінкові аспекти та критика EUT

Попри свою логічну привабливість і математичну строгість, теорія очікуваної корисності зазнала критики з боку представників поведінкової економіки та психології. Основні зауваження зводяться до наступного:

1. Люди не завжди діють раціонально. Поведінкові експерименти, зокрема парадокс Еллсберга чи парадокс Алле, показали, що реальні рішення часто суперечать передбаченням EUT.

2. Суб'єктивні уявлення про ймовірності та корисність є нестабільними. Люди можуть переоцінювати або недооцінювати малоймовірні події (наприклад, катастрофи чи виграш у лотерею).

3. Емоційні та соціальні чинники (наприклад, страх, довіра, соціальний вплив) часто мають більшу вагу, ніж раціональні розрахунки.

Ці обмеження призвели до появи альтернативних моделей, таких як теорія перспектив (Prospect Theory) Каганемана і Тверські, яка враховує психологічні аспекти ризикованих виборів.

Попри критику, EUT залишається основою для численних прикладних моделей у сфері аналізу ризиків, побудови стратегій управління невизначеністю, оптимізації ресурсів і моделювання поведінки суб’єктів в економіці та безпеці. У кримінальному аналізі EUT використовується для: Прогнозування поведінки злочинців в умовах підвищеного ризику бути спійманими. Оцінки ефективності запровадження заходів безпеки. Підтримки прийняття управлінських рішень при розподілі ресурсів між альтернативними антикримінальними заходами.

У сфері технічної та інформаційної безпеки EUT лежить в основі рішень щодо впровадження нових систем захисту, страхування кіберризиків, а також визначення оптимального балансу між витратами на безпеку і потенційними втратами від загроз.

Дерево рішень – це потужний аналітичний і візуалізаційний інструмент, який широко застосовується для моделювання, аналізу та оптимізації процесів прийняття рішень у складних і неоднозначних ситуаціях. Цей підхід дозволяє приймачу рішення (Decision Maker – DM) систематизувати усі можливі сценарії розвитку подій, варіанти вибору, відповідні наслідки, ймовірності настання подій і значення очікуваної корисності кожного з результатів.

На відміну від суто числових моделей (наприклад, матриць рішень), дерево рішень забезпечує наочну структуру, що полегшує інтерпретацію складних послідовних рішень, що приймаються в умовах ризику, невизначеності або неповної інформації.

Графічно дерево рішень являє собою ієрархічну структуру, яка починається з вихідної точки (кореня дерева) і далі розгалужується на основі

варіантів рішень, випадкових подій і кінцевих наслідків. Його основними складовими є:

1. Вузли рішень (decision nodes)

Позначаються квадратами і відображають точки, в яких особа, що приймає рішення, обирає одну з можливих альтернатив або стратегій. Наприклад, у ситуації загрози витоку даних рішенням може бути або інвестувати в нову систему шифрування, або підвищити внутрішній контроль доступу.

2. Вузли випадковостей (chance nodes)

Позначаються колами і представляють точки, у яких настання певної події залежить від випадковості або зовнішніх факторів. Для кожного варіанту подій зазначається ймовірність їх настання. Наприклад, впровадження нової системи безпеки може з імовірністю 0,8 запобігти кібератаці, а з імовірністю 0,2 – виявитися неефективним.

3. Кінцеві вузли або результати (terminal nodes / outcomes)

Позначаються трикутниками або кінцевими листками дерева. Вони показують фінальні наслідки кожної гілки дерева — тобто результат певного ланцюга рішень і випадковостей. Кожному результату призначається значення корисності або витрат, яке може бути як об’єктивним (економічна вартість), так і суб’єктивним (рівень безпеки, задоволення тощо).

Процес побудови дерева рішень можна узагальнити у кілька послідовних етапів:

1. Формалізація проблеми: Визначення мети, критеріїв ефективності, обмежень та ключових змінних.

2. Ідентифікація всіх можливих рішень: Зіставлення альтернативних стратегій, які доступні DM.

3. Ідентифікація ймовірних подій: Для кожної альтернативи зазначаються можливі події, що можуть статися в результаті, з відповідними ймовірностями.

4. Оцінка результатів: Присвоєння кожному кінцевому вузлу значення корисності або витрат.

5. Розрахунок очікуваної корисності (Expected Utility): Застосування правила очікуваної корисності для обчислення очікуваного значення кожної альтернативи.

6. Вибір оптимального рішення: Обрання тієї гілки, яка має найвищу очікувану корисність або найменші очікувані витрати (залежно від мети моделі).

Ілюстративний приклад: дерево рішень у сфері управління безпекою

Завдання:

Керівник підрозділу інформаційної безпеки має обрати між двома стратегіями:

Стратегія А – встановлення дорогої, але надійної системи багаторівневого захисту.

Стратегія B – оновлення чинних програм безпеки з помірними витратами.

Для кожної стратегії існує ймовірність успішного або неуспішного запобігання атакам (табл. 4.1):

Таблиця 4.1

Стратегія	Ймовірність успіху	Корисність (у балах)	Ймовірність невдачі	Корисність
A	0,85	90	0,15	20
B	0,6	70	0,4	30

Розрахунок очікуваної корисності:
EU(A) = 0,85 × 90 + 0,15 × 20 = 76,5 + 3 = 79,5
EU(B) = 0,6 × 70 + 0,4 × 30 = 42 + 12 = 54

Таким чином, дерево рішень наочно показує, що Стратегія A є кращим вибором з точки зору очікуваної корисності.

Дерево рішень – це не лише метод візуального представлення складних виборів, а й інструмент стратегічного мислення, що поєднує формальну логіку, ймовірнісні міркування та аналіз корисності. Його застосування є надзвичайно ефективним у сферах, що вимагають зваженого, прозорого та обґрунтованого вибору – від медичних рішень і екологічного прогнозування до кримінального аналізу та інформаційної безпеки.

Приклад дерева графа (спрощено):
graph TD
A[Початкове рішення] --> B[Варіант 1]
A --> C[Варіант 2]
B --> D[Успіх (0.7)]
B --> E[Невдача (0.3)]
C --> F[Успіх (0.5)]
C --> G[Невдача (0.5)]

Матриця наслідків (payoff matrix)

Матриця наслідків (англ. *payoff matrix*, також відома як матриця виграшів або втрат) є базовим аналітичним інструментом, який широко застосовується в процесі прийняття управлінських рішень в умовах невизначеності, ризику та множинності альтернатив. Вона відображає наслідки – виграші, втрати або інші кількісні/якісні показники ефективності – для кожного можливого поєднання рішень (альтернатив) та сценаріїв (станів зовнішнього середовища, параметричних умов або поведінкових сценаріїв системи).

У структурі матриці наслідків рядки відображають множину альтернативних рішень, які потенційно може реалізувати суб’єкт управління. Ці рішення формуються на основі доступної інформації, цілей управління та обмежень, що існують у системі. Суб’єкт управління, яким може виступати

як людина (менеджер, аналітик), так і автоматизована система підтримки прийняття рішень (СППР), розглядає кожне рішення як стратегічний варіант дії, спрямований на досягнення оптимального результату за умов обмеженої або неповної інформації.

У термінах теорії рішень, альтернатива (альтернативне рішення) – це формалізований вибір дії з множини допустимих варіантів, що мають бути взаємовиключними, повними та операціоналізованими. Іншими словами, кожен рядок у матриці є формалізованою стратегією, яка передбачає певну поведінкову або ресурсну реакцію суб'єкта управління на невизначене середовище. У системному аналізі управлінських ситуацій ці рядки дозволяють структурувати простір можливостей для стратегічного або тактичного планування.

Стовпці матриці наслідків відображають множину можливих сценаріїв розвитку подій, які, як правило, є екзогенними щодо суб'єкта управління. Тобто, вони не підлягають прямому контролю чи управлінському впливу, проте мають фундаментальне значення для кінцевого результату вибору. У теорії рішень і сценарному моделюванні такі сценарії називають станами природи, станами середовища або детермінантами зовнішніх умов.

Ці сценарії репрезентують множину можливих ситуацій, у яких може опинитися система, і характеризуються високим ступенем невизначеності, ймовірності або суб'єктивної оцінки. Їхня роль полягає в тому, щоб встановити контекст реалізації рішень – умови, за яких кожне рішення матиме різні наслідки. У моделі системного мислення сценарії є проявом динамічного середовища, що може змінюватися під впливом політичних, економічних, соціальних, екологічних або технологічних чинників.

Таким чином, стовпці матриці дозволяють формалізувати вплив зовнішніх змінних на ефективність рішень, забезпечуючи підґрунтя для аналізу ризиків, чутливості та адаптивності стратегій.

Комірки матриці наслідків містять інтегральні оцінки результату, що виникає внаслідок реалізації певного управлінського рішення в умовах конкретного сценарію. З наукового погляду, ці оцінки можна розглядати як значення функції результату (*payoff function*), яка відображає взаємозалежність між змінною вибору (рішенням) та умовною змінною (сценарієм).

Залежно від характеру задачі, ці наслідки можуть бути кількісними (наприклад, чистий прибуток, витрати, продуктивність, втрати, часові затрати, рівень ризику в балах) або якісними, якщо йдеться про експертні оцінки, логіко-лінгвістичні шкали (наприклад, «високий ризик», «незадовільна ефективність») чи нечіткі змінні у системах нечіткого моделювання.

З позицій управлінської теорії, саме комірки матриці є головною обчислювальною базою для порівняльного аналізу рішень, адже вони дозволяють формалізовано оцінити, яке з рішень є найбільш доцільним за різних обставин. У випадку багатокритеріального підходу в кожній комірці може міститися векторна оцінка (наприклад, {економічна ефективність,

рівень безпеки, соціальний вплив}), що потребує застосування спеціалізованих методів агрегування або компромісного ранжування.

У контексті прийняття рішень в умовах ризику комірки також можуть бути представлені як математичні сподівання результатів, з урахуванням ймовірностей настання відповідних сценаріїв.

Узагальнюючи, можна стверджувати, що структура матриці наслідків – як поєднання множини альтернатив (рядки), множини сценаріїв (стовпці) та множини наслідків (комірки) – формує основу для системного, формалізованого та кількісно-орієнтованого аналізу управлінських ситуацій. Саме завдяки цій трикомпонентній структурі матриця забезпечує адаптивність і гнучкість у моделюванні та виборі оптимальних стратегій в умовах багатофакторної невизначеності.

Матриця наслідків слугує інтеграційною платформою для представлення складних, багатофакторних системних ситуацій у компактному, логічно структурованому вигляді, що дозволяє значно підвищити ефективність візуального, евристичного та формалізованого аналізу. У контексті теорії прийняття рішень вона виконує функцію проміжної моделі, що забезпечує трансформацію вихідної інформації – зокрема, альтернативних управлінських дій та відповідних сценаріїв зовнішнього середовища – у придатний для кількісної обробки формат.

Використання табличної структури дозволяє формалізувати навіть слабо структуровані проблеми (ill-structured problems) завдяки декомпозиції складної проблемної ситуації на окремі елементи (альтернативи, стани природи, наслідки), що сприяє застосуванню методів аналітичного моделювання. Такий підхід особливо ефективний при високому ступені невизначеності або інформаційної асиметрії, що властиво реальним умовам прийняття управлінських рішень у складних соціально-економічних або техніко-технологічних системах.

Матриця наслідків є базовим конструктивним елементом у класичних концепціях теорії прийняття рішень, що функціонують в умовах різного ступеня визначеності щодо майбутніх сценаріїв (станів природи). Саме вона дозволяє застосовувати низку нормативних критеріїв вибору, зокрема:

1. Критерій Вальда (максимін) – реалізується в умовах крайнього песимізму, де суб’єкт вибирає стратегію, що забезпечує максимальний виграш серед мінімальних можливих наслідків. Метод актуальний у середовищах з високим рівнем невизначеності.

2. Критерій Севіджа (мінімального жалю) – спрямований на зменшення максимального упущеного виграшу, ґрунтується на концепції «жалю» як міри неефективності вибору.

3. Критерій Лапласа – базується на припущенні рівноймовірності сценаріїв, що дозволяє розрахувати математичне очікування наслідків для кожної альтернативи.

4. Ймовірнісний (байєсівський) підхід – застосовується за наявності інформації про ймовірності реалізації кожного зі сценаріїв, і забезпечує вибір альтернативи з максимальним очікуваним виграшем.

5. Мінімаксна стратегія – поширена у контекстах стратегічної взаємодії (наприклад, у теорії ігор), де важливо звести до мінімуму можливі втрати у найгіршому випадку.

Кожен з цих підходів, будучи формалізованим в математичних моделях, оперує саме матрицею наслідків як вхідним набором даних, що дозволяє обчислювати показники ефективності альтернатив, знаходити компромісні стратегії або визначати допустимі межі ризику.

Узагальнено, матриця наслідків є інтерфейсом між реальними системними процесами та математичною моделлю ситуації прийняття рішень, забезпечуючи точність, адаптивність і структурованість аналітичного процесу. Її застосування сприяє підвищенню якості стратегічного мислення, мінімізації когнітивних помилок у виборі, а також забезпеченню методологічної прозорості в процедурі обґрунтування управлінських рішень.

Матриця наслідків забезпечує базову платформу для проведення аналізу чутливості – методики, яка дозволяє оцінити, як зміна параметрів сценаріїв або вихідних даних впливає на вибір оптимального рішення.

Таким чином, матриця наслідків у чутливісному аналізі виступає як своєрідна «лабораторія» тестування поведінки системи рішень у різних умовах.

У сучасному управлінні більшість рішень не можуть бути зведені до одного критерію ефективності. Саме тому виникає потреба у багатокритеріальному аналізі, де оцінюються різні аспекти наслідків: економічна доцільність, соціальна значущість, екологічна безпека, технологічна ефективність тощо.

Сучасні цифрові системи підтримки прийняття рішень (СППР), а також модулі аналітики в програмному забезпеченні для управління проєктами, ризиками чи підприємствами активно використовують концепцію матриці наслідків.

Матриця наслідків не лише слугує інструментом фіксації потенційних виграшів або втрат, а й є концептуальним ядром сучасних підходів до аналізу рішень. Її використання дозволяє глибше зрозуміти взаємозв’язок між вибором, невизначеністю та критеріями оцінки результату, забезпечуючи основу для побудови адаптивної, гнучкої та аналітично обґрунтованої моделі прийняття управлінських рішень.

Таблиця 4.2

Приклад матриці наслідків

Рішення/Сценарій	Сценарій 1	Сценарій 2	Сценарій 3
Варіант A	40	30	20
Варіант B	25	50	15
Варіант C	35	20	45

Системні стратегії мінімізації та уникнення ризиків

Мінімізація ризиків передбачає цілеспрямовану зміну структури системи або її параметрів задля зниження ймовірності небажаного впливу або його наслідків. Основними підходами є:

1. Розширене моделювання сценаріїв: прогнозування декількох сценаріїв з урахуванням стохастичної природи системи;
2. Використання бар'єрних технологій (наприклад, у кібербезпеці – фаєрволи, IDS);
3. Інституційне резервування: запровадження страхування ризиків, резервного фінансування, стратегічних запасів.

Граф 4.1. Зниження сукупного ризику за рахунок впровадження багаторівневого захисту:

```
pie
    title Частки ризику за рівнями контролю
    "Базовий ризик": 60
    "Зниження після первинного аналізу": 20
    "Після впровадження резервування": 10
    "Залишковий ризик": 10
```

Стратегія уникнення передбачає відмову від ризикової діяльності або її заміну на альтернативу з нижчим ризиковим профілем.

Таблиця 4.3

Порівняння стратегій управління ризиками

Стратегія	Переваги	Недоліки
Мінімізація	Гнучкість, керованість	Вартість, час
Уникнення	Абсолютне виключення впливів	Втрата вигоди, обмеження розвитку
Прийняття	Простота, економічність	Ймовірність втрат
Передача (трансфер)	Зниження відповідальності	Витрати на передачу

Оцінка ефективності рішень у багатокритеріальних умовах

Багатокритеріальні моделі

Для оцінки рішень, що враховують численні критерії (вартість, безпека, час, соціальні наслідки), використовуються методи багатокритеріального аналізу (Multi-Criteria Decision Analysis – MCDA):

Метод **ANP/AHP** (аналіз ієрархій/мереж);

Метод **TOPSIS** (Technique for Order of Preference by Similarity to Ideal Solution);

Метод **ELECTRE/MACBETH** (переважний аналіз);

Метод **SMART/SWING** (спрощена шкала важливості).

Граф 4.2. Приклад вагових коефіцієнтів у багатокритеріальній моделі:

```
barChart
    title Вагові коефіцієнти для критеріїв оцінки рішення
    x-axis Критерії
    y-axis Вага
    data
        "Безпека": 0.35
        "Вартість": 0.25
        "Тривалість": 0.20
        "Іміджеві наслідки": 0.10
        "Гнучкість": 0.10
```

Приклад інтегральної оцінки рішення

Таблиця 4.4

Бальна оцінка альтернатив (за шкалою 1-5)

Альтернатива	Безпека	Вартість	Тривалість	Імідж	Гнучкість	Інтегральна оцінка
A	5	4	3	2	3	4,05
B	3	5	5	3	2	3,65
C	4	3	4	4	4	3,95

Інтегральна оцінка обчислюється як сума добутків балів на вагові коефіцієнти.

Системне прийняття рішень в умовах ризику вимагає поєднання формалізованих моделей (дерево рішень, матриця наслідків, теорія корисності) з якісними оцінками альтернатив. Найефективніші підходи — це багатокритеріальний аналіз з урахуванням мінливих сценаріїв, що дозволяє враховувати як кількісні, так і якісні чинники. Інтеграція ризик-орієнтованого мислення в системне управління є необхідною умовою підвищення надійності та стійкості складних технічних, соціальних або економічних систем.

4.2. Інтеграція ризик-менеджменту в системне управління організацією

Інтеграція ризик-менеджменту в системне управління організацією є ключовим компонентом стратегічного управління. В умовах постійної мінливості зовнішнього середовища, зростаючої складності бізнес-процесів та інформаційної насиченості, ефективне управління ризиками (Enterprise Risk Management – ERM) стає не лише інструментом зниження загроз, а й джерелом конкурентної переваги.

ERM – це стратегічний підхід до управління всіма ризиками організації, що інтегрується в загальну систему управління та охоплює всі

рівні організаційної структури. Метою ERM є створення цілісної, гнучкої та адаптивної системи реагування на ризики на всіх етапах життєвого циклу організації.

Таблиця 4.5

Основні елементи системи ERM

Компонент	Характеристика
Ідентифікація ризиків	Виявлення джерел ризику та зон вразливості
Оцінка ризиків	Кількісний і якісний аналіз впливу ризиків
Планування заходів	Визначення стратегій уникнення, мінімізації або передачі ризиків
Моніторинг і звітність	Постійне відстеження, аналіз динаміки ризиків і результатів управлінських дій
Адаптація і розвиток	Безперервне вдосконалення методів та стратегій

Граф 4.3. Інтегрованої системи ERM:

```
graph TD
   A[Ідентифікація ризиків] --> B[Оцінка ризиків]
   B --> C[Розробка стратегій управління]
   C --> D[Реалізація та моніторинг]
   D --> E[Збір зворотного зв'язку]
   E --> F[Адаптація системи ERM]
   F --> A
```

ERM впроваджується за принципом циклічності, що забезпечує сталість розвитку та гнучкість до змін середовища.

Моніторинг, реакція та адаптація ERM – три взаємозв’язані підсистеми, що забезпечують функціонування ERM в реальному часі.

А. Моніторинг

Моніторинг ризиків включає:

1. Збір інформації з внутрішніх і зовнішніх джерел
2. Аналіз змін у середовищі
3. Визначення тригерів для запуску реактивних дій

Таблиця 4.6

Моніторинг ризиків

Джерело моніторингу	Тип інформації	Частота оновлення
Внутрішній аудит	Оцінка процесів, звітність	Щоквартально
BI-системи	Дані про KPI, бізнес-аналітика	В реальному часі
Зовнішні платформи	Дані про макросередовище	Щоденно/щотижнево

B. Реакція

Під реакцією розуміють реалізацію управлінських рішень у відповідь на зміну рівня ризику:

1. Запуск контрзаходів
2. Перерозподіл ресурсів
3. Інформування зацікавлених сторін

Реакція має бути швидкою, проте базованою на заздалегідь визначених сценаріях (реактивне vs. проактивне управління).

C. Адаптація

Адаптація – це механізм навчання системи:

1. Коригування параметрів моделі управління ризиками
2. Врахування нових сценаріїв
3. Впровадження інноваційних технологій (AI/ML, блокчейн, цифрові двійники)

Граф 4.4. Адаптация

```
flowchart LR
   M[Моніторинг] --> R[Реакція] --> A[Адаптація] --> M
```

Корпоративна Культура безпеки – це сукупність цінностей, переконань і моделей поведінки, що визначають ставлення організації до ризиків. Вона є критичним компонентом ефективного ERM.

Таблиця 4.7

Рівні корпоративної культури (адаптовано від моделі Reason, 1997)

Рівень культури	Характеристика
Патологічний	Відсутність інтересу до ризиків, заперечення проблем
Реактивний	Дії в основному після інцидентів
Калькульований	Часткова формалізація процесів управління ризиками
Проактивний	Системний підхід до виявлення та аналізу ризиків
Генеруючий	Постійне вдосконалення, інновації, повне інтегрування культури безпеки

Граф 4.5. Розвитку культури безпеки:

```
graph LR
   P[Патологічна] --> R[Реактивна] --> C[Калькульована] --> Pr[Проактивна] --> G[Генеруюча]
```

Інтеграція ризик-менеджменту в системне управління організацією – це не лише побудова окремої функціональної підсистеми, а й формування нової управлінської парадигми, що забезпечує стійкість, гнучкість та стратегічну спроможність організації. Комплексність ERM, її зв’язок із культурою

безпеки та адаптивними підсистемами дозволяє формувати системно зорієнтовану організацію, готову до викликів XXI століття.

4.3. Критична інфраструктура та стратегічне управління ризиками

У сучасному світі критична інфраструктура (КІ) – це сукупність систем і об'єктів, функціонування яких є життєво важливим для забезпечення національної безпеки, економічної стабільності, охорони здоров'я, громадського порядку та добробуту населення. Порушення функціонування цих систем через ризики техногенного, природного або кібернетичного характеру може спричинити масштабні cascading-ефекти та надзвичайні ситуації.

У цьому підрозділі розглядаються системні підходи до класифікації критичних систем, оцінки ризиків у контексті їх взаємопов’язаності та вразливостей, а також стратегічне сценарне планування як інструмент забезпечення стійкості та адаптивності організацій і державних систем до загроз.

Критична інфраструктура – це сукупність фізичних або віртуальних систем і об'єктів, порушення яких призводить до серйозних наслідків для життєдіяльності суспільства, економіки або державного управління.

Таблиця 4.8

Основні категорії критичних інфраструктур

Категорія	Приклади	Характер загроз
Енергетика	Електростанції, ГТС, ЛЕП	Атаки, аварії, кібервразливості
Транспорт	Аеропорти, порти, залізничні вузли	Деструкція логістики, саботаж
Зв’язок і телекомунікації	Мобільні мережі, супутниковий зв'язок	Кібератаки, фізичне пошкодження
Водопостачання та каналізація	Водогони, насосні станції	Забруднення, теракти, збій обладнання
Фінансова система	Банки, платіжні системи, біржі	Фішинг, крадіжка даних, системні збої
Здоров’я	Лікарні, фармацевтичні мережі	Біозагрози, технічні збої, дефіцит ресурсів
Урядування	Адміністративні системи, критичні бази даних	Sabotage, інформаційні атаки

Граф 4.6. Системний підхід до ідентифікації КІ

```
graph TD
A[Ідентифікація систем] --> B[Оцінка критичності]
B --> C[Класифікація залежностей]
C --> D[Визначення cascading-ефектів]
D --> E[Пріоритизація захисту]
```

Поняття каскадного ефекту

Cascading-ефекти виникають, коли порушення у одній частині системи (або одній інфраструктурі) спричиняє ланцюгову реакцію в інших сферах або галузях. Такий ефект може мати експоненційний характер.

Приклад:

Виведення з ладу енергетичного вузла → порушення водопостачання → збій роботи лікарень → зростання смертності

Таблиця 4.9

Методика аналізу ризиків каскадного типу

Етап	Дія
1. Визначення критичних вузлів	Аналіз систем з найбільшою кількістю залежностей
2. Виявлення взаємозв’язків	Побудова графу взаємозалежностей
3. Моделювання сценаріїв	Імітаційне або агентне моделювання
4. Прогнозування наслідків	Кількісна оцінка економічних, соціальних, екологічних втрат
5. Формування матриці ризиків	Побудова з урахуванням мультисистемного впливу

Граф 4.7. Методика аналізу ризиків каскадного типу

```
graph LR
A[Порушення в енергетиці] --> B[Втрата енергопостачання]
B --> C[Зупинка транспорту]
B --> D[Втрата зв’язку]
C --> E[Порушення логістики]
D --> F[Параліч координації Служб]
```

Таблиця 4.10

Матриця ризиків для мультисистемного сценарію

Інфраструктура	Ймовірність	Вразливість	Потенційний вплив	Загальний ризик
Енергетика	Висока	Середня	Високий	Високий
Зв’язок	Середня	Висока	Високий	Високий
Здоров’я	Низька	Висока	Середній	Середній

Принципи сценарного підходу

Сценарне планування – це метод передбачення майбутніх варіантів розвитку подій на основі побудови альтернативних сценаріїв. У контексті критичної інфраструктури використовується для розробки стратегій адаптації та відновлення.

Таблиця 4.11

Типи сценаріїв

Тип сценарію	Характеристика	Приклад
Оптимістичний	Найкращий можливий розвиток подій	Швидке відновлення енергосистеми після аварії
Реалістичний	Найбільш імовірний перебіг	Часткове порушення логістики
Песимістичний	Найгірший варіант з cascading-ефектами	Системне відключення критичних вузлів

Таблиця 4.12

Побудова стратегічних резервів

Категорія резервів	Приклади	Роль у кризі
Технічні ресурси	Генератори, мобільні мережі	Забезпечення автономності
Інформаційні резерви	Резервні бази даних, план БК (BCP)	Відновлення інформаційних функцій
Персонал	Резервні команди, багатофункціональні фахівці	Гнучкість та заміщення кадрів
Фінансові ресурси	Страхові фонди, державні резерви	Зниження економічних наслідків

4.8. Граф інтеграції сценарного підходу

```
graph TD
A[Аналіз поточних загроз] --> B[Генерація сценаріїв]
B --> C[Оцінка впливу]
C --> D[Розробка стратегічних резервів]
D --> E[Інтеграція у план дій]
```

Інтеграція системного управління ризиками в контексті критичної інфраструктури вимагає міждисциплінарного підходу, що поєднує інженерний, соціально-економічний, інформаційний та організаційний аналіз. Сценарне планування та врахування cascading-ефектів є ключем до забезпечення стійкості та здатності адаптуватися до складних загроз.

У наступному підрозділі буде розглянуто інструменти цифрового прогнозування ризиків із застосуванням штучного інтелекту та симуляційних моделей для багатофакторного аналізу в умовах високої невизначеності.

4.4. Системне забезпечення сталого розвитку в контексті ризиків

Сталий розвиток – це парадигма довготривалого функціонування суспільства, економіки та навколишнього середовища на засадах балансу між

економічною ефективністю, соціальною справедливістю та екологічною доцільністю. У системному аналізі сталий розвиток розглядається як цілісна система, що включає численні взаємозалежні підсистеми та фактори ризику, які можуть порушити цей баланс.

Системна безпека в даному контексті – це здатність складної соціо-еколого-економічної системи протистояти внутрішнім та зовнішнім загрозам, зберігаючи основні функції, структуру та здатність до адаптації та трансформації.

Таблиця 4.13

Ключові компоненти системної безпеки для сталого розвитку

Компонент	Характеристика
Інституційна стійкість	Спроможність урядових структур реагувати на виклики
Економічна стабільність	Диверсифікація, адаптивність до глобальних змін
Екологічна рівновага	Відновлення біорізноманіття, ресурсоефективність
Технологічна безпека	Інновації у сфері «зелених» та безпечних технологій
Інформаційна відкритість	Прозорість та залучення громадян до ухвалення рішень

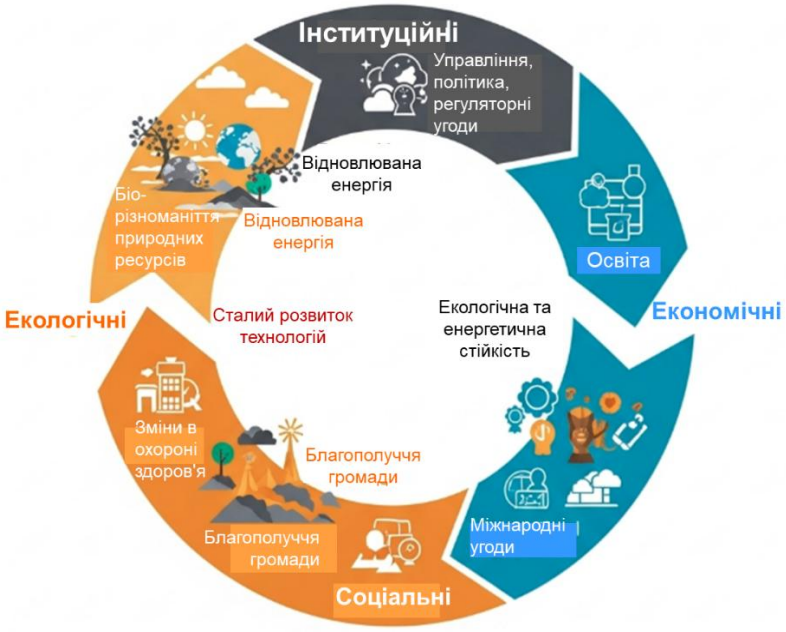

Рис. 4.1. Взаємозв’язок між компонентами системної безпеки.
Інфографіка, що демонструє зв’язки між екологічними, економічними, соціальними та інституційними елементами у забезпеченні сталого розвитку.

ESG-фактори та ризики сталості

Підходи до оцінки та управління ризиками в умовах сталого розвитку значною мірою базуються на концепції ESG (Environmental, Social, Governance) – середовищних, соціальних та управлінських факторів.

Environmental (E) – включає зміну клімату, забруднення, зниження ресурсів; Social (S) – права працівників, гендерна рівність, соціальна

відповідальність; Governance (G) – корпоративна етика, прозорість, ефективне управління.

Таблиця 4.14

ESG-фактори та типові ризики

Категорія	ESG-фактор	Типовий ризик
Екологія	Зміна клімату	Порушення ланцюгів постачання, зниження агровиробництва
Соціальна	Гендерна нерівність	Соціальні протести, зниження лояльності персоналу
Управління	Корпоративна непрозорість	Втрата довіри інвесторів, юридичні наслідки

Інтеграція ESG-факторів у системний аналіз ризиків дозволяє ідентифікувати довгострокові загрози, знизити нестабільність управлінських рішень, а також підвищити резильєнтність організаційних структур.

Глобальні ризики – це ризики, що мають потенціал викликати катастрофічні наслідки для значної частини світового населення, економіки або природного середовища. Вони є мультидисциплінарними, взаємозалежними та мають високий ступінь невизначеності.

Кліматичні зміни викликають зростання частоти екстремальних погодних явищ, танення льодовиків, підвищення рівня моря.

Основні наслідки:

1. Зниження аграрної продуктивності.
2. Масове переміщення населення (екобіженці).
3. Руйнування критичної інфраструктури.

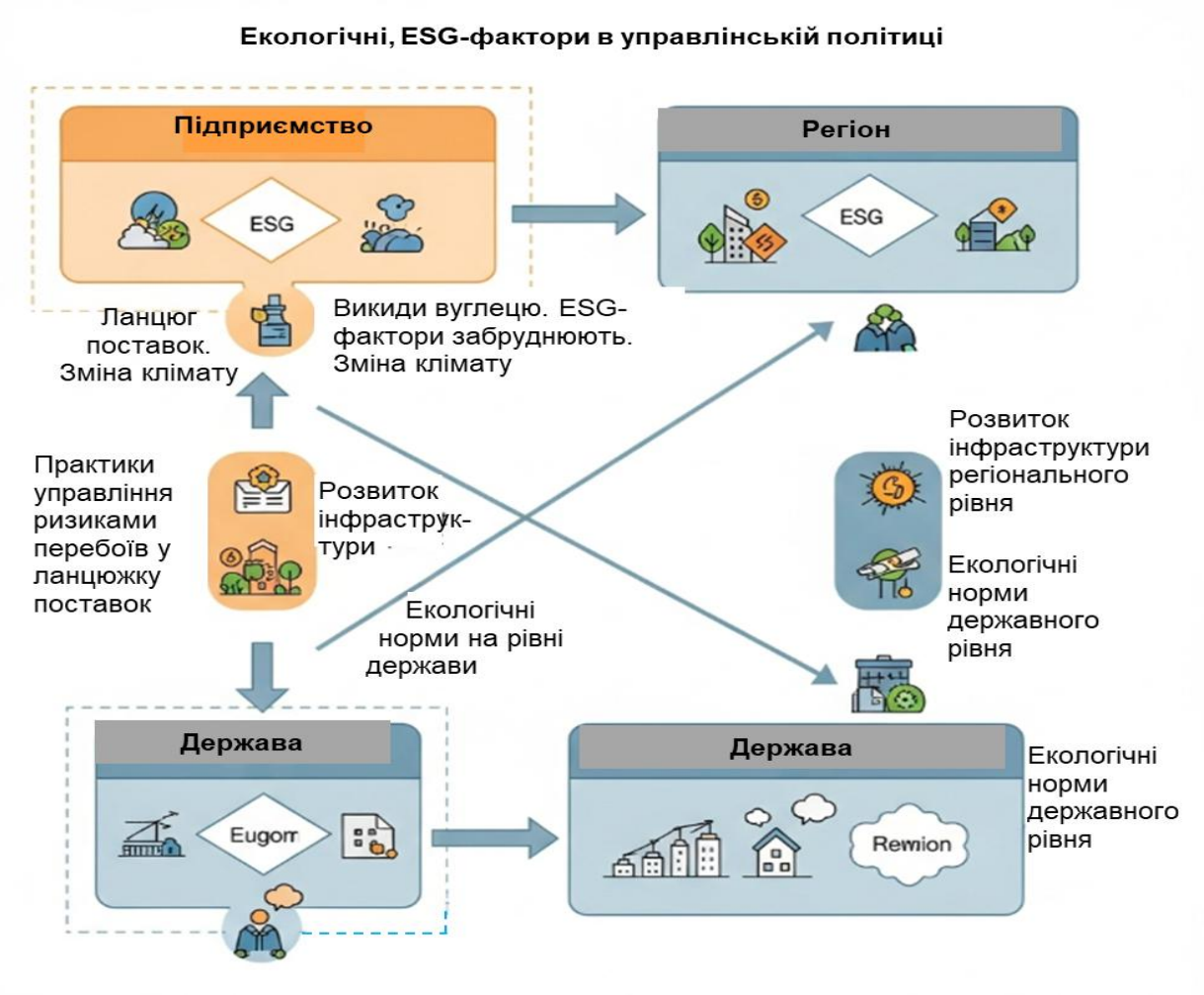

Рис. 4.2. Модель інтеграції ESG-індикаторів у системне управління ризиками. *Діаграма, що демонструє процес впровадження ESG-факторів у політику управління ризиками на рівні підприємства, регіону, держави.*

Кібербезпека стала одним із головних елементів системної безпеки, що напряму впливає на сталий розвиток у цифрову епоху.

Типи загроз:

1. Атаки на енергосистеми та транспорт
2. Витоки персональних та фінансових даних
3. Штучно створені інформаційні кризи (дезінформація)

Соціальні ризики – це виклики, пов’язані зі зміною демографії, нерівністю, міграційними процесами та суспільною нестабільністю.

Системні наслідки:

1. Зростання напруги в суспільстві
2. Розширення бідності та соціального виключення
3. Зниження ефективності управління

Таблиця 4.15

Компаративний аналіз глобальних ризиків

Ризик	Джерело	Характер впливу	Рівень системної небезпеки
Кліматичний	Екологічний	Повільний, кумулятивний	Високий
Кібернетичний	Технологічний	Раптовий, системний	Дуже високий
Соціальний	Соціально-економічний	Середньо- та довгостроковий	Високий

Стратегії системного забезпечення сталості

1. Ризик-орієнтоване управління (Risk-based governance): інтеграція ризиків у всі етапи прийняття рішень.
2. Трансформаційна адаптація: гнучка перебудова систем у відповідь на нові виклики.
3. Цифрова трансформація управління: використання big data, штучного інтелекту та цифрових близнюків для передбачення ризиків.
4. Сценарне планування: побудова моделей розвитку з урахуванням глобальних трендів.
5. Глобальна співпраця: мережі обміну знаннями, кращими практиками та моніторинговими даними.

Кліматичні зміни вже призвели до низки масштабних екологічних катастроф, що мають довгострокові системні наслідки. Прикладом є повені 2021 року у Західній Європі, лісові пожежі в Австралії 2019-2020 рр. та урагани в Карибському басейні.

Таблиця 4.16

Вплив кліматичних катастроф

Параметр	Приклад	Наслідки для сталого розвитку
Економічні втрати	Понад $10 млрд збитків	Руйнування інфраструктури, зниження ВВП
Соціальні наслідки	Евакуація сотень тисяч людей	Збільшення числа біженців, психоемоційний стрес
Екологічні руйнування	Знищення лісів та біорізноманіття	Порушення екосистем, зниження природних ресурсів
Управлінські виклики	Неефективність екстрених заходів	Відсутність координації між органами влади

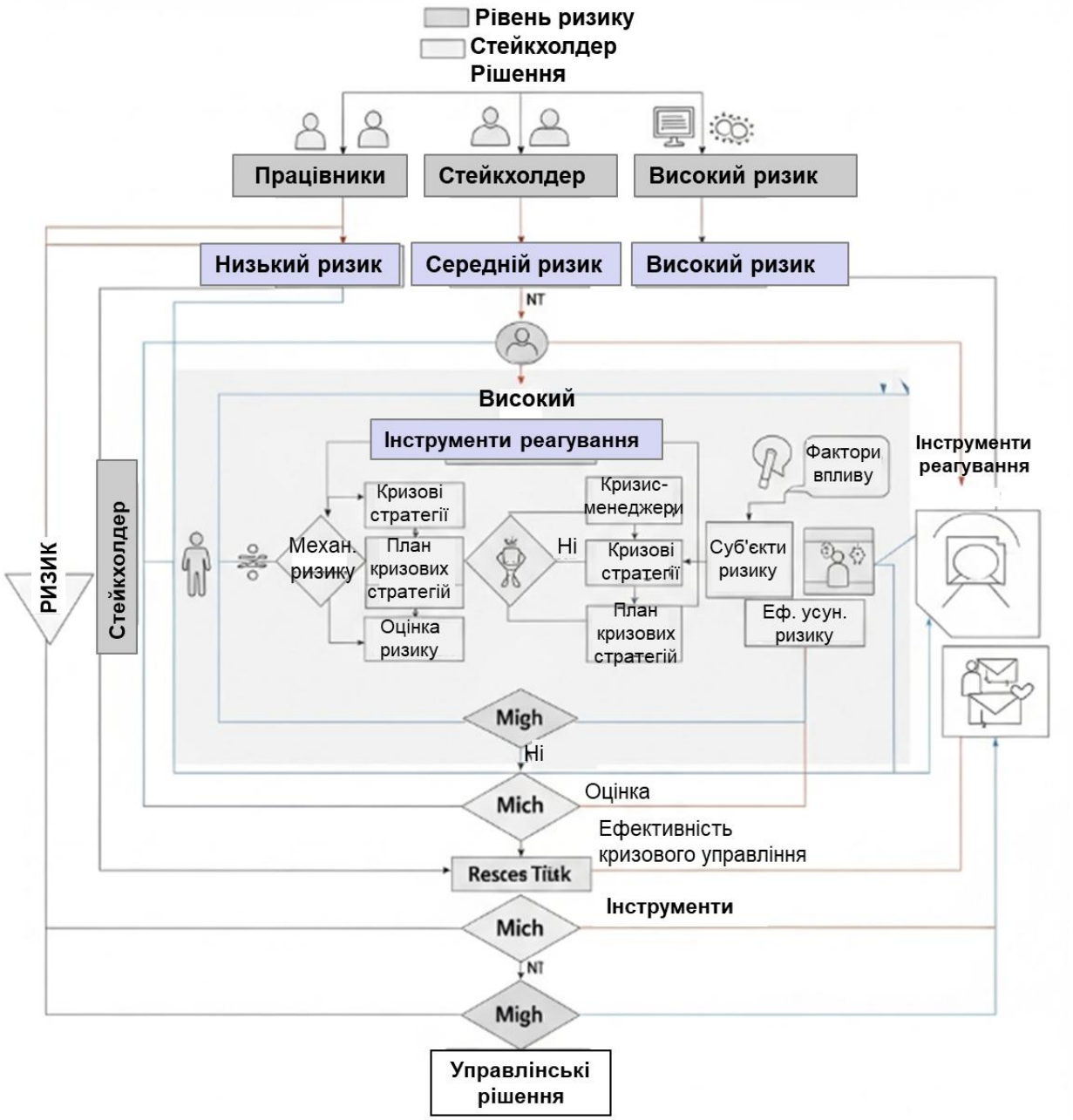

Рис. 4.3. Архітектура системної моделі сталого розвитку в умовах ризиків. *Модель, що об’єднує рівні ризиків, стейкхолдерів, інструменти реагування та управлінські рішення.*

Рис. 4.4. Модель системного впливу кліматичних катастроф на сталий розвиток

Інфографіка, що демонструє вплив кліматичних катастроф на економіку, екологію, соціальну сферу та управління із зазначенням зворотних зв'язків.

Зі зростанням цифровізації економіки кіберзагрози стають ключовим фактором ризику. Кіберінциденти можуть паралізувати критичну інфраструктуру (енергетику, транспорт, телекомунікації), спричиняти витоки конфіденційних даних і підривати довіру до інститутів.

Таблиця 4.17

Ключові типи кіберризиків

Тип загрози	Приклад атаки	Потенційний вплив
Атаки на енергосистеми	Вірус Stuxnet, 2010	Відключення електропостачання, аварії
Фішингові атаки	Витік даних з банків	Фінансові втрати, шахрайство
Дезінформація	Маніпуляція суспільною думкою	Соціальна напруга, політична дестабілізація

Рис. 4.5. Кіберризики як мультидоменна загроза сталості

Діаграма, що показує взаємозв'язок кіберзагроз із економічними, соціальними та політичними наслідками.

У сучасному глобалізованому світі соціальні виклики набувають дедалі більшого значення як латентні, але потужні тригери політичної турбулентності, дестабілізації інституційних структур та ескалації конфліктів. Зокрема, феномени соціальної нерівності, демографічних змін і міграції виступають не ізольованими процесами, а тісно взаємопов'язаними елементами більш складної соціоекономічної та політико-культурної системи, які чинять системний вплив на безпекове середовище держав і регіонів.

1. Соціальна нерівність як структурний каталізатор нестабільності

Нерівність у розподілі ресурсів, доступі до послуг, можливостях участі у політичному житті є джерелом фрустрації, маргіналізації та зростання соціальної напруги.

Вона може набувати різних форм:

1) економічної нерівності (розриви в доходах, власності, доступі до праці);

2) освітньої та цифрової нерівності;
3) територіальної (регіональної);
4) гендерної або етнокультурної.

У суспільствах із високим рівнем нерівності зростає ймовірність масових протестів, популістичних рухів, радикалізації молоді, зниження довіри до інституцій і легітимності державної влади. Ці процеси вже давно описані в рамках теорій відносної депривації (R. Gurr), конфлікту ресурсів (H. Blalock) та фреймінгу соціальних проблем (Snow & Benford).

Дослідження Світового банку, МВФ і ООН неодноразово підкреслювали, що нерівність не лише підриває соціальну єдність, а й істотно уповільнює економічне зростання, що створює замкнене коло кризи.

2. Демографічні зміни: старіння населення, урбанізація, «демографічні бульбашки»

Демографічна динаміка є критичним параметром для прогнозування стійкості держав, оскільки впливає як на економічну активність, так і на політичну стабільність. Зокрема:

– старіння населення у розвинених країнах призводить до зростання тиску на соціальні фонди, системи охорони здоров'я та пенсійне забезпечення, що створює соціально-економічну напругу між поколіннями;

– «демографічні бульбашки» – вибухове зростання чисельності молоді (youth bulge) в країнах, що розвиваються, при поєднанні з безробіттям і відсутністю перспектив може призводити до масових протестів, насильства або вербування до екстремістських угруповань;

– інтенсивна урбанізація та демографічна концентрація в мегаполісах без належної інфраструктури викликають соціальну поляризацію, екологічні ризики, зростання злочинності та появу неформальних поселень (slums), що функціонують поза правовим полем.

Ці виклики породжують структурні конфлікти ресурсів та конкуренцію за робочі місця, доступ до житла, води, енергії, що поглиблює політичну фрагментацію.

3. Міграція як фактор трансформації політичного ландшафту

Міграційні процеси, зокрема вимушена міграція, транскордонна мобільність трудових ресурсів або зміна етнодемографічного складу населення, формують комплексну систему викликів безпеці, що охоплює:

– культурну інтеграцію / дезінтеграцію;
– міжетнічні та міжконфесійні напруження;
– поширення нелегальних ринків та кримінальних мереж;
– зміни політичних уподобань електорату (наприклад, радикалізація у відповідь на міграційний тиск).

У політичному вимірі масова міграція може слугувати інструментом гібридного впливу (міграційна зброя), формувати антиінституційні настрої, посилювати праворадикальні або ксенофобські рухи. Це вже спостерігалося в контексті криз 2015 року в ЄС, війни в Сирії, повномасштабного вторгнення росії в Україну, що спричинили багатомільйонні потоки біженців і політичну реакцію в країнах-реципієнтах.

Системний ефект: накопичення соціальних викликів як «точка біфуркації» для державності

Інтеграція соціальної нерівності, демографічної турбулентності та міграційних трансформацій створює кумулятивний ефект дестабілізації, особливо у державах із низьким рівнем інституційної стійкості, слабкою соціальною політикою або конфліктогенною політичною культурою.

У таких умовах:

– легітимність влади знижується;
– сценарії соціального вибуху стають більш вірогідними;
– можливість політичної радикалізації різко зростає.

Ці процеси формують так звану «точку біфуркації» – момент, коли система перестає бути стабільною й або трансформується, або деградує в напрямку авторитаризму, сепаратизму або затяжного конфлікту.

Соціальні виклики не є виключно гуманітарними або соціологічними категоріями – вони є інтегральною частиною сучасної парадигми політичної безпеки та стратегічного планування. Їх аналіз потребує міждисциплінарного підходу, що поєднує інструменти соціології, демографії, політичної економії, конфліктології та управління ризиками.

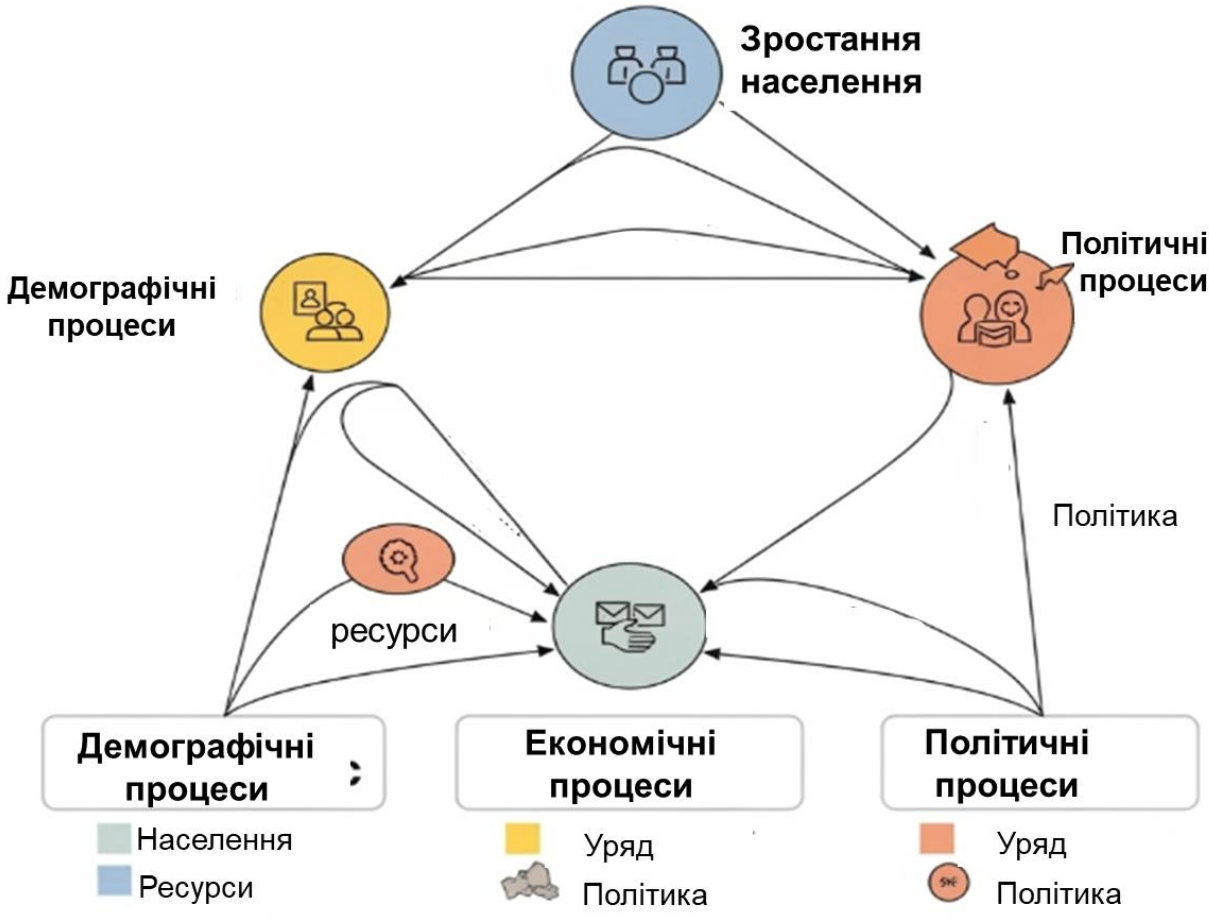

Рис. 4.6. Соціальні ризики у контексті системного аналізу
Графічна модель із відображенням взаємозв'язку демографічних, економічних і політичних чинників.

Моделі оцінки ризиків сталого розвитку

Для системного управління необхідні кількісні моделі, що дозволяють оцінити вплив різних ризиків на показники сталості.

Модель ризику сталості (Sustainability Risk Model, SRM) включає такі компоненти:

1. Індикатори вразливості (V): екологічна, соціальна, економічна вразливість.
2. Індикатори загрози (T): ймовірність настання небезпечної події.
3. Індикатори адаптивності (A): здатність системи реагувати та відновлюватися.

Формула ризику:

$R=T\times V\times(1-A)R = T \times V \times (1 - A)R=T×V×(1−A)$

де RRR — загальний рівень ризику, що враховує ймовірність, потенційну шкоду і ступінь готовності.

ESG-звітність та стандарти сталості

Корпорації та державні структури все активніше впроваджують ESG-стандарти для прозорості у сфері сталого розвитку.

Таблиця 4.18

Основні стандарти

Стандарт	Опис	Застосування
GRI (Global Reporting Initiative)	Міжнародний стандарт звітності з сталості	Вимірювання та звітність ESG-факторів
SASB (Sustainability Accounting Standards Board)	Сфокусований на фінансово значущих показниках ESG	Для інвесторів, аналітиків
ISO 26000	Керівництво з соціальної відповідальності	Орієнтири для організацій будь-якого типу

Рис. 4.7. Процес формування ESG-звітності
Діаграма циклу збору, аналізу, верифікації та публікації ESG-даних.

Для моніторингу стану системи сталого розвитку рекомендується використовувати такі ключові показники:

Таблиця 4.19

Практичні індикатори ризиків сталого розвитку

Показник	Опис	Джерело даних
Вуглецевий слід (CO2 footprint)	Викиди парникових газів	Екологічні агентства, підприємства
Індекс нерівності Джині	Вимір соціальної нерівності	Статистичні служби
Індекс кібербезпеки	Рівень захисту IT-інфраструктури	Сертифікаційні органи, внутрішні аудити
Індекс адаптивності системи	Здатність до відновлення після криз	Аналітичні дослідження

Системне забезпечення сталого розвитку в умовах ризиків – це багаторівнева, мультидисциплінарна задача, що вимагає інтеграції екологічних, соціальних, економічних та управлінських факторів. Системна безпека і ESG-концепції є ключовими орієнтирами у формуванні стратегій управління ризиками.

Для ефективного управління необхідно використовувати інноваційні технології, кількісні моделі ризиків, міжнародні стандарти та активне залучення всіх стейкхолдерів.

Контрольні питання

1. Що таке теорія корисності і як вона застосовується в управлінні ризиками?
2. Які основні елементи дерева рішень і як його використовують для аналізу ризиків?
3. Як формується матриця наслідків і яку роль вона відіграє у системному прийнятті рішень?
4. Назвіть і опишіть основні системні стратегії мінімізації ризиків.
5. Що означає стратегія уникнення ризиків, і в яких ситуаціях її доцільно застосовувати?
6. Які методи використовуються для оцінки ефективності рішень у багатокритеріальних умовах?
7. Як поєднати кількісні та якісні підходи при прийнятті рішень в умовах невизначеності?
8. Що таке ERM (Enterprise Risk Management) і які його ключові компоненти?
9. Які основні підсистеми входять до складу системи управління ризиками організації?
10. Яку роль відіграє моніторинг у системі управління ризиками?
11. Як забезпечується ефективна реакція на ризики у процесі системного управління?
12. Чому адаптація системи управління ризиками є необхідною у динамічному середовищі?
13. Що таке корпоративна культура безпеки і як вона впливає на ризик-менеджмент?
14. Які заходи формують культуру безпеки у організації?
15. Як класифікуються критичні інфраструктурні системи? Наведіть приклади.
16. Що таке cascading-ефекти і чому вони є важливими при оцінці ризиків?
17. Як здійснюється оцінка ризиків із урахуванням cascading-ефектів?
18. Що таке сценарне планування і які його основні етапи у стратегічному управлінні ризиками?
19. Яка роль стратегічних резервів у забезпеченні стійкості критичної інфраструктури?

20. Як інтегрувати управління стратегічними резервами у систему управління ризиками?
21. Як системна безпека пов’язана зі сталим розвитком?
22. Що таке ESG-фактори і як вони впливають на управління ризиками сталості?
23. Назвіть основні глобальні ризики, що впливають на сталий розвиток, і охарактеризуйте їх.
24. Які особливості прогнозування кліматичних ризиків у системному управлінні?
25. Як враховувати соціальні ризики при формуванні стратегій сталого розвитку?

Кейси до розділу 4

Кейс 1. Прийняття рішень в умовах конфлікту цілей у секторі оборони

У процесі формування плану реагування на кібератаку в підрозділі Збройних сил було виявлено суперечливі цілі: з одного боку – зберегти стабільність у критичній IT-інфраструктурі, з іншого – не допустити витоку інформації, навіть ціною тимчасового відключення зв’язку.

Використовуючи системний підхід до прийняття рішень в умовах ризику, побудуйте багатокритеріальну матрицю альтернатив, визначте ваги для кожного критерію, проаналізуйте ймовірні наслідки. Поясніть, як механізми сценарного аналізу можуть допомогти в ситуації стратегічної невизначеності.

Кейс 2. Інтеграція ризик-менеджменту у корпоративну систему управління банком

Фінансова установа розпочала інтеграцію ризик-менеджменту в загальну систему стратегічного управління. Існуючі практики управління ризиками були фрагментарними: окремо працював відділ внутрішнього аудиту, IT-безпеки, юридичного супроводу.

Завдання – розробити єдину карту ризиків організації (risk map), ідентифікувати типи ризиків (операційні, репутаційні, стратегічні), побудувати систему взаємодії між підрозділами та запропонувати механізми моніторингу на рівні правління банку.

Кейс 3. Управління ризиками в системі критичної інфраструктури міста

Міський центр управління транспортом відповідає за координацію світлофорів, камер, інформаційних табло. Унаслідок навмисного втручання в

систему (кібератаки) було паралізовано низку магістралей під час евакуації у надзвичайній ситуації.

Використайте концепцію управління ризиками у критичній інфраструктурі для моделювання уразливості системи. Визначте пріоритетні елементи для захисту, опишіть модель загроз і запропонуйте стратегію зміцнення стійкості із застосуванням принципу «resilience by design».

Кейс 4. Побудова ризик-орієнтованої ESG-стратегії для великого підприємства

Підприємство хімічної промисловості в Україні готується до залучення міжнародних інвесторів. Нові вимоги вимагають від нього прозорої екологічної (E), соціальної (S) та управлінської (G) політики. Проте діючі процедури оцінювання ризиків переважно зосереджені на фінансових загрозах.

Здійсніть трансформацію системи ризик-менеджменту із включенням ESG-факторів. Побудуйте матрицю «ризик – вплив – відповідальність», обґрунтуйте використання кількісних та якісних індикаторів для оцінювання ризиків сталого розвитку та сформулюйте підхід до прийняття рішень на рівні правління.

Кейс 5. Розробка системи управління ризиками для досягнення цілей сталого розвитку в територіальній громаді

Територіальна громада у післякризовий період планує впровадити програму сталого розвитку: енергоефективність, екологічне відновлення, цифровізація послуг. Проте існує високий рівень управлінських ризиків – недофінансування, відсутність цифрових навичок у персоналу, низька довіра з боку мешканців.

Застосовуючи системний підхід до управління ризиками, сформуйте дерево цілей та відповідних ризиків, визначте механізми контролю, адаптації та моніторингу на рівні громади. Запропонуйте інтегровану модель управління проєктами із вбудованим ризик-менеджментом.

Висновок по розділу 4

Управління ризиками є ключовим компонентом ефективного системного управління організаціями та інфраструктурними комплексами в умовах постійної невизначеності і складності. Розглянутий розділ висвітлює як теоретичні основи, так і практичні інструменти, що забезпечують системний підхід до ідентифікації, аналізу та мінімізації ризиків.

Теорія корисності, дерево рішень та матриця наслідків створюють комплексний аналітичний каркас для прийняття оптимальних рішень у середовищі ризику. Ці інструменти дають змогу враховувати різні сценарії, суб’єктивні переваги та потенційні наслідки, що підвищує якість

управлінських рішень. Водночас системні стратегії мінімізації і уникнення ризиків дозволяють не лише зменшувати імовірність негативних подій, але й побудувати гнучкі сценарії реагування. Важливим аспектом є оцінка ефективності рішень у багатокритеріальному контексті, що відображає складність сучасного бізнес-середовища та багатофакторність цілей організацій.

Підхід ERM (Enterprise Risk Management) у системному управлінні дає змогу організаціям інтегрувати процеси управління ризиками на всіх рівнях діяльності, забезпечуючи комплексний контроль та послідовність дій. Підсистеми моніторингу, швидкої реакції та адаптації створюють динамічну структуру, що дозволяє оперативно реагувати на нові виклики, підтримувати стабільність і конкурентоспроможність. Корпоративна культура безпеки відіграє фундаментальну роль, формуючи спільні цінності та відповідальність, необхідні для ефективного управління ризиками у всіх підрозділах.

Критична інфраструктура є основою національної безпеки та економічної стійкості, тому класифікація критичних систем і розуміння їх вразливостей є першочерговим завданням управління ризиками. Оцінка ризиків з урахуванням cascading-ефектів дозволяє виявити потенційні ланцюгові негативні наслідки, які можуть поширюватися між системами, створюючи додаткові виклики для безпеки. Сценарне планування та формування стратегічних резервів є ключовими інструментами, що підвищують готовність систем до надзвичайних ситуацій і сприяють збалансованому розподілу ресурсів.

Сталий розвиток вимагає інтегрованого підходу до безпеки, що поєднує екологічні, соціальні та управлінські фактори. ESG-критерії стають стратегічним орієнтиром для оцінки і управління ризиками, що впливають на довгострокову життєздатність організацій і суспільств. Глобальні ризики – кліматичні, кібернетичні, соціальні – мають транснаціональний характер і здатні кардинально змінювати соціоекономічні системи. Врахування цих ризиків в рамках системного управління є необхідною умовою забезпечення адаптивності, інноваційності та сталості в сучасних умовах.

Таким чином, системне управління ризиками – це динамічний, комплексний процес, що інтегрує аналітичні методи, стратегічне планування та корпоративну культуру. Воно спрямоване на забезпечення безперервності діяльності, підвищення стійкості систем і підтримку сталого розвитку в умовах невизначеності та глобальних викликів.

ВИСНОВКИ

Навчальний посібник «Системний аналіз та прогнозування ризиків» комплексно висвітлює теоретико-методологічні основи, сучасні системні підходи до ідентифікації, оцінки, моделювання та управління ризиками в умовах складності, динамічності та невизначеності різноманітних систем. Представлений матеріал охоплює ключові напрями досліджень у сфері системного аналізу ризиків, починаючи з фундаментальних понять і принципів системного мислення, і закінчуючи інноваційними технологіями прогнозування та цифровими платформами моніторингу.

Розділ 1 послужив міцним фундаментом, що дозволяє глибше зрозуміти сутність системного підходу у вивченні ризиків. Історія виникнення системного аналізу демонструє еволюцію від класичних концепцій фон Берталанфі, Форрестера та Черчмана до сучасних міждисциплінарних досліджень, які включають інтеграцію кіберфізичних і соціотехнічних систем. Основні поняття – система, структура, зв’язки, середовище – сформували загальну мову дослідження ризиків, що забезпечує узгодженість у визначенні типів систем (технічних, соціальних, кіберфізичних) і їхньої поведінки в умовах взаємодії з зовнішнім середовищем.

Методологічні принципи системного аналізу, такі як цілісність, ієрархічність і зворотний зв’язок, є ключовими для моделювання і прогнозування ризиків, дозволяючи розглядати ризики не ізольовано, а як результат складної взаємодії підсистем і факторів. Інструментарій, який включає побудову причинно-наслідкових діаграм, системну динаміку, когнітивне моделювання та метод аналізу ієрархій (AHP), надає практичні засоби для всебічної оцінки ризиків та їхніх джерел.

Розділ 2 поглибив знання про методи виявлення та оцінювання ризиків у складних системах, що характеризуються високим ступенем невизначеності та множинними взаємозв’язками. Застосування системно орієнтованих підходів у виявленні небезпек та вразливостей, а також методів картування ризиків, формує комплексну картину потенційних загроз.

Мультикритеріальні методи (AHP, TOPSIS, ELECTRE) дозволяють інтегрувати суб'єктивні експертні оцінки з об'єктивними даними, що підвищує достовірність і гнучкість прийняття рішень у сфері ризик-менеджменту. Вивчення моделей нечіткої логіки, інтервального аналізу та байєсівських мереж розкриває методологію роботи з невизначеністю та чутливістю систем, а когнітивне моделювання в соціально-технічних системах допомагає розробляти адаптивні сценарії управління ризиками в динамічних умовах.

Третій розділ сфокусований на прогнозуванні ризиків із використанням моделей, які враховують динаміку та часові затримки, що притаманні реальним системам. Системна динаміка за Форрестером з петлями зворотного зв’язку і методи імітаційного та агентного моделювання надають потужні засоби для аналізу розвитку ризикових процесів у часі.

Застосування класичних статистичних методів, таких як регресійні моделі, ARIMA та часові ряди, у поєднанні з експертними підходами (дельфі-методом) формує основу для надійного прогнозування ризиків. Особливе місце посідає інтеграція штучного інтелекту: нейронні мережі, глибоке навчання та машинне навчання відкривають нові горизонти для виявлення прихованих патернів і аномалій ризиків, що підвищує якість прийняття управлінських рішень.

Інформаційні системи та цифрові платформи моніторингу, такі як цифрові двійники, IoT-середовища і інструменти візуалізації, забезпечують оперативний збір, аналіз і відображення системних ризиків, що підвищує прозорість і ефективність управління.

Четвертий розділ окреслив управління ризиками як невід'ємний складник системного управління в організаціях та критичних інфраструктурах. Теоретичні засади системного прийняття рішень, зокрема теорія корисності, дерева рішень, багатокритеріальні матриці, формують рамки для розробки стратегій мінімізації і уникнення ризиків.

Інтеграція ризик-менеджменту в загальну систему управління організацією через ERM, моніторинг і адаптаційні підсистеми, а також формування корпоративної культури безпеки є критично важливими для сталого функціонування і розвитку. Особлива увага приділяється управлінню ризиками у критичній інфраструктурі з урахуванням каскадних ефектів та сценарного планування.

Підхід до забезпечення сталого розвитку через призму системної безпеки та врахування ESG-факторів розширює контекст ризик-менеджменту, включаючи глобальні виклики кліматичних, кібернетичних і соціальних ризиків, що визначають нові вимоги до системного аналізу і прогнозування.

Навчальний посібник «Системний аналіз та прогнозування ризиків» представляє собою цілісний комплекс знань, що поєднує класичні наукові теорії з сучасними практичними інструментами і технологіями. Він слугує не лише теоретичною базою, а й практичним керівництвом для фахівців з ризик-менеджменту, системних аналітиків, дослідників складних соціально-технічних систем, а також для студентів і аспірантів відповідних спеціальностей.

Увага до міждисциплінарного підходу, інтеграція цифрових технологій і штучного інтелекту в процеси прогнозування і управління ризиками відкривають широкі перспективи подальших досліджень і впровадження інноваційних методів у практику.

В умовах зростаючої складності і динамічності систем, підвищення невизначеності і взаємозалежностей між компонентами, системний аналіз ризиків набуває особливої актуальності як інструмент забезпечення безпеки, надійності і сталого розвитку сучасних організацій, інфраструктур і суспільства загалом.

ГЛОСАРІЙ ТЕРМІНІВ:

Cascading effects (каскадні ефекти) – ефекти «доміно», коли одна подія в системі спричиняє ланцюг взаємопов'язаних наслідків. Наприклад, відмова одного елемента може призвести до лавиноподібного колапсу всієї мережі.

Dashboard (дашборд) – інтерактивний інтерфейс, що забезпечує зведене відображення ключових показників і даних у режимі реального часу для підтримки управлінських рішень.

Delphi-метод – метод багатоетапного експертного опитування з дотриманням анонімності та статистичною обробкою результатів, який дає змогу досягти колективного консенсусу.

Digital Twin (цифровий двійник) – віртуальна модель фізичного об'єкта чи процесу, що у режимі реального часу відображає його стан і функціонування на основі даних сенсорів.

Edge computing (крайова обробка даних) – технологія обробки даних, яка виконується максимально близько до джерела їх створення (наприклад, на IoT-пристроях чи сенсорах), а не у віддаленій хмарній інфраструктурі.

ELECTRE / MACBETH – методи багатокритеріального прийняття рішень, що ґрунтуються на попарному порівнянні альтернатив і побудові системи пріоритетів.

ERM (Enterprise Risk Management) – комплексна система управління ризиками, інтегрована на всі рівні діяльності організації (стратегічний, тактичний, операційний).

ESG-фактори – фактори сталого розвитку, що охоплюють три виміри: Environmental (екологічні), Social (соціальні) та Governance (управлінські).

Fail-safe (відмова-безпечний режим) – проєктне рішення чи система, що у разі збою автоматично переходить у безпечний стан або мінімізує можливі негативні наслідки.

FMEA (Failure Mode and Effects Analysis) – метод системного аналізу потенційних відмов у системі та оцінки їхніх можливих наслідків.

Fishbone-діаграма (діаграма Ісікави, «кістяк риби») – інструмент для структурованого аналізу причин виникнення проблем чи ризиків.

Fuzzy AHP / Fuzzy TOPSIS – модифікації класичних методів багатокритеріального аналізу рішень, що враховують невизначеність і нечіткість (fuzzy logic).

GRC (Governance, Risk and Compliance) – інтегрована система корпоративного управління, управління ризиками та дотримання нормативних вимог.

Heatmap (теплова карта) – графічне представлення даних у вигляді кольорової карти, де інтенсивність кольору відображає величину показника.

IDEF / SAD – методи структурного аналізу та моделювання систем і процесів (наприклад, IDEF0 – для функціонального моделювання).

IoT-середовище (Internet of Things) – середовище, у якому фізичні об’єкти (пристрої) підключені до мережі та здійснюють обмін даними між собою і зовнішніми системами.

SMART / SWING – методи оцінювання та визначення вагових коефіцієнтів критеріїв у багатокритеріальному аналізі рішень.

SWOT-аналіз – метод стратегічного аналізу, що оцінює внутрішні фактори (Strengths – сильні сторони, Weaknesses – слабкі сторони) та зовнішні (Opportunities – можливості, Threats – загрози).

Сенсорний аналіз – процес оцінювання даних, що надходять від сенсорів (датчиків), для виявлення змін, відхилень чи аномалій у системі.

Tree of Faults (дерево відмов) – ієрархічна модель, що графічно відображає причини, які можуть призвести до критичних відмов у системі.

What-if analysis (аналіз «що, якщо») – метод дослідження сценаріїв, що дозволяє оцінити можливі наслідки гіпотетичних змін у змінних чи умовах.

Fuzzy AHP / Fuzzy TOPSIS – модифікації класичних методів багатокритеріального аналізу рішень з урахуванням нечіткої (fuzzy) логіки.

GRC – Governance, Risk and Compliance – інтегрована система управління, ризиків і дотримання нормативних вимог (зазвичай у корпоративному контексті).

Heatmap – графічне представлення даних у вигляді кольорової карти, яка відображає інтенсивність показників.

IDEF / SAD – методи структурного аналізу і моделювання систем і процесів (наприклад, IDEF0 – для функціонального моделювання).

IoT-середовище – середовище, де фізичні об’єкти (пристрої) підключені до мережі та обмінюються даними – Інтернет речей.

SMART / SWING – методи оцінювання та вагового ранжування критеріїв у багатокритеріальному аналізі рішень.

SWOT-аналіз – метод стратегічного аналізу, що оцінює внутрішні (Strengths, Weaknesses) і зовнішні (Opportunities, Threats) фактори.

Сенсорний аналіз – оцінювання даних, що надходять від сенсорів (датчиків) для виявлення змін або аномалій у системі.

Tree of Faults (дерево відмов) – модель, що ієрархічно відображає причини, які можуть призвести до критичних відмов у системі.

What-if analysis – метод аналізу сценаріїв: дослідження наслідків гіпотетичних змін у змінних або умовах.

Адаптивність – здатність системи змінювати свою поведінку або структуру відповідно до змін у зовнішньому чи внутрішньому середовищі.

Альтернатива – один із можливих варіантів вибору у процесі прийняття рішення, що конкурує з іншими за досягненням мети.

Взаємозв’язки – сукупність причинно-наслідкових або функціональних відношень між елементами системи.

Гомеостаз – властивість системи підтримувати внутрішню стабільність, навіть за умов змін у зовнішньому середовищі.

Декомпозиція – метод розкладання складної системи або задачі на

простіші компоненти для полегшення аналізу або управління.

Емерджентність – поява нових властивостей системи, які не зумовлені окремими її частинами, але виникають у результаті їх взаємодії.

Евристика – практичний підхід або правило, що дозволяє знаходити рішення швидко і без повного аналізу всіх варіантів.

Ідентифікація системи – процес встановлення її складу, структури та параметрів на основі спостереження або аналізу.

Інтеграція – процес об'єднання окремих частин у цілісну структуру з новими функціональними властивостями.

Когнітивна модель – уявне або формалізоване представлення знань, уявлень і переконань, які впливають на прийняття рішень.

Критерій ефективності – кількісний або якісний показник, що дозволяє оцінити доцільність або результативність рішення.

Матриця рішень – таблична форма представлення альтернатив, параметрів середовища та результатів вибору.

Метафора системи – образне уявлення про функціонування або структуру системи, що допомагає її краще зрозуміти.

Модель – умовне відображення об'єкта або процесу, створене для вивчення його властивостей, прогнозування або оптимізації.

Модель світу – суб'єктивне бачення реальності, на яке спирається суб'єкт у процесі аналізу чи прийняття рішень.

Моделювання – процес побудови та використання моделей для дослідження складних об'єктів і прогнозування їх поведінки.

Множинність критеріїв – ситуація, коли рішення має враховувати кілька (часто суперечливих) цілей або обмежень.

Невизначеність – брак точних або повних даних, що ускладнює прогнозування результатів дій або стану системи.

Обмеження – умови або межі, які звужують можливості для прийняття рішення чи дії в системі.

Оптимальність – властивість рішення, що забезпечує найкращий результат за заданим критерієм або кількома критеріями.

Оцінювання рішень – процес порівняння альтернатив за заданими критеріями для виявлення найбільш доцільного варіанту.

Параметр системи – характеристика, що описує певний аспект стану або поведінки системи у кількісній чи якісній формі.

Петля зворотного зв'язку – механізм, за якого результат впливає на подальший розвиток процесу чи зміну поведінки елементів.

Прийняття рішень – процес вибору одного з кількох можливих варіантів дій на основі аналізу даних, цілей і обмежень.

Раціональність – властивість рішення бути логічно обґрунтованим, послідовним і цілеспрямованим.

Система – сукупність взаємопов'язаних елементів, які функціонують як єдине ціле для досягнення певної мети.

Системна динаміка – метод дослідження змін системи у часі через моделювання потоків, запасів та зворотних зв'язків.

Сценарний аналіз – підхід до прогнозування майбутнього розвитку подій через побудову декількох логічних сценаріїв.

Точка прийняття рішення – момент або ситуація, у якій суб’єкт має обрати один із доступних варіантів дій.

Штучний інтелект – набір технологій, здатних імітувати інтелектуальні функції людини, зокрема аналіз, навчання та планування.

СПИСОК ЛІТЕРАТУРИ

1. Балтовський О.А., Ісмайлов К.Ю., Сіфоров О.І., Форос Г.В., Заєць О.М. Теорія систем і системний аналіз: навч.посібник /За заг. ред. д.т н., доц. О.А. Балтовського. Одеський держ. унів-т внутр. справ, 2020. 156 с.
2. Балтовський О.А., Форос Г.В., Пядишев В.Г., Сіфоров О.І. Системи підтримки прийняття рішень: навчальний посібник. Одеса: РВВ ОДУВС. 2022. 176 с.
3. Катренко А.В. Системний аналіз: підручник. К.: КНЕУ: Новий Світ, 2020. 396 с.
4. **Назарець О. В. Системний аналіз: Підручник. 2-е вид., перероб. і доп. Львів: Видавництво Львівської політехніки, 2022. 528 с.**
5. **Панасюк В. В. Системний аналіз: Підручник. 2-е вид., перероб. і доп. Київ: ВПЦ «Київський університет», 2022. 448 с.**
6. Прокопенко Т.О. Теорія систем і системний аналіз: навч.посіб. Черкаси: ЧДТУ, 2019. 139 с.
7. **Системний аналіз: навчальний посібник / В. В. Коваленко, В. М. Коваленко. 2-ге вид., перероб. та доп. К.: НТУУ «КПІ імені Ігоря Сікорського»,**
8. **Стефанюк В. О. Системний аналіз: Навчальний посібник. Київ: НУ «Львівська політехніка», 2021. 224 с.**
9. **Тарасюк Г. М. Управління проектами: навчальний посібник для студентів вищих навчальних закладів. 2 е вигляд. К.: Каравела, 2016. 320с.**
10. Тепман Л. Н. Ризики в економіці: Навч. посібник для студ. вузів / За ред. В. А. Швандар. К. 2012. 379 с.
11. Теоретичні основи забезпечення якості прийняття управлінських рішень в умовах європейської інтеграції : монографія / М. М. Новікова, Н. О. Кондратенко, М. В. Боровик та ін.; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : «Друкарня Мадрид», 2020. 335 с.
12. **Тихоненко В. В. Ризикують все, скрізь і завжди. Безпека та управління ризиками. Корпоративні системи. 2017. «1. с. 57 60**
13. **Управління ризиком у ринковій економіці / В. Н. Вяткін, В. А. Гамза, Ю. Ю. Катеринославський, Дж. Дж. Хемптон. К.: ЗАТ «Видання в «Економіка»», 2012. 195 с.**
14. **Уткін Е. А., Фролов Д. А. Управління ризиками підприємства: Навчально-практичний посібник. До: ТЕІС, 2013. 247 с.**
15. **Федоренко В. І. Системний аналіз: Підручник. 2-е вид., перероб. і доп. Харків: НТУ «ХПІ», 2022. 464 с.**
16. Фесік Л. І. Адаптивне управління: еволюція поняття та сутнісна характеристика. URL : http://umo.edu.ua/images/content/nashi_vydanya/metod_upr_osvit/v_5/29.pdf
17. Шарапов О.Д., Дербенцев В.Д. Системний аналіз. Навч метод. посібник для самостійного вивчення дисципліни. К.:КНЕУ, 2015. 154с.
18. **Шевчук В. В. Системний аналіз: Навчальний посібник. Київ: НТУУ «КПІ ім. Ігоря Сікорського», 2021. 208 с.**

позначено не підтверджені джерела