МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет кораблебудування
імені адмірала Макарова

МЕТОДИЧНІ ВКАЗІВКИ

до виконання практичних робіт за темою: «Ризик-стратегія в управлінні безпекою суб'єкта господарювання у надзвичайних ситуаціях»

Рекомендовано Методичною радою НУК

ВИДАВНИЦТВО
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
КОРАБЛЕБУДУВАННЯ
ІМ. АДМІРАЛА МАКАРОВА
2023

УДК 351.86.614.8
М64

Автори:
В. А. Дубінін, канд. військ. наук, доцент кафедри адміністративного та конституційного права Національного університету кораблебудування імені адмірала Макарова;
Л. М. Маркіна, д-р техн. наук, професор кафедри аудиту та технологій захисту довкілля Державного закладу «Державна екологічна академія післядипломної освіти та управління»;
С. Ю. Ушкац, канд. фіз.-мат. наук, доцент кафедри екології та природоохоронних технологій Національного університету кораблебудування імені адмірала Макарова;
Н. Ю. Жолобенко, аспірант кафедри екології та природоохоронних технологій Національного університету кораблебудування імені адмірала Макарова;
О. В. Власенко, науковий співробітник проблемної науково-дослідної лабораторії прикладної екології Державного закладу «Державна екологічна академія післядипломної освіти та управління»

Рецензенти:
І. Л. Михелєв, канд. техн. наук, доцент;
С. С. Коваль, канд. техн. наук, доцент

Рекомендовано Методичною радою НУК

Г20 **Методичні** вказівки до виконання практичних робіт за темою: «Ризик-стратегія в управлінні безпекою суб'єкта господарювання у надзвичайних ситуаціях» / В. А. Дубінін, Л. М. Маркіна, С. Ю. Ушкац, Н. Ю. Жолобенко, О. В. Власенко. – Миколаїв : НУК, 2023. – 80 с.

Матеріали методичних вказівок допоможуть у формуванні світоглядних та етичних основ здорового способу життя і підвищенні інформаційно-просвітницького рівня населення з питань безпеки життєдіяльності. Вони можуть бути науково-методичним підґрунтям при вирішенні завдань забезпечення безпеки людей, профілактики травматизму та стійкості функціонування суб'єктів господарювання в умовах надзвичайних ситуацій, зумовлених небезпечними техногенними та природними процесами.

Призначено для студентів ЗВО всіх спеціальностей денної, заочної та інших форм навчання, які вивчають дисципліну «Безпека життєдіяльності» або «Техногенна безпека», а також для викладачів цієї дисципліни.

УДК 351.86.614.8

ЗМІСТ

Перелік використаних скорочень....4
Вступ....6
1. Основи теорії ризику....8
1.1. Поняття ризику....8
1.2. Класифікація видів ризику....13
1.3. Методологія аналізу та оцінки ризику....16
1.4. Послідовність проведення аналізу ризику....19
1.5. Якісні методи аналізу ризику....21
1.6. Кількісна оцінка ризику....26
2. Логіко-графічні методи аналізу ризику....32
2.1. Визначення та символи, що використовуються при побудові дерев....32
2.2. Аналіз дерева відмов....36
2.3. Побудова дерева відмов....37
2.4. Якісна і кількісна оцінка дерева відмов....47
2.5. Аналітичний висновок для простих схем дерева відмов....48
2.6. Дерево з повторюваними подіями....50
2.7. Ймовірнісна оцінка дерева відмов....51
2.8. Переваги та недоліки методів дерева відмов....56
3. Застосування теорії ризику для оцінки рівня безпеки....58
3.1. Критерії прийнятного ризику....58
3.2. Управління ризиком....62
3.3. Застосування теорії ризику в технічних системах....65
3.4. Оцінка ризику аварій....70
Список використаних джерел....76

ПЕРЕЛІК ВИКОРИСТАНИХ СКОРОЧЕНЬ

АНВ – аналіз наслідків відмов;

АНДП – аналіз небезпек за допомогою «дерева причин»;

АНДН – аналіз небезпек за допомогою «дерева наслідків»;

АНМПВ – аналіз небезпек методом потенційних відхилень;

АПП – аналіз помилок персоналу;

БЖД – безпека життєдіяльності;

В – вибух;

ВПА – вихідна подія аварії;

З – забруднення;

ЗНЕ – зливно-наливна естакада;

Л – лабораторія;

ЛВ – летальні випадки;

ЛЗР – легкозаймиста рідина;

НЗ – випадки непрацездатності;

НПС – навколишнє природне середовище;

НС – надзвичайна ситуація;

О – отруєння;

Підсистема «АБО» – частина системи, компоненти якої з'єднані послідовно;

Підсистема «І» – частина системи, компоненти якої з'єднані паралельно;

ПНС – продуктово-насосна станція;

П – пожежа;

ПНА – причинно-наслідковий аналіз;

ПАТ – попередній аналіз небезпек;

ПХ – приміщення для зберігання СНП;

ППБЕ – порушення правил будови та експлуатації пристрою;

ППБ – порушення правил пожежної безпеки;

РП – резервуарний парк;

СНС – єдина система попередження надзвичайних ситуацій;

СНП – світлі нафтопродукти;

ССП – спринклерна система пожежогасіння;

СП – система пожежогасіння;

ТТ – технологічний трубопровід.

ВСТУП

На Землі немає такої людини, якій не загрожують небезпеки. Реалізуючись у просторі і часі, небезпеки загрожують не тільки людині, а й суспільству, державі і всьому світу в цілому. Тому профілактика безпеки і захист від них – найактуальніша проблема, у вирішенні якої повинні бути зацікавлені не тільки окремі особистості, а й держава і вся світова спільнота.

У той же час не можна забезпечити абсолютну безпеку для особистості, суспільства, держави. Під безпекою розуміється такий рівень небезпеки, з яким на даному етапі розвитку людства можна змиритися. Безпека – це прийнятний ризик. Щоб його досягти, необхідне вироблення ідеології безпеки, формування відповідного рівня мислення і поведінки людини і суспільства в цілому. Саме цими проблемами і займається наука «Безпека життєдіяльності».

Сьогодні Безпека життєдіяльності (БЖД) спирається на усвідомлену потребу суспільства, на правила безпечної поведінки, вироблені практикою або суміжними областями науки, на закони держави і міжнародного права з безпеки і захисту населення. Однак цього недостатньо. В основі БЖД повинні бути систематизовані й узагальнені знання про об'єктивні закономірності існування і розвитку природи, людини та суспільства.

Майбутні фахівці повинні бути готові до дій в екстремальних умовах надзвичайних ситуацій (НС) з метою вибо-

ру оптимальних і правильних рішень, спрямованих на захист персоналу установ, об'єктів економіки і населення, а також на істотне ослаблення (запобігання) впливу різних вражаючих факторів НС. Тому студентам необхідно знати ризик-стратегію в управлінні безпекою суб'єкта господарювання у надзвичайних ситуаціях.

1. ОСНОВИ ТЕОРІЇ РИЗИКУ

1.1. Поняття ризику

Ризик – це кількісна оцінка небезпеки, яка чисельно дорівнює ймовірності небажаної з точки зору безпеки події.

Стосовно до проблеми безпеки життєдіяльності такою подією може бути погіршення здоров'я або смерть людини, аварія або техногенна катастрофа, небезпечне природне явище, забруднення навколишнього середовища, руйнування екологічної системи, загибель групи людей або зростання смертності населення, збільшення соціальної напруженості, матеріальний збиток від реалізації небезпек або збільшення витрат на безпеку.

Під терміном «збиток» розуміють фактичні й імовірні економічні втрати та (або) погіршення стану природного середовища внаслідок змін у навколишньому середовищі.

Ступінь ризику являє собою двокомпонентну величину, яка характеризується збитком від впливу конкретного небезпечного фактора і ймовірністю його виникнення. Чисельно ступінь ризику дорівнює добутку ймовірності небажаної з точки зору безпеки події на шкоду, що наноситься цією подією.

Фактор ризику – це подія, явище або процес, який безпосередньо не завдає будь-якої шкоди, але збільшує ймовірність виникнення несприятливої з точки зору безпеки події.

Аналітично ризик виражає частоту реалізації небезпек по відношенню до можливого їх числа. В загальному вигляді

$$R = \frac{N(t)}{Q(f)}, \tag{1.1}$$

де R – ризик; N – кількісний показник числа небажаних подій в одиницю часу t; Q – число об'єктів, схильних до певного фактора ризику.

Поняття «ризик» включає в себе ще один аспект – це кількісна характеристика дії небезпек, що формуються конкретною діяльністю людини. Наприклад, кількість смертельних випадків, кількість випадків захворювання, кількість випадків тимчасової та постійної непрацездатності (інвалідності), спричиненої дією на людину будь-якого небезпечного фактора (електричний струм, шкідлива речовина, предмет, що рухається, тощо), віднесених на певну кількість жителів (працівників) за конкретний період часу.

Значення ризику для конкретного небезпечного фактора можна отримати зі статистики нещасних випадків, випадків захворювання тощо за різні проміжки часу: зміну, добу, тиждень, квартал, рік.

Імовірність виникнення небезпеки (ризику) – величина, істотно менша одиниці. Крім того, область можливої реалізації небезпеки поширена в просторі й часі. У термінах ризику прийнято описувати також небезпеки від достовірних подій, які відбуваються з імовірністю, що є рівною одиниці, наприклад забруднення навколишнього середовища відходами конкретного промислового підприємства. У цьому випадку «ризик» еквівалентний збитку й величина ризику дорівнює величині збитку.

Таким чином, кількісна оцінка ризику є процесом оцінки чисельних значень ймовірності і наслідків небажаних процесів, явищ, подій.

Небезпеки можуть реалізуватися у формі травм, захворювань або загибелі людини тільки в тому випадку, якщо область формування небезпек (ноксосфера) перетинається

з областю, в якій можливе перебування людини (гомосфера). У виробничих умовах – це джерело небезпеки (один з елементів виробничого середовища) і робоча зона (рис. 1.1).

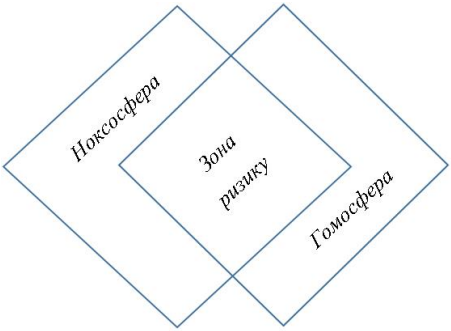


Рис. 1.1. Область дії небезпеки на людину

Загальний ризик для людей виражається двома категоріями:

– індивідуальний ризик, який визначається як ймовірність того, що людина зазнає певний вплив у ході своєї діяльності;

– соціальний ризик, який визначається як співвідношення між кількістю людей, загиблих в одній аварії, і ймовірністю цієї аварії.

У виробничих умовах розрізняють індивідуальний і колективний ризик.

Індивідуальний ризик характеризує реалізацію небезпеки певного виду діяльності для конкретного індивідуума – виробничий травматизм і професійна захворюваність, частота нещасних випадків і професійних захворювань.

Колективний ризик – це ймовірність травмування або загибелі двох або більше осіб від впливу небезпечних і шкідливих виробничих факторів.

Як відомо, основна аксіома безпеки стверджує, що абсолютна безпека неможлива, тобто ймовірність загибелі людини за жодних умов не може дорівнювати нулю. Тому найменшим рівнем ризику прийнято вважати прийнятний ризик.

Сучасне суспільство займає егоцентричні позиції, вважається, що людське життя безцінне. Але в реальному світі за все доводиться платити, в тому числі і за безпеку. Реально існує межа, за якою витрати на досягнення більш високого рівня безпеки сприймаються суспільством і окремими людьми як надмірні. Так, наприклад, ризик загибелі людини в дорожньо-транспортній пригоді в 2018 році в Україні склав 1,04, 10^{-4} (за офіційними даними МВС), а в Німеччині $5 \cdot 10^{-5}$. Показники відрізняються приблизно в 2,04 разів. При цьому кліматичні умови, автомобілі, правила дорожнього руху і люди в цих країнах цілком порівнянні і нема пояснення такої відмінності. Зрозуміло, що причини слід шукати в організації дорожнього руху, а, отже, у витратах на безпеку дорожнього руху, які в цих країнах прийнято вважати достатніми.

Прийнятний ризик – це ймовірність загибелі людини, з якою суспільство на даному етапі свого розвитку готове примиритися і на зниження якого воно не готове витрачати додаткові кошти. Це певний оптимальний рівень, при якому витрати на безпеку і тяжкість наслідків від впливу даного небезпечного фактора врівноважують один одного на думку тих, хто має реальну владу в даному конкретному суспільстві людей.

Використання ризику як єдиного показника шкоди при оцінці дії різних небезпечних і шкідливих факторів на людину застосовується для обґрунтованого порівняння безпеки різних галузей економіки і типів робіт, аргументації соціальних переваг і пільг для певної категорії осіб тощо.

Класифікація джерел небезпеки і рівні ризику загибелі людини від їх впливу представлені в таблиці 1.1.

Величина ризику є не тільки оцінкою безпеки для якоїсь одної галузі промисловості, а й для оцінки зміни рівня безпеки з часом і за різних умов праці, для кількісного встановлення діапазону ризику для всієї промисловості в цілому.

Таблиця 1.1. **Класифікація джерел і рівнів ризику смерті людини у промислово розвинених країнах (*R* – кількість смертельних випадків – людина на рік)**

Джерело	Причина	Середнє значення
Внутрішнє середовище організму людини	Генетичні та соматичні захворювання, старіння	$R_{ср} = 0{,}6…10^{-2}$
Природне середовище проживання	Нещасний випадок через вплив стихійних лих (землетруси, урагани, повені тощо)	загальний $R_{ср} = 10^{-5}$: – повені 4×10^{-6}; – землетруси 3×10^{-6}; – грози 6×10^{-7}; – урагани 3×10^{-8}
Техносфера	Нещасні випадки; захворювання, викликані забрудненням навколишнього середовища	$R_{ср} = 10^{-4}...10^{-6}$
Професійна діяльність	Професійні захворювання, нещасні випадки на виробництві (під час професійної діяльності)	– безпечна $R_{ср} = 10^{-4}$; – відносно безпечна $R_{ср} = 10^{-3}...10^{-4}$; – небезпечна $R_{ср} = 10^{-2}…10^{-3}$; – особливо небезпечна $R_{ср} > 10^{-2}$
Соціальне середовище	Самогубства, злочини, військові дії	$R_{ср} = (0{,}5 – 1{,}5)\times10^{-4}$

Очікуваний (прогнозований) ризик *R* – це добуток частоти реалізації конкретної небезпеки *f* на добуток імовірностей знаходження людини в «зоні ризику» при різному регламенті технологічного процесу:

$$R = f\prod_{i}^{n} p_i, \qquad (1.2)$$

де *f* – число нещасних випадків (смертельних випадків) від даної небезпеки чол./рік (для вітчизняної практики $f = Кч/10^{-3}$,

тобто відповідає значенню коефіцієнта частоти нещасного випадку Кч, поділеного на 1000); $\prod_{i}^{n} p_i$ – добуток імовірностей перебування працівника в «зоні ризику» для кожного *i*-го фактора.

Використання формули (1.2) для оцінки ймовірності виробничого ризику зручно тим, що дозволяє визначати величини ризиків впливу різних негативних факторів для конкретного технологічного процесу виробництва, проводити оцінку значущості кожного фактора з позиції безпеки.

1.2. Класифікація видів ризику

Залежно від факторів ризику та об'єктів ризику розрізняють індивідуальний, техногенний, екологічний, соціальний та економічний ризик.

Індивідуальний ризик – це ймовірність реалізації потенційних небезпек при виникненні небезпечних ситуацій для однієї людини. Його можна визначити як відношення кількості людей, загиблих від реалізації фактора ризику до загальної кількості людей, що піддаються впливу даного фактора за певний період часу:

$$Ri = \frac{P(t)}{L(f)}, \tag{1.3}$$

де *Ri* – індивідуальний ризик; *P* – число постраждалих (загиблих) в одиницю часу *t* від певного фактора ризику *f*; *L* – число людей, схильних до відповідного фактора ризику в одиницю часу *t*.

Джерелом індивідуального ризику у виробничій сфері є професійна діяльність, а найбільш поширеним фактором ризику – небезпечні і шкідливі виробничі фактори.

Технічний ризик виражає ймовірність аварії або катастрофи при експлуатації машин, механізмів, реалізації технологічних процесів, будівництві та експлуатації будівель і споруд:

$$Rm = \frac{\Delta T(t)}{T(f)}, \tag{1.4}$$

де Rm – технічний ризик; ΔT – число аварій в одиницю часу t на ідентичних технічних системах і об'єктах; T – число ідентичних технічних систем і об'єктів, схильних до загального фактора ризику f.

Найбільш поширені фактори технічного ризику: помилковий вибір за критеріями безпеки напрямків розвитку техніки і технологій; вибір потенційно небезпечних конструктивних схем і принципів дії технічних систем; експлуатаційних навантажень; неправильний вибір конструкційних матеріалів; недостатній запас міцності; відсутність у проєктах технічних засобів безпеки; неякісне доведення конструкції, технології, документації за критеріями безпеки; заданого хімічного складу конструкційних матеріалів; недостатня точність конструктивних розмірів; порушення режимів термічної та хіміко-термічної обробки деталей; регламентів складання і монтажу конструкцій і машин; використання техніки не за призначенням; порушення паспортних (проєктних) режимів експлуатації; несвоєчасні профілактичні огляди та ремонти; порушення вимог транспортування і зберігання.

Екологічний ризик – це можливість появи непереборних порушень у стані навколишнього середовища: забруднення місцевості шкідливими виробничими відходами, зміна кліматичних особливостей території (наприклад, опустелювання або заболочування земель), радіоактивне забруднення, кислотні опади і т. д.

З точки зору кількісної оцінки поняття «екологічний ризик» може бути сформульовано як відношення величини можливого збитку від впливу шкідливого екологічного фактора за певний інтервал часу до нормованої величини інтенсивності цього фактора. Під можливим збитком насамперед мається на увазі здоров'я людини.

Екологічний ризик виражає ймовірність екологічного лиха, катастрофи, порушення подальшого нормального функціонування та існування екологічних систем і об'єктів у результаті антропогенного втручання в природне середовище або стихійного лиха. Небажані події екологічного ризику можуть проявлятися як безпосередньо в зонах втручання, так і за їх межами:

$$Ro = \frac{\Delta O(t)}{O}, \tag{1.5}$$

де Ro – екологічний ризик; ΔO – число антропогенних екологічних катастроф і стихійних лих в одиницю часу t; O – число потенційних джерел екологічних руйнувань на розглянутій території.

Масштаби екологічного ризику R_o^m оцінюються процентним співвідношенням площі кризових або катастрофічних територій ΔS до загальної площі розглянутого біогеоценозу S:

$$R_o^m = \frac{\Delta S}{S} 100. \tag{1.6}$$

У сучасних умовах основним джерелом екологічного ризику є техногенний вплив на навколишнє природне середовище, а найбільш поширеними факторами екологічного ризику – забруднення водойм, атмосферного повітря шкідливими речовинами, ґрунтів відходами виробництва; зміна газового складу повітря; енергетичне забруднення біосфери.

Соціальний ризик характеризує масштаби і тяжкість негативних наслідків надзвичайних ситуацій, а також різного роду явищ і перетворень, що знижують якість життя людей. По суті – це ризик для групи або спільноти людей. Оцінити його можна, наприклад, по динаміці смертності, розрахованій на групу з 1000 осіб:

$$R_c = \frac{1000(C_2 - C_1)}{L}(t), \tag{1.7}$$

де *Rc* – соціальний ризик; C_1 – число померлих в одиницю часу *t* (смертність) у досліджуваній групі на початку періоду спостереження до розвитку надзвичайної події; C_2 – смертність у тій же групі людей в кінці періоду спостереження, наприклад на стадії загасання надзвичайної ситуації; *L* – загальна чисельність досліджуваної групи.

Економічний ризик визначається співвідношенням користі і шкоди, одержуваних товариством від розглянутого виду діяльності:

$$Re = \frac{\text{В}}{\text{П}} 100, \qquad (1.8)$$

де *Re* – економічний ризик, %; В – шкода суспільству від розглянутого виду діяльності; П – користь.

Використання розглянутих видів ризику дозволяє знайти оптимальні рішення щодо забезпечення безпеки як на рівні окремого підприємства, так і в більших масштабах.

1.3. Методологія аналізу та оцінки ризику

Методологічне забезпечення аналізу ризику являє собою сукупність методів, методик і програмних засобів, що дозволяють всебічно виявити небезпеки й оцінити ризик надзвичайної ситуації.

При вирішенні комплексних питань безпеки широко застосовується методологія ризику, яка заснована на визначенні ймовірності небажаних подій і тяжкості їх наслідків. Використовуючи кількісні показники ризику, можна оцінювати потенційну небезпеку і порівнювати небезпеки різної природи. При цьому під показниками небезпеки найчастіше розуміють індивідуальний або соціальний ризик загибелі людей або ризик заподіяння шкоди.

Аналіз ризику є невід'ємною частиною системного підходу до прийняття політичних рішень і практичних заходів при вирішенні завдань попередження або зменшення небезпеки

для життя людини, шкоди майну і навколишньому середовищу, званого управління ризиком.

Оцінка ризику – це аналіз походження (виникнення) і масштабів ризику в конкретній ситуації.

Ступінь ризику розглядається як добуток ймовірності виникнення конкретної небезпечної події і величини збитку від його наслідків. Ступінь ризику можна представити як математичне очікування величини збитку від небажаної події:

$$R(m) = \sum_{i=1}^{n} pi \times mi, \qquad (1.9)$$

де *pi* – ймовірність настання події, пов'язаної зі збитком; *mi* – величина збитку, заподіяного економіці.

Оскільки ймовірність настання несприятливої події – величина безрозмірна, а збиток вимірюється в грошових одиницях (у гривнях), то ступінь ризику також має розмірність грошових одиниць, що зручно при прийнятті управлінських рішень.

Значення індивідуального ризику використовується для кількісної оцінки потенційної небезпеки на конкретному робочому місці або для певного виду діяльності.

Значення соціального ризику застосовується для інтегральної кількісної оцінки небезпечних виробничих об'єктів та характеристики масштабу впливу аварії.

Можна виділити три загальні складові процесу управління ризиком:

– збір інформації про поточний стан виробничої безпеки;

– аналіз ризику;

– контроль виробничої безпеки.

Аналіз ризику базується на зібраній інформації та визначає заходи щодо контролю безпеки, тому основним завданням аналізу ризику є обґрунтування рішень при управлінні ризиком (рис. 1.2).

Аналіз ризику або ризик-аналіз – це систематичне використання наявної інформації для виявлення небезпек і оцінки

ризику для осіб або груп населення, майна або навколишнього середовища.

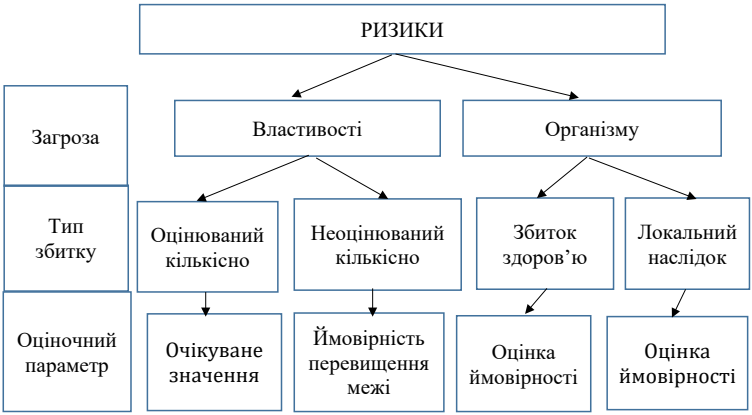


Рис. 1.2. Схема аналізу ризику

Аналіз ризику полягає у виявленні небезпек і оцінці ступеня ризику. При цьому під небезпекою розуміється джерело потенційного збитку або шкоди (або ситуація з можливістю нанесення шкоди), а під ідентифікацією небезпеки – процес виявлення і визнання, що небезпека існує, і визначення її характеристик.

Оцінка ризику включає в себе аналіз частоти виникнення небажаних з точки зору безпеки подій і аналіз наслідків цих подій.

Аналіз ризику проводиться за наступною схемою:

1. Планування та організація проведення аналізу ризику.
2. Ідентифікація небезпек.
2.1. Виявлення небезпек.
2.2. Попередня оцінка характеристик небезпек.
3. Оцінка ризику.
3.1. Аналіз частоти виникнення небезпечних подій.
3.2. Аналіз наслідків цих подій.
3.3. Аналіз невизначеностей при аналізі ризику.
4. Розробка рекомендацій з управління ризиком.

Застосовувані методи (методики) повинні задовольняти наступним вимогам:

– відповідність розглянутій технічній системі;

– вони повинні ґрунтуватися на принципах і критеріях, установлених у чинній нормативно-технічній документації;

– отримані результати повинні сприяти найкращому розумінню характеру небезпеки, дозволяти виявити найбільш «слабкі» місця і процеси в системі функціонування об'єкта і намітити оптимальні шляхи управління ризиком.

1.4. Послідовність проведення аналізу ризику

1. Планування та організація робіт. На цьому етапі необхідно:

– вказати причини, що викликали необхідність проведення аналізу ризику;

– ідентифікувати й описати аналізовану технічну систему;

– підібрати команду виконавців, які залучаються для проведення аналізу ризику;

– встановити робочі джерела інформації про безпеку системи;

– визначити вихідні дані для аналізу ризику;

– проаналізувати невизначеності аналізу ризику;

– визначити цілі аналізу ризику та критерії прийнятного ризику.

2. Ідентифікація небезпек. Основне завдання – на основі зібраної інформації про об'єкт і досвіду роботи подібних систем виявити всі властиві даній технічній системі небезпеки. На цьому ж етапі проводиться попередня оцінка небезпек з метою вибору одного з трьох напрямків діяльності:

а) у разі незначності виявлених небезпек припинити подальший аналіз;

б) при значній невизначеності виявлених небезпек провести більш детальний попередній аналіз ризику;

в) виробити рекомендації щодо зменшення небезпек.

У першому випадку процес аналізу ризику може закінчуватися вже на етапі ідентифікації небезпек.

3. Оцінка ризику. З усіх ідентифікованих небезпек необхідно вибрати небезпеки з неприйнятним рівнем ризику. При цьому критерії прийнятного ризику і результати оцінки ризику можуть бути виражені якісно (у вигляді текстового опису) або кількісно (наприклад, у вигляді кількості нещасних випадків або аварій на рік).

Оцінка ризику включає в себе аналіз ймовірності виникнення небезпечної події і аналіз тяжкості наслідків цих подій. Однак, коли тяжкість наслідків незначна або подія вкрай малоймовірна, досить оцінити один параметр. Для аналізу частоти зазвичай використовуються:

– історичні дані за відповідними типами технічних систем або видами діяльності;

– статистичні дані щодо аварійності та надійності обладнання;

– логічні методи аналізу «дерева подій» або «дерева відмов»;

– експертна оцінка з урахуванням думки фахівців у даній області.

Аналіз тяжкості наслідків включає в себе оцінку впливу на людей, майно або навколишнє середовище. Для прогнозування наслідків необхідно розуміти сутність аварійних процесів, діючих вражаючих факторів і оцінити ступінь ураження досліджуваних об’єктів впливу.

В ході проведення оцінки ризику слід проаналізувати можливу невизначеність результатів, викликану неточністю інформації по надійності обладнання і помилках персоналу, а також прийнятими допущеннями в застосовуваних при розрахунку моделях аварійного процесу.

Аналіз невизначеності – це оцінка невизначеності результатів оцінки ризику, викликаної невизначеністю вихідних даних і точністю використаних моделей.

Слід підкреслити, що часто складні і дорогі розрахунки дають значення ризику, точність якого дуже невелика.

Якісні (інженерні) методи аналізу ризику дозволяють досягати основних цілей аналізу ризику при використанні меншого обсягу інформації і витрат праці. Однак кількісні методи оцінки ризику завжди дуже корисні, а в деяких ситуаціях – і єдино можливі, зокрема, для порівняння небезпек різної природи або при експертизі особливо небезпечних складних технічних систем.

4. Розробка рекомендацій з управління ризиком. Існуючий ризик може бути визнаний прийнятним, в іншому випадку необхідно вказати заходи щодо зменшення ризику. Заходи з управління ризику можуть мати технічний, експлуатаційний або організаційний характер.

Слід зауважити, що іноді можуть відбуватися події, що вважалися раніше надзвичайно малоймовірними. Тяжкість наслідків таких подій може бути дуже велика. Наприклад, катастрофа океанського лайнера «Титанік» або аварія на японській атомній електростанції «Фукусіма». В обох випадках відбулися природні катаклізми, які раніше ніколи не спостерігалися і вважалися неймовірними. Технічні системи потрапили в умови експлуатації, при яких їх функціонування стало неможливим.

1.5. Якісні методи аналізу ризику

Існують наступні методи ідентифікації можливих небезпек:

1. Інженерні методи. На основі зібраних статистичних даних проводиться ймовірнісний аналіз небезпек і побудова дерев небезпеки.

2. Модельні методи. За накопиченими вихідними даними і результатами спостережень будують моделі впливу шкідливих і небезпечних факторів на окрему людину, на професійні та соціальні групи населення.

3. Експертні методи. Проводиться оцінка ймовірностей небезпечних подій опитуванням експертів у даній галузі науки, техніки або технологій.

4. Соціологічні методи. Визначаються ймовірності небезпечних подій шляхом опитування населення.

Для більш точної і достовірної оцінки ризику ці методи застосовують спільно.

Якісні методи аналізу небезпек дозволяють визначити джерела виникнення небезпек, можливі аварії або нещасні випадки, розробити заходи для запобігання небезпечних подій і для зниження тяжкості їх наслідків.

Перед проведенням якісного аналізу необхідно ідентифікувати джерела небезпек. Для цього збирають вихідні дані і проводять попередній аналіз небезпек.

При аналізі небезпек вибір певного якісного методу залежить від мети аналізу та особливостей технічної системи. Існують наступні якісні методи аналізу небезпек:

– попередній аналіз небезпек;
– аналіз наслідків відмов;
– аналіз небезпек за допомогою «дерева причин»;
– аналіз небезпек за допомогою «дерева наслідків»;
– аналіз небезпек методом потенційних відхилень;
– аналіз помилок персоналу;
– причинно-наслідковий аналіз.

Попередній аналіз небезпек (ПАН) полягає у виявленні джерела небезпек, визначенні причин виникнення небезпечних станів і характеристиці небезпек у залежності від викликаних ними наслідків.

Порядок здійснення попереднього аналізу небезпек:

1. Визначення технічних характеристик технічної системи, процесу, використовуваних джерел енергії, матеріалів та їх властивостей, які ушкоджуються.

2. Пошук нормативно-технічної документації, дія якої поширюється на дану технічну систему або процес.

3. Здійснюють перевірку використовуваної технічної документації на її відповідність нормам і правилам безпеки.

4. Складають перелік небезпек, в якому вказують ідентифіковані джерела небезпек, можливі вражаючі фактори, хід протікання потенційних аварій та інші виявлені недоліки.

В ході ПАН проводиться перша спроба виявити потенційно небезпечні частини технічної системи й окремі події, які можуть привести до виникнення небезпек. Цей аналіз виконується на початковому етапі розробки системи. Детальний аналіз можливих подій зазвичай проводиться після того, як система повністю визначена за допомогою дерева відмов.

Аналіз наслідків відмов (АНВ) – якісний метод ідентифікації небезпек, заснований на системному підході, що дозволяє зробити певні прогнози. АНВ є аналізом індуктивного типу, за допомогою якого систематично, на основі послідовного розгляду одного елемента за іншим, аналізуються всі можливі види відмов або аварійні ситуації і виявляється їх результуючий вплив на систему. Вивчення окремих аварійних ситуацій і відмов елементів дозволяють визначити їх вплив на інші прилеглі елементи і систему в цілому. АНВ здійснюють у наступному порядку:

1. Технічну систему поділяють на складові компоненти.

2. Для кожного компонента системи виявляють усі можливі відмови.

3. Вивчають усі потенційні аварії, які можуть бути викликані відмовами компонентів досліджуваного об’єкта.

4. Відмови, які ранжують за ступенем небезпеки і розробляють заходи, що дозволяють уникнути виникнення цих відмов.

За допомогою АНВ можна оцінити потенційну небезпеку будь-якого технічного об’єкта.

Аналіз небезпек за допомогою «дерева причин» потенційної аварії (АНДП) дозволяє виявити комбінації відмов обладнання, помилки персоналу і зовнішніх впливів, що

призводять до аварійної ситуації (основної події). АНДП виконують у наступному порядку:

1. Вибирають можливу подію-аварію або відмову, яка може призвести до аварії.

2. Виявляють фактори, які можуть призвести до заданої аварії.

3. Будують орієнтований граф «дерево», вершина (корінь) якого є потенційною аварією.

Проведення аналізу за допомогою «дерева причин» можливо тільки після детального вивчення робочих функцій усіх компонентів розглянутої технічної системи. На роботу системи впливає людський фактор, наприклад, можливість здійснення оператором помилки. Тому бажано всі потенційні інциденти – «відмови операторів» – вводити в зміст дерева причин-відмов. Дерево відображає статичний характер подій. Побудовою декількох дерев можна відобразити їх динаміку, тобто розвиток подій у часі. Для визначення послідовності подій при аварії, що включає складні взаємодії між технічними системами забезпечення безпеки, використовується дерево подій.

Аналіз небезпек за допомогою «дерева наслідків» потенційної аварії (АНДН) відрізняється від АНДП тим, що в цьому випадку задається критична подія – ініціатор, і досліджують всю групу подій – наслідків, до яких вона може привести. Аналіз причин наслідків починається з вибору критичної події. Критичні події вибирають таким чином, щоб вони служили зручними відправними точками для аналізу, причому більшість аварійних ситуацій розвивається за критичною подією у вигляді ланцюга окремих подій. Процедура побудови діаграми-дерева наслідків складається з вибору першого ініціюючого події, за яким слідують інші події, визначені на даному етапі роботи.

При аналізі причин-наслідків використовуються комбіновані методи «дерева відмов (виявити причини) і дерева по-

дій (показати наслідки)», причому всі явища розглядаються в природній послідовності їх появи.

Аналіз небезпек методом потенційних відхилень (АНПВ) включає в себе процедуру штучного створення відхилень за допомогою ключових слів. Для цього розбивають технологічний процес або технічну систему на складові частини і, створюючи за допомогою ключових слів відхилення, систематично вивчають їх потенційні причини і ті наслідки, до яких вони можуть привести на практиці.

Аналіз помилок персоналу (АПП) є одним з найважливіших елементів методології оцінки небезпек і дозволяє врахувати вплив людського фактора, тобто врахувати як помилки, що ініціюють або погіршують аварійну ситуацію, так і здатність персоналу здійснювати коригувальні дії з управління аварією.

АПП включає наступні етапи:

1. Вибір системи і виду роботи.
2. Визначення мети.
3. Ідентифікація виду потенційної помилки.
4. Ідентифікація наслідків.
5. Ідентифікація можливості виправлення помилки.
6. Ідентифікація причини помилки.
7. Вибір методу запобігання помилки.
8. Оцінка ймовірності помилки.
9. Оцінка ймовірності виправлення помилки.
10. Розрахунок ризику.
11. Вибір шляхів зниження ризику.

Причинно-наслідковий аналіз (ПНА) виявляє причини аварії або катастрофи і є складовою частиною загального аналізу небезпек. Він завершується прогнозом нових аварій і складанням плану заходів щодо їх попередження. ПНА включає в себе наступні етапи:

1. Точний і об’єктивний опис аварії.
2. Визначення подій, що передували аварії.

3. Побудова орієнтованого графіка «дерева причин», починаючи з останньої стадії розвитку подій, тобто з самої аварії.

4. Виявлення логічних зв'язків «дерева причин».

5. Розробка попереджувальних заходів для виключення повторення аналогічних аварій.

1.6. Кількісна оцінка ризику

Кількісний аналіз небезпек дає можливість розрахувати ймовірності виникнення небезпечних подій і тяжкість наслідків цих подій. Для проведення кількісного аналізу застосовуються статистичний аналіз і різні методи розрахунку ймовірностей.

Для зручності розрахунків складні системи розбивають на підсистеми. Підсистемою називають частину системи, яку виділяють за певною ознакою, що відповідає конкретним цілям і завданням функціонування системи. Підсистема може розглядатися як самостійна система, що складається з інших підсистем, тобто ієрархічна структура складної системи може складатися з підсистем різних рівнів, де підсистеми нижчих рівнів входять складовими частинами в підсистеми вищих рівнів. У свою чергу, підсистеми складаються з компонентів-частин системи, які розглядаються без подальшого поділу як єдине ціле.

Логічний аналіз внутрішньої структури системи і визначення ймовірності небажаних подій як функції окремих складових подій є одним із завдань аналізу небезпек.

Підсистемою «І» називають ту частину системи, компоненти якої з'єднані паралельно. До відмови такої підсистеми призводить відмова всіх її компонентів.

Якщо відмови компонентів можна вважати взаємно незалежними, то ймовірність відмови в підсистемі «І»:

$$P(A) = \prod_{i=1}^{n} P(A_i), \qquad (1.10)$$

де $P(A)$ – ймовірність події A (відмова всієї підсистеми «І»); $P(A_i)$ – ймовірність відмови i-го компонента підсистеми «І»; n – загальна кількість компонентів підсистеми «І».

На практиці створення підсистем «І» здійснюється дублюванням або резервуванням. Даний технічний прийом застосовують у разі, якщо необхідно досягти високого ступеня надійності системи, особливо в системах, що забезпечують безпеку.

Підсистемою «АБО» називають частину системи, компоненти якої з'єднані послідовно. До небажаної події в такій підсистемі призводить відмова будь-якого компонента підсистеми.

Якщо відмови компонентів взаємно незалежні, то ймовірність відмови в підсистемі «АБО»:

$$P(A) = 1 - \prod_{i=1}^{n} \left(1 - P\left(A_i\right)\right). \qquad (1.11)$$

Для рівноможливих відмов імовірність відмови в цій підсистемі:

$$P(A) = 1 - (1 - p)^n. \qquad (1.12)$$

Цей вислів свідчить про високу ймовірність відмови у складних систем, навіть якщо вони складаються з елементів з високою надійністю. Наприклад, при ймовірності відмови компонента $p = 0{,}05$ підсистема «АБО», що складається з 20 компонентів ($n = 20$), має ймовірність того, що відмови в підсистемі не відбудеться, дорівнює

$$(1 - p)^n = (1 - 0{,}05)^{20} = 0{,}358.$$

При аналізі ризику слід враховувати наступні аспекти:

1. Пристрої, операції, дії персоналу, які з точки зору безпеки виконують одні і ті ж функції в системі, можуть вважатися з'єднаними паралельно.

2. Пристрої, операції, дії персоналу, кожні з яких необхідно для запобігання небезпечної події, повинні розглядатися як з'єднані послідовно.

На практиці часто підсистеми «І» чи «АБО» можуть складатися з компонентів, у свою чергу з'єднаних у підсистеми «І» чи «АБО» в будь-яких комбінаціях.

Імовірність виникнення небезпеки – величина, істотно менша одиниці. Крім того, точки реалізації небезпеки розподілені в просторі і часі. Це означає, що, наприклад, імовірність пожежі в одній будівлі населеного пункту набагато вище, ніж ймовірність одночасної пожежі всіх будівель цього населеного пункту. Або ймовірність п'яти поспіль дуже холодних зим набагато нижче однієї дуже холодної зими.

Таким чином, чим більший відрізок часу або кількість суб'єктів, які ризикують, ми візьмемо, тим визначенішим стане величина збитку, який суб'єкти отримають у сукупності за цей відрізок часу.

У термінах ризику прийнято описувати і небезпеки від достовірних подій, що відбуваються з імовірністю, рівною одиниці. Таким прикладом є забруднення навколишнього середовища відходами конкретного промислового підприємства. У цьому випадку «ризик» еквівалентний ступеню ризику і, відповідно, величина ризику дорівнює величині збитку.

Зазвичай при оцінці ступеня ризику його характеризують двома величинами – ймовірністю події P і наслідками X, які у вираженні математичного очікування виступають як співмножники:

$$R = P \cdot X. \tag{1.13}$$

По відношенню до джерел небезпек оцінка ризику передбачає розмежування нормального режиму роботи $R_{н}$ і аварійних ситуацій $R_{ав}$:

$$R = R_{н} + R_{ав} = P_{н}X_{н} + P_{ав}X_{ав}. \tag{1.14}$$

У разі, коли наслідки невідомі, то під ризиком розуміють ймовірність настання певного поєднання небажаних подій:

$$R = \sum_{i=1}^{n} P\,I. \tag{1.15}$$

При необхідності можна використовувати визначення ризику як ймовірності перевищення межі x:

$$R = P\{\xi > x\}, \tag{1.16}$$

де ξ – випадкова величина.

Техногенний ризик оцінюють за формулою, що включає ймовірність небажаної події і величину наслідків у вигляді збитку U:

$$R = PU. \tag{1.17}$$

Якщо кожній небажаній події, що відбувається з імовірністю P_i, відповідає збиток U_i, то величина ризику буде являти собою очікувану величину збитку U^*:

$$R = U^* = \sum_{i=1}^{n} P_i U_i. \tag{1.18}$$

Якщо всі ймовірності настання небажаної події однакові ($P_i = P$, i = 1, ..., n), то

$$R = P \sum_{i=1}^{n} U_i . \tag{1.19}$$

Коли існує небезпека здоров'ю та матеріальним цінностям, ризик доцільно представляти у векторному вигляді з різними одиницями вимірювання за координатними осями:

$$\vec{R} = \vec{U}\,\vec{P}. \tag{1.20}$$

Перемноження в правій частині цього рівняння проводиться покомпонентно, що дозволяє порівнювати ризики.

Індивідуальний ризик можна визначити як очікуване значення заподіяної шкоди U^* за інтервал часу T і віднесене до групи людей чисельністю M людей:

$$R = U^*/(MT). \tag{1.21}$$

Загальний ризик для групи людей (колективний ризик)

$$R = U^*/T. \tag{1.22}$$

Приклад. Провести чисельну оцінку ризику надзвичайної події в технічній системі, що складається з 3-х підсистем, з незалежними відмовами. Ймовірності відмов підсистем: $P_1 = 10^{-3}$, $P_2 = 10^{-4}$, $P_3 = 10^{-2}$, очікувані збитки від відмов підсистем $U_1 = 10^6$ грн, $U_2 = 5 \cdot 10^6$ грн, $U_3 = 10^5$ грн.

Розв'язання. Визначимо величину ризику надзвичайної події технічної системи як очікувану величину збитку:

$$R = U = \sum_{i=1}^{3} P_i U_i = P_1 U_1 + P_2 U_2 + P_3 U_3 =$$

$$= 10^{-3} \cdot 10^6 + 10^{-4} \cdot 5 \cdot 10^6 + 10^{-2} \cdot 10^5 = 1000 + 500 + 1000 = 2500 \text{ грн.}$$

Приклад. Провести чисельну оцінку ризику надзвичайної події в технічній системі, що складається з 5-ти підсистем з незалежними рівно можливими відмовами $P = 10^{-2}$. Очікувані збитки від відмов підсистем $U_1 = 10^6$, $U_2 = 10^7$, $U_3 = 10^8$, $U_4 = 10^9$, $U_5 = 10^{10}$.

Розв'язання. Визначимо величину ризику надзвичайної події технічної системи з рівно можливими відмовами підсистем як очікувану величину збитку:

$$R = U = P \cdot \sum_{i=1}^{5} U_i = P \cdot \left(U_1 + U_2 + U_3 + U_4 + U_5\right) =$$

$$= 10 - 2\ (1 + 10 + 102 + 103 + 104)\ 106 = 11\ 110\ 000 \text{ грн.}$$

Контрольні питання

1. У чому полягає різниця між поняттями «ризик» і «ступінь ризику»?
2. Що таке «прийнятний ризик»?
3. Які види ризику можна виділити в залежності від факторів ризику та об'єктів ризику?
4. З якою метою проводять аналіз ризику?
5. Яка послідовність проведення аналізу ризику?
6. З якою метою проводять оцінку ризику? Порядок проведення оцінки ризику.

7. Які існують якісні методи аналізу небезпек? Який порядок здійснення аналізу небезпек якісними методами?

8. Для чого проводиться кількісний аналіз небезпек?

9. За якими формулами підраховується ймовірність відмови в підсистемі «І» та в підсистемі «АБО»?

10. У яких випадках ризик еквівалентний ступеню ризику?

2. ЛОГІКО-ГРАФІЧНІ МЕТОДИ АНАЛІЗУ РИЗИКУ

Виникнення і хід протікання промислових аварій і техногенних катастроф, як правило, характеризується комбінацією різних випадкових локальних подій, що виникають із заздалегідь невідомою ймовірністю на різних стадіях аварії (відмови обладнання; людські помилки при проєктуванні та експлуатації; впливу непередбачуваних форс-мажорних обставин). Для того, щоб виявити причинно-наслідкові зв'язки між цими подіями, необхідно застосувати логіко-графічні методи побудови дерев відмов і подій.

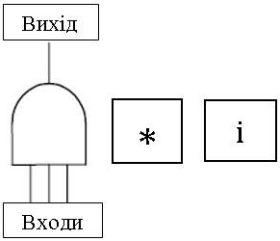
При побудові дерева відмов виявляються комбінації відмов обладнання, помилок персоналу і зовнішніх (природних або техногенних) впливів, що призводять до основної події (аварійної ситуації). Метод використовується для визначення можливості виникнення аварійної ситуації та розрахунку її ймовірності (на основі завдання ймовірностей вихідних подій).

Дерево подій – послідовність подій, що виходять з основної (кінцевої) події (аварійна ситуація). Застосовується для аналізу розвитку аварійної ситуації.

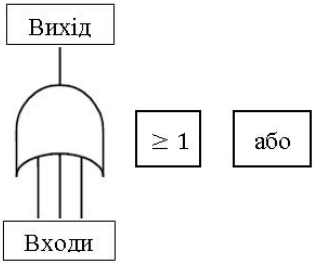
2.1. Визначення та символи, що використовуються при побудові дерев

При побудові дерев відмов і дерев подій прийнято використовувати спеціальні символи й умовні позначення. Нижче наведені найбільш часто вживані з них:

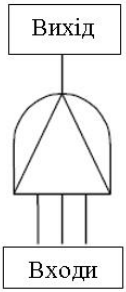
1. Схема «І» (схема збігу) – сигнал на виході з'являється тільки тоді, коли надходять всі вхідні сигнали (множення подій). Для умовного зображення схеми і застосовуються такі символи:



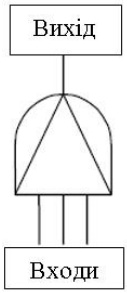
2. Схема «АБО» (схема об'єднання) – сигнал на виході з'являється при надходженні на вхід будь-якого одного або більшого числа сигналів (сума подій). Для умовного зображення схеми «АБО» застосовуються наступні символи:



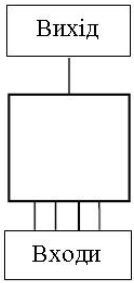
3. Схема виключає «АБО»: сигнал на виході розглядається як проміжна подія і з'являється при надходженні на вхід одного і тільки одного вхідного сигналу. Задля умовного зображення цієї схеми застосовується наступний символ:



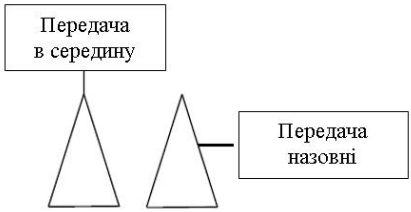
4. Схема «І» з пріоритетом: логічно еквівалентна схемі «І», але вхідні сигнали повинні надходити в певному, заздалегідь заданому порядку. Для умовного зображення схеми «І» з пріоритетом застосовується наступний символ:



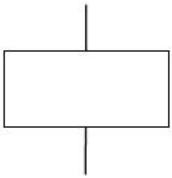
5. Спеціальна схема: відображає будь-яку іншу дозволену комбінацію вхідних сигналів, для її зображення використовується символ:



6. Вхід або вихід зображуються за допомогою трикутників, що дозволяє уникнути повторення окремих ділянок дерева. Пряма, вхідна в вершину трикутника, означає перехід всередину відповідної гілки, а пряма, що бере початок з середини бічної сторони трикутника – перехід до іншої гілки:

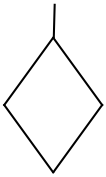


7. Результуюча подія: настає в результаті заздалегідь певної комбінації несправностей на вході логічної схеми. Для умовного позначення результуючої події застосовується наступний символ:



8. Первинна відмова (або несправність елемента), зображується у вигляді круга:

9. Неповна подія – це несправність, причини якої на даному етапі дослідження не вдалося однозначно визначити через відсутність необхідної інформації або вона не представляє інтересу. Така подія може бути деталізована шляхом показу первинних несправностей, які його викликають. Для умовного зображення неповної події застосовується наступний символ:



2.2. Аналіз дерев відмов

Небезпеки існують завжди, але явно проявляються лише у виняткових випадках. Для реалізації потенційної небезпеки необхідне виконання певних умов, які прийнято називати причинами виникнення небезпеки.

Небезпека-наслідок деякої причини або групи причин, які, в свою чергу, можуть бути наслідком іншої причини або групи причин. Причини і наслідки утворюють складні ієрархічні структури або системи, для графічної ілюстрації цих структур і систем використовують такі схеми: «дерево подій», «дерево причин», «дерево відмови», «дерево небезпеки», «дерево несправностей».

Процедура побудови дерева несправностей (відмов) включає, як правило, наступні етапи:

1. Визначення небажаної (завершальної) події.

2. Ретельне вивчення передбачуваного режиму використання системи та її можливу поведінку.

3. Визначення функціональних властивостей подій більш високого рівня для виявлення причин тих чи інших несправностей системи і проведення більш глибокого аналізу поведінки системи з метою виявлення логічного взаємозв'язку подій нижчого рівня, здатних привести до відмови системи.

4. Побудова дерева несправностей (відмов) для логічно пов'язаних подій на вході. Ці події повинні визначатися в термінах ідентифікованих незалежних первинних відмов. Щоб отримати кількісні результати для завершальної небажаної події дерева, необхідно задати ймовірність відмови, коефіцієнт готовності, інтенсивність відмов, інтенсивність відновлень та інші показники, що характеризують первинні події, за умови, що події дерева несправностей не є надлишковими.

Більш суворий і систематичний аналіз передбачає виконання наступних процедур: визначення меж системи, побудова дерева несправностей, якісна оцінка, кількісна оцінка.

Зазвичай система зображується у вигляді блок-схеми, що показує всі функціональні взаємозв'язки й елементи. При побудові дерева несправностей виключно важливу роль набуває правильне завдання граничних умов. Однією з основних вимог, що пред'являються до граничних умов, є вибір завершальної небажаної події, зробити який необхідно з особливою ретельністю, оскільки саме для нього і будується дерево несправностей. Крім того, щоб проведений аналіз був зрозумілий всім зацікавленим особам, дослідник зобов'язаний скласти перелік всіх припущень, прийнятих при визначенні системи і побудові дерева несправностей.

2.3. Побудова дерева відмов

Перш ніж приступити до побудови дерева несправностей, необхідно найретельнішим чином вивчити технічну систему. Дерево відмов використовується для умовного уявлення існуючих у технічній системі умов, потенційно здатних викликати її відмову, а також для виявлення існуючих в ній слабких з точки зору надійності місць. Залежно від конкретних цілей аналізу дерева несправностей для побудови останнього фахівці з надійності зазвичай використовують або метод первинних відмов, або метод вторинних відмов, або метод ініційованих відмов.

Метод первинних відмов. Відмова елемента називається первинною, якщо вона відбувається в нормальних умовах функціонування системи. Побудова дерева несправностей на основі обліку первинних відмов не становить великої складності, оскільки дерево будується тільки до тієї точки, де ідентифіковані первинні відмови елементів, які викликають відмову системи. Для ілюстрації цього методу розглянемо наступний приклад (рис. 2.1). Вважається, що відмова вимикача полягає лише в тому, що він не замикається, відмовами електричної проводки можна знехтувати, а завершальною подією є відсутність освітлення від лампочки.

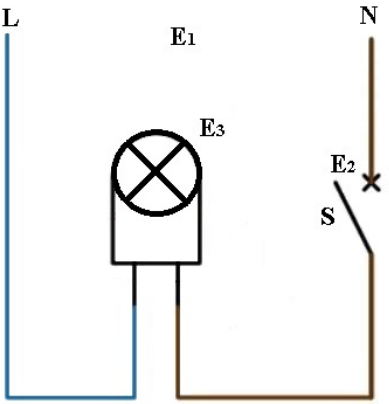


Рис. 2.1. Електрична схема системи освітлення

Дерево відмов для тієї системи представлено на рис. 2.2. Основними, або первинними, подіями дерева несправностей є відмова джерела живлення E_1, відмова вимикача E_2 і перегорання (відмова) лампочки E_3.

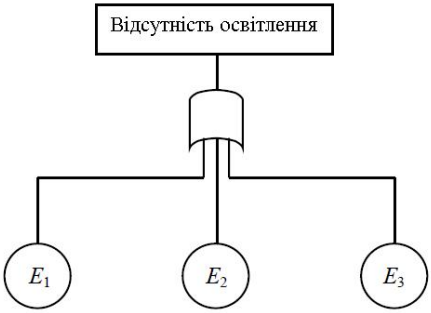


Рис. 2.2. Дерево відмов
для випадку первинних відмов

Найбільший інтерес становить завершальна подія «відсутність освітлення», і тому саме йому приділяється основна увага при аналізі. Дерево несправностей, зображене на рисунку, показує, що вихідні події являють собою входи схеми «АБО»: при настанні будь-якої з трьох первинних

подій E_1, E_2, E_3 відбувається завершальна подія (відсутність освітлення).

Метод вторинних відмов. Так як вторинні відмови можуть викликатися несприятливим впливом навколишніх умов, надмірними навантаженнями на елементи системи в процесі експлуатації або первинними відмовами самих елементів системи, необхідно більш глибоке дослідження технічної системи. На рис. 2.3 показано просте дерево несправностей із завершальною подією «припинення вироблення електроенергії генератором». Дерево відмов відображає такі первинні події, як відмова вимикача (відсутність замикання), несправності внутрішніх ланцюгів генератора і запобіжника. Вторинні відмови зображуються прямокутником як проміжна подія. Вторинні відмови відбуваються внаслідок незадовільного технічного обслуговування, несприятливого впливу зовнішнього середовища, стихійного лиха і т. д.

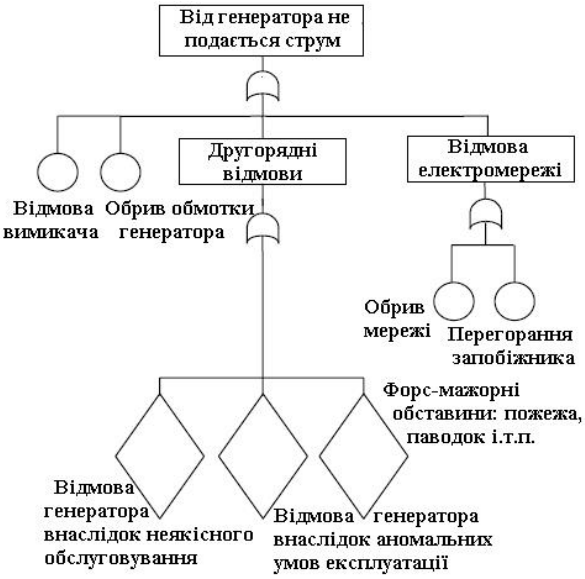


Рис. 2.3. Дерево несправностей
для випадку вторинних відмов

Метод ініційованих відмов. Подібні відмови виникають при правильному використанні елемента, але в невстановлений час або в недозволеному місці. Іншими словами, ініційовані відмови – це збої операцій координації подій на різних рівнях дерева несправностей: від первинних відмов до завершальної події (небажаної або кінцевої).

Типовим прикладом ініційованої відмови є надходження помилкового сигналу на будь-який електротехнічний пристрій (наприклад, двигун або перетворювач). Взаємозв'язок між основними та ініційованими відмовами показано на рис. 2.4.

Рис. 2.4. Дерево несправностей для випадку основних та ініційованих відмов

Різноманіття причин аварійності і травматизму найбільш повно і зручно представляється у вигляді діаграми-дерева причин, що відображає процес появи і розвитку ланцюга передумов. Основними компонентами діаграми причин або небезпек є вузли (або вершини) і взаємозв'язки між ними. Під вузлами маються на увазі події, властивості і стани елементів даної системи, а також логічні умови їх трансформації (додавання «АБО» і перемноження «І»).

Операція «І» означає, що перед тим, як відбудеться деяка подія «А», має відбутися кілька подій, наприклад, «Б» і «В». У ймовірнісному аспекті така операція виражається логічним множенням:

$$P(A) = P(Б)\cdot P(В). \qquad (2.1)$$

Операція «АБО» означає, що деяка подія «Г» буде мати місце, якщо відбудеться хоча б одна з декількох подій або всі події, наприклад, «Д» і «Е». У цьому випадку ймовірність появи події «Г» матиме вигляд алгебраїчної суми:

$$P(Г) = P(Д) + P(Е) – P(Д)\cdot P(Е). \qquad (2.2)$$

Приклад. Загибель людини від ураження електричним струмом може статися за умов, коли тіло стає частиною ланцюга з достатньою для нанесення ураження силою струму. Отже, щоб стався нещасний випадок (головна подія «А»), необхідне одночасне існування трьох подій (рис. 2.5).

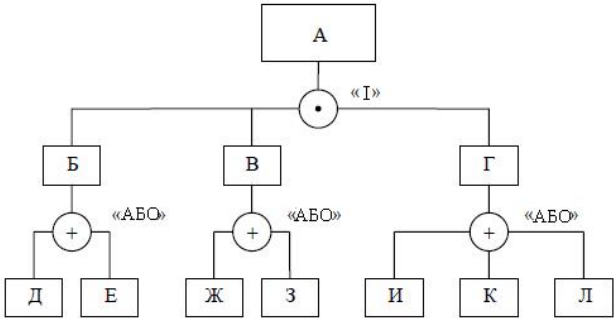


Рис. 2.5. Дерево причин ураження людини електричним струмом

Подія «Б» – наявність потенційно високої напруги на корпусі електричної установки.

Подія «В» означає появу людини на струмопровідному фундаменті, з'єднаному з землею.

Подія «Г» – торкання тілом людини корпусу електроустановки.

У свою чергу, подія «Б» може бути наслідком будь-якої з двох подій-передумов «Д» і «Е», де «Д» – зниження опору ізоляції струмоведучих частин, «Е» – дотик струмоведучими частинами корпусу установки.

Подія «В» також обумовлюється двома передумовами: «Ж» – вступ людини на струмопровідний фундамент,

«З» – дотик незахищеною поверхнею тіла людини до заземлених елементів приміщення.

Подія «Г» є результатом появи однієї з трьох передумов: «І» – потреба ремонту, «К» – потреба техобслуговування, «Л» – використання електроустановки за призначенням, або нормальна експлуатація установки.

Аналіз дерева небезпеки полягає у виявленні умов, мінімально необхідних і достатніх для виникнення або невиникнення головної події «А». Аналітично вираз умови реалізації даного нещасного випадку має вигляд:

$$P(А) = P(Б)\cdot P(В)\cdot P(Г) =$$

$$= [P(Д) + P(Е)]\cdot[P(Ж) + P(З)]\cdot[P(І) + P(К) + P(Л)]. \quad (2.3)$$

Приклад. На автотранспортному підприємстві автомобіль-тягач через технічну несправність був відправлений у ремонт, а на заміну йому з резерву був узятий інший тягач. Ніхто не звернув уваги на те, що резервний тягач виявився іншої моделі. Зчіпний пристрій резервного тягача був такої ж конструкції, тільки розташований на іншій висоті від землі.

У дворі підприємства водій тягача приступив до зчеплення тягача з причепом. Через те, що зчіпні пристрої тягача і причепа були розташовані на різній висоті, зробити зчеплення виявилося неможливо. Водій покинув автомобіль для того, щоб з'ясувати причину неможливості зробити зчеплення, забувши поставити тягач на гальмо стоянки. У той момент, коли водій знаходився між причепом і тягачем, тягач через вібрацію, викликану працюючим двигуном, покотився назад по невеликому нахилу і придавив водія до рами причепа. В результаті водій отримав тілесні ушкодження середньої тяжкості. Дерево причин даного нещасного випадку представлено на рис. 2.6, де X_1 – зазвичай використовуваний тягач, який вийшов з ладу;

X_2 – інший тягач використовувався в роботі;
X_3 – відмінність у висоті причепа і нового тягача;
X_4 – здійснення зчіпки неможливе;
X_5 – водій стає між тягачем і причепом;
X_6 – невключене ручне гальмо;
X_7 – вібрації від працюючого двигуна;
X_8 – двір має ухил;
X_9 – тягач рухається до причепа;
X_{10} – водій затискається між причепом і тягачем;
N – нещасний випадок (травма).

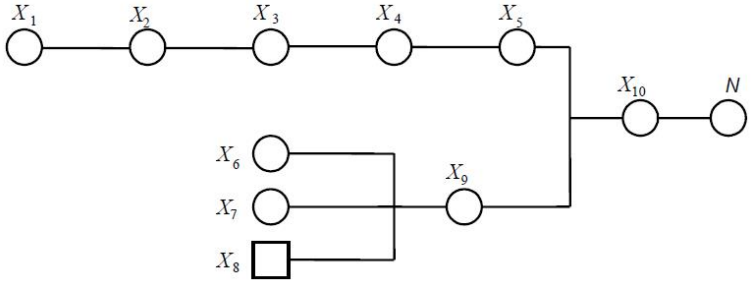


Рис. 2.6. Дерево причин аварії тягача

Зауважимо, що X_8 – фактор постійного характеру, а решта факторів носять випадковий характер.

Аналіз події полягає у з'ясуванні причин нещасного випадку, виявленні джерел небезпеки та виробленні попереджувальних заходів. Результати аналізу наведені в табл. 2.1.

Таблиця 2.1. **Результати аналізу події**

Причини нещасного випадку	Джерела небезпеки	Попереджувальні заходи
Двір з ухилом	Невідповідне місце стоянки автомобілів	Реконструкція двору
Тягач, що вийшов з ладу	Поломка обладнання	Попереджувальний ремонт транспортних засобів

Продовж. табл. 2.1

Різна висота з'єднувального пристрою причепа і тягача	Технічна несумісність обладнання	Стандартизація з'єднання обладнання
Невключене гальмо стоянки, працюючий двигун	Недостатня підготовка персоналу	Інструктаж водіїв

Приклад. При побудові «дерева подій» для визначення безпеки виконання зварювальних робіт вихідна подія аварії (ВПА) – іскра, що викликає загоряння. У разі виникнення задимлення в приміщенні автоматично спрацьовує спринклерна система пожежогасіння (ССП). При великому вогнищі пожежі необхідно відповідно до інструкції включити систему пожежогасіння (СП) і викликати пожежних. Можливе «дерево подій» представлене на рис. 2.7, де «сходинка» вгору означає спрацьовування відповідної системи, а «сходинка» вниз – її відмова.

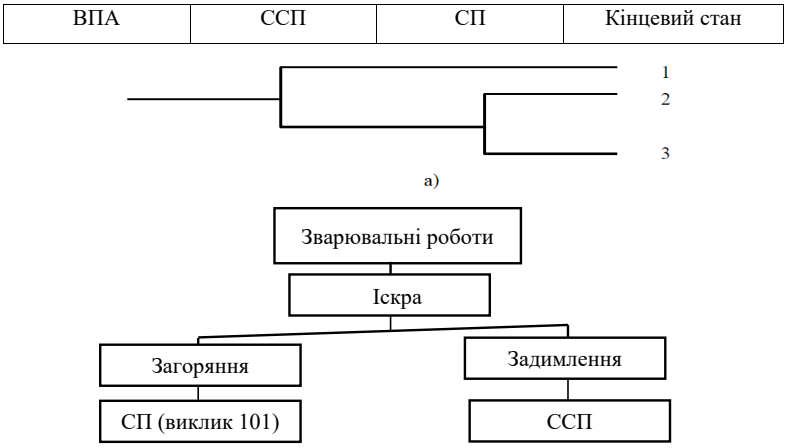


Рис. 2.7. Дерево подій при виконанні зварювальних робіт:
а – принципова схема; ***б*** – діаграма подій

Аналіз кінцевих умов показує, що стан під номером 3 пов'язаний з тяжкими наслідками, тому шлях, що приводить до кінцевого стану 3, є аварійним. Якщо відомі ймовірність настання ВПА і ймовірність відмов СПП і СП, то за допомогою методів теорії ймовірностей можна розрахувати ризик пожежі з тяжкими наслідками.

При аналізі чергової вихідної події аварії аналогічним чином будується відповідне «дерево подій», визначаються можливі аварійні ланцюжки і обчислюється ймовірність їх реалізації. В остаточному вигляді величина ризику $R = \sum r_i$, де r_i – ймовірність реалізації i-ого аварійного ланцюжка.

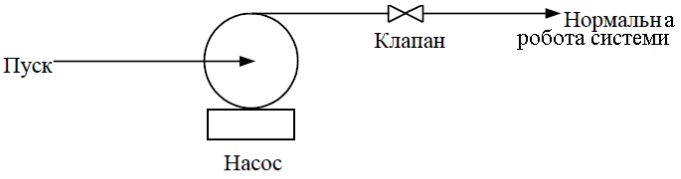
На рис. 2.8 показана система послідовно з'єднаних елементів, яка включає насос і клапан, що мають відповідно ймовірності безвідмовної роботи 0,98 і 0,95, а також наведено дерево рішень для цієї системи. Згідно з прийнятим правилом верхня гілка відповідає бажаному варіанту роботи системи, а нижня – небажаному. Дерево рішень розглядається зліва направо. Якщо насос не працює, система відмовляє незалежно від стану клапана. Якщо насос працює, за допомогою другої вузлової точки вивчається ситуація, чи працює клапан.

Імовірність безвідмовної роботи системи $P = 0{,}98 \cdot 0{,}95 = 0{,}931$. Імовірність відмови $Q = 0{,}98 \cdot 0{,}05 + 0{,}02 = 0{,}069$, і сумарна ймовірність двох станів системи дорівнює одиниці. Цей результат можна отримати іншим способом за допомогою таблиці істинності (табл. 2.2).

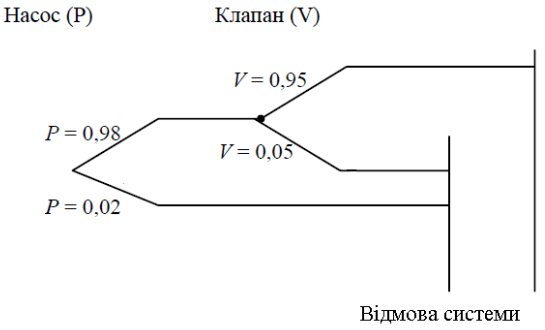
Таблиця 2.2. **Таблиця істинності**

Стан насоса	Стан клапана	Можливість працездатного стану системи	Можливість відмови системи
Працює	Працює	0,98–0,95	–
Відмова	Працює	–	0,02–0,95
Працює	Відмова	–	0,98–0,05
Відмова	Відмова	–	0,02–0,05
Сумарна величина		0,931	0,069

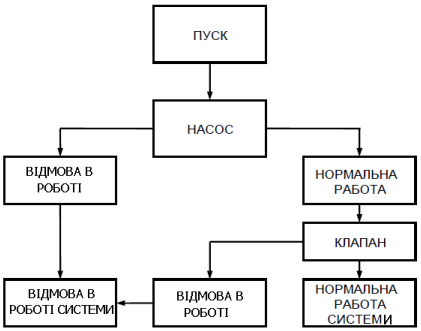
Методи аналізу дерев – найбільш трудомісткі, вони застосовуються для аналізу проєктів або модернізації складних технічних систем і виробництв та вимагають високої кваліфікації виконавців.



а)



б)



в)

Рис. 2.8. Дерево рішень для двохелементної схеми (робота насоса):
а – принципова схема; ***б*** – дерево рішень; ***в*** – діаграма рішень

2.4. Якісна і кількісна оцінка дерева відмов

Викладений нижче підхід заснований на використанні так званих мінімальних перетинів дерева несправностей. Перетин визначається як безліч елементарних подій, що призводять до небажаного результату. Якщо з безлічі подій, що належать деякому перетину, не можна виключити жодного і в той же час ця безліч подій призводить до небажаного результату, то в цьому випадку говорять про наявність мінімального перетину. Виявлення мінімальних перетинів вимагає великих витрат часу, і для їх знаходження потрібно машинний алгоритм. Приклад якісної оцінки дерева несправностей представлений на рис. 2.9.

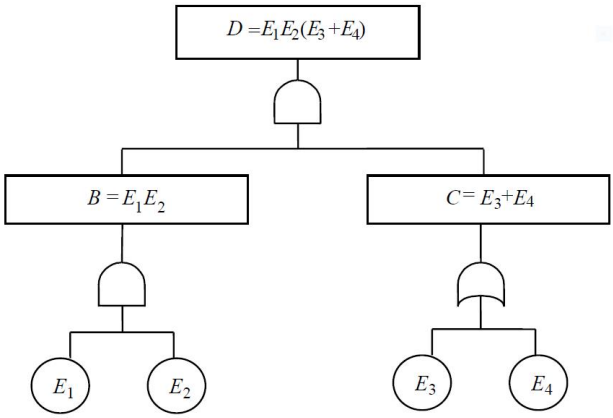


Рис. 2.9. Дерево несправностей для гіпотетичного випадку

Кількісна оцінка проводиться на підставі інформації про такі кількісні показники надійності для завершальної події, як імовірність відмови, інтенсивність відмов або інтенсивність відновлень. У першу чергу обчислюють показники надійності елемента, потім знаходять критичний шлях і, нарешті, оцінюють завершальну подію. Кількісна оцінка дерева здійснюється або статичним моделюванням, або аналітичним методом.

Примітка. Проміжна відмова може з'явитися тільки в тому випадку, коли мають місце обидві події E_1 і E_2. Що стосується проміжної події С, то вона може відбутися тільки при появі події E_3 або E_4. Завершальна подія настає тільки при появі одночасно проміжних подій В і С.

У першому випадку дерево несправностей моделюється на комп'ютері зазвичай для декількох тисяч або навіть мільйонів циклів функціонування системи. При цьому основними етапами моделювання є:

– задання показників надійності для елементарних подій;

– програмування моделі дерева несправностей;

– складання переліку відмов, що призводять до завершальної події, і переліку відповідних мінімальних перетинів;

– обчислення необхідних кінцевих результатів.

У другому випадку використовують існуючі аналітичні методи.

2.5. Аналітичний висновок для простих схем дерева відмов

Для того щоб дерево несправностей відповідало своєму призначенню, в ньому використовуються схеми, що показують логічні зв'язки між відмовами основних елементів системи і завершальною подією. Для представлення цих логічних схем у математичній формі застосовуються основні закони булевої алгебри.

Схема «АБО» зображується символами *U* або «+». Будь-який з цих символів показує об'єднання подій, пов'язаних зі схемою «АБО». Математичний опис схем «АБО» з двома подіями на вході наведено на рис. 2.10.

Подія B_0 на виході схеми «АБО» записується в булевій алгебрі як

$$B_o = B_1 + B_2, \qquad (2.4)$$

де B_1 і B_2 – події на вході.

Схема «І» зображується символом «·» або «П». Цей символ позначає перетин подій. Схема «І» з двома входами показана на рис. 2.11.

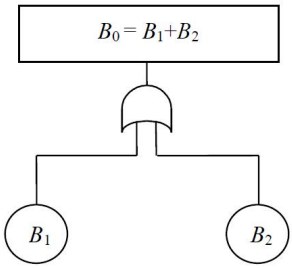


Рис. 2.10. Схема «АБО» з двома входами

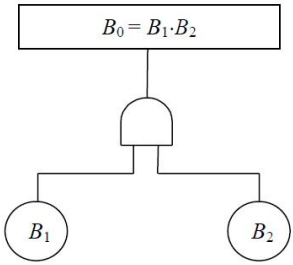


Рис. 2.11. Схема «І» з двома входами

Подія B_0 на виході схеми «І» записується в булевій алгебрі як

$$B_0 = B_1 \cdot B_2. \qquad (2.5)$$

Схема «І» з пріоритетом логічно еквівалентна схемі «І», але відрізняється від неї тим, що події на її вході повинні відбуватися в певному порядку. Схема «І» з пріоритетом, що має два входи, показана на рис. 2.12. У даному випадку передбачається, що подія A_1 має настати раніше події A_2.

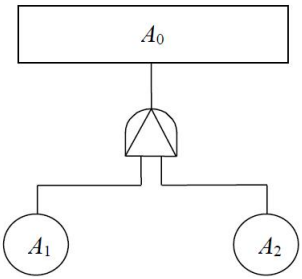


Рис. 2.12. Схема «І» з пріоритетом з двома входами

2.6. Дерево з повторюваними подіями

Характерна конфігурація такого дерева несправностей показана на рис. 2.13.

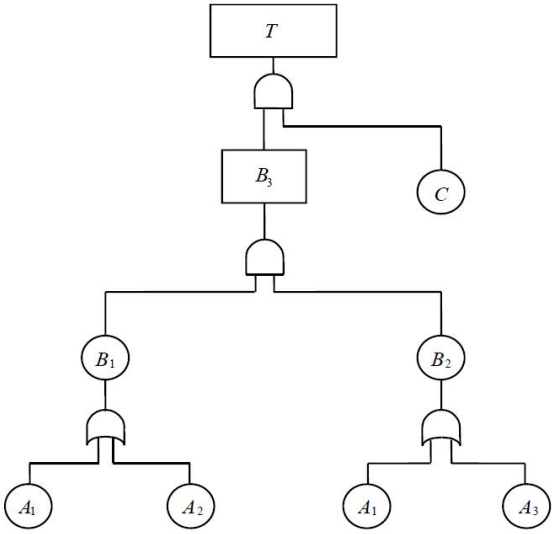


Рис. 2.13. Дерево відмов у разі повторюваних подій:
A_1, A_2, A_3 і C – елементарні події; B_1, B_2, B_3 – проміжні події;
T – завершальна подія

У цьому випадку дерево несправностей можна представити за допомогою наступних булевих виразів:

$$T = C \cdot B_3, \qquad B_1 = A_1 + A_2,$$

$$B_3 = B_1 \cdot B_2, \qquad B_2 = A_1 + A_3.$$

Підставляючи в перший вираз співвідношення для B_1, B_2 і B_3, одержуємо $T = C \cdot (A_1+A_2) \cdot (A_1+A_3)$.

Згідно з рис. 2.10, відмова A_1 є повторюваною елементарною подією, тому отриманий вираз необхідно спростити, використовуючи розподільний закон булевої алгебри. В результаті отримуємо $T = C \cdot [A_1 + A_2 \cdot A_3]$, і початкове дерево несправностей приймає вигляд, показаний на рис. 2.14.

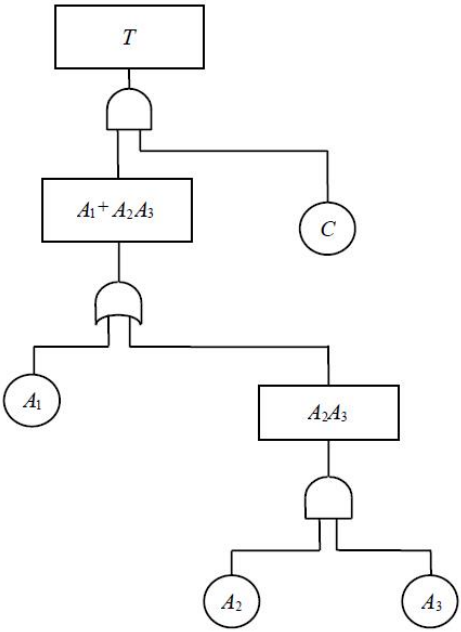


Рис. 2.14. Спрощене дерево несправностей

Таким чином, перш ніж знаходити кількісні показники надійності та ризику, доцільно спростити вирази з повторюваними подіями, використовуючи властивості булевої алгебри.

2.7. Ймовірнісна оцінка дерева відмов

Схема «АБО». Для пояснення ймовірнісного аспекту роботи цієї схеми проаналізуємо схему «АБО» з двома входами, зображену на рис. 2.15. Для цієї схеми ймовірність появи завершальної події має вигляд:

$$P(T) = P(a) + P(b) – P\,(a \cdot b). \qquad (2.6)$$

Якщо a і b – статистично незалежні події і добуток $P(a)$ та $P(b)$ дуже малий, то отриманий вираз можна наближено записати як

$$P(T) \approx P(a) + P(b). \qquad (2.7)$$

У разі схеми «АБО» з n входами маємо

$$P(a + b + c + ... + n) \approx P(a) + P(b) + P(c) + ... + P(n). \quad (2.8)$$

Цей наближений вираз дає хороші результати, якщо ймовірності появи елементарних подій $P(a)$, $P(b)$, $P(c)$,... , $P(n)$ дуже малі, і точний результат, якщо події a, b, c,... , n є несумісними.

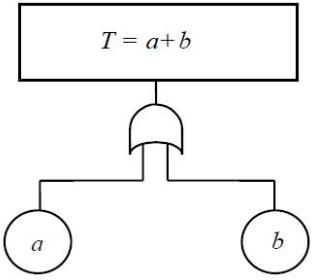


Рис. 2.15. Схема «АБО» з двома входами

Схема «І». У разі схеми «І» з двома входами (рис. 2.16) події a і $в$ статистично незалежні і для отримання ймовірності появи завершальної події застосовується правило множення ймовірностей:

$$P(ав) = P(a) \cdot P(в). \quad (2.9)$$

Для схеми «І» з n входами даний вираз можна записати в загальному вигляді:

$$P(a \cdot b \cdot c \cdot ... \cdot n) = P(a) \cdot P(b) \cdot P(c) \cdot ... \cdot P(n). \quad (2.10)$$

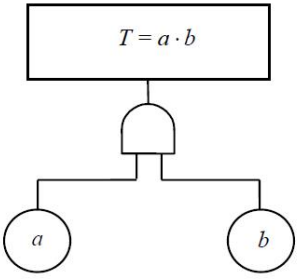


Рис. 2.16. Схема «І» з двома входами

Приклад. Потрібно обчислити ймовірність появи завершальної події гіпотетичного дерева несправностей, зображеного на рис. 2.17.

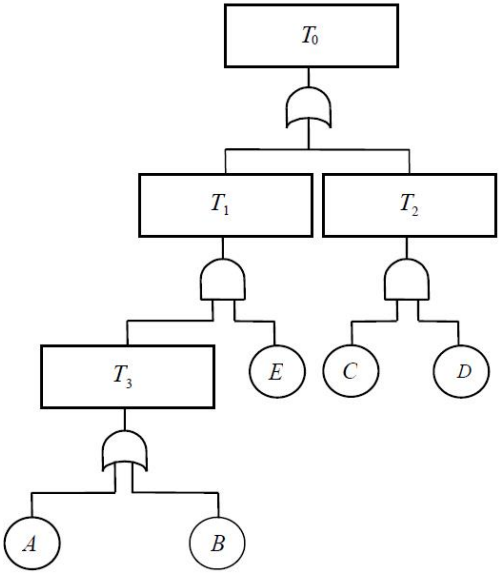


Рис. 2.17. Гіпотетичне дерево подій

Припустимо, що основні події A, B, C, D і E статистично незалежні і що P(A) = P(B) = P(C) = P(D) = P(E) = 1/5. В даному випадку дерево не містить повторюваних елементарних подій, тому можна обчислити ймовірність конкретних подій на виході кожної логічної схеми. Однак якби в гілках дерева несправностей були присутні повторювані події, то перш ніж обчислювати ймовірності тих чи інших подій на виході кожної логічної схеми, необхідно було б виключити повторювані події (тобто отримати мінімальні перетини). Для даного дерева несправностей рішення може бути отримано наступними двома методами.

Метод 1. Запишемо вираз для завершальної події через елементарні події, тобто (2.11):

$$T_0 = T_1 + T_2. \qquad (2.11)$$

Оскільки $T_2 = C \cdot D$, $T_1 = T_3 \cdot E$, $T_3 = A + B$, то $T_0 = E \cdot (A + B) + C \cdot D$, і, отже, $P(T_0) = P(E \cdot A + E \cdot B + C \cdot D)$.

Розкриваючи отриманий вираз, можна отримати формулу для ймовірності появи завершальної події. При допущенні про статистичну незалежність подій (відмов) можна знайти кількісну оцінку ймовірності появи завершальної події.

Метод 2. Цей метод визначення чисельного значення ймовірності появи події заснований на обчисленні ймовірності появи проміжної події. У даних випадках передбачається, що події (відмови) статистично незалежні. Використовуючи правило множення ймовірностей, отримуємо наступний кількісний результат для ймовірностей появи проміжних подій і завершальної події:

$P(T_3) = P(A) + P(B) - P(A) \cdot P(B) = 1/5 + 1/5 - 1/25 = 9/25,$

$P(T_2) = P(C) \cdot P(D) = 1/5 \cdot 1/5 = 1/25,$

$P(T_1) = P(T_3) \cdot P(E) = 9/25 \cdot 1/5 = 9/125,$

$P(T_0) = P(T_1) + P(T_2) - P(T_1) \cdot P(T_2) = 9/125 + 1/25 - 9/125 \cdot 1/25 = 341/3125.$

Приклад. Припустимо, що в дереві несправностей, зображеному на рис. 2.17, подія Е замінюється подією Д (рис. 2.18). Для отримання ймовірності появи завершальної події нового дерева, зображеного на рис. 2.18, застосуємо метод 1 з попереднього прикладу. Вираз, що зв'язує завершальну подію з основними подіями (включаючи повторювану подію D), має вигляд (2.12):

$$T_0 = (A + B) \cdot D + C \cdot D \quad \text{або} \quad T_0 = AD + B \cdot D + C \cdot D. \qquad (2.12)$$

Ймовірність появи завершальної події визначається за формулою (2.13):

$$P(D\cdot A + B\cdot D + C\cdot D) = P(D\cdot A) + P(B\cdot D) + P(C\cdot D) - P(D\cdot A\cdot B\cdot D) - $$
$$- P(D\cdot A\cdot C\cdot D) - P(B\cdot D\cdot C\cdot D) + P(D\cdot A\cdot B\cdot D\cdot C\cdot D). \quad (2.13)$$

У разі неповторюваних статистично незалежних подій

$$P(D\cdot A+B\cdot D + C\cdot D) = P(A)\cdot P(D) + P(B)\cdot P(D) + P(C)\cdot P(D) -$$
$$- P(D)\cdot P(A)\cdot P(B) - P(A)\cdot P(C)\cdot P(D) - P(B)\cdot P(C)\cdot P(D) +$$
$$+ P(A)\cdot P(B)\cdot P(C)\cdot P(D).$$

Отже, ймовірність появи завершальної події дорівнює:

$$P\,(D\cdot A + B\cdot D + C\cdot D) =$$
$$= 1/25 + 1/25 + 1/25 - 1/125 - 1/125 - 1/125 + 1/625 = 61/625.$$

Однак якщо спочатку виключаються повторювані події, то дерево несправностей, представлене на рис. 2.18, приводиться до дерева, показаного на рис. 2.19. Вираз для завершальної події цього дерева несправностей приймає вигляд (2.14):

$$T_0 = D \cdot T_1, \quad (2.14)$$

де $T_1 = A + B + C$.

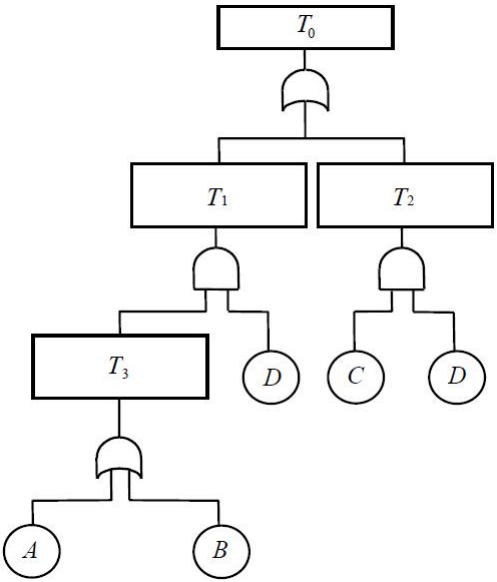


Рис. 2.18. Дерево несправностей у разі повторюваної події

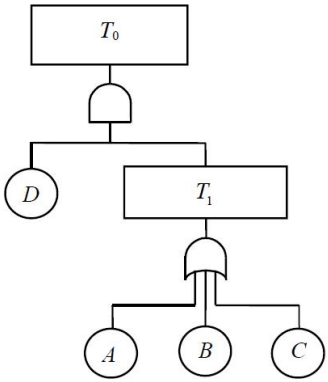


Рис. 2.19. Дерево несправностей при відсутності повторюваних подій

У разі статистично незалежних подій імовірність появи завершальної події дорівнює

$$P(D \cdot T_1) = P(D) \cdot P(T_1) = 1/5 \cdot 61/625 = 61/3125,$$

де $P(A + B + C) = P(A) + P(B) + P(B) - P(A) \cdot P(B) - P(A) \cdot P(C) - P(B) \cdot P(C) + P(A) \cdot P(B) \cdot P(C) = 61/625$.

Зауважимо, що якщо ймовірності появи елементарних відмов дуже малі, існування залежності подій не вносить великої похибки в кінцевий результат. Однак, перш ніж знаходити остаточне значення ймовірності, необхідно спробувати виключити всі випадки залежності подій у дереві несправностей.

2.8. Переваги та недоліки методу дерева відмов

Даний метод, як і будь-який інший, має певниі переваги і недоліки. Так, наприклад, метод дає повне уявлення про поведінку технічної системи, але вимагає від фахівців з надійності глибокого розуміння роботи технічної системи і конкретного розгляду кожен раз тільки однієї певної відмови; допомагає дедуктивно виявляти відмови; дає конструкторам, користувачам і керівникам можливість наочного обґрунтування конструктивних змін і аналізу компромісних рішень;

дозволяє виконувати кількісний і якісний аналіз надійності; полегшує аналіз надійності складних систем. Разом з тим реалізація методу вимагає значних витрат коштів і часу. Крім того, отримані результати важко перевірити; важко врахувати стану часткової відмови елементів, оскільки при використанні методу, як правило, вважають, що система знаходиться або в справному стані, або в стані відмови. Істотні труднощі виникають і при отриманні в загальному випадку аналітичного рішення для дерев, що містять резервні вузли і відновлювані вузли з пріоритетами, не кажучи вже про ті значні зусилля, які потрібні для охоплення всіх видів множинних відмов.

Контрольні питання

1. Які символи використовуються при побудові дерев подій і дерев відмов?
2. У чому полягає процедура побудови дерева відмов?
3. У чому сутність методу первинних відмов?
4. У чому сутність методу вторинних відмов?
5. У чому сутність методу ініційованих відмов?
6. Що таке «мінімальний перетин дерева несправностей»?
7. Як проводиться кількісна оцінка дерева відмов?
8. Які переваги та недоліки методу дерева відмов?

3. ЗАСТОСУВАННЯ ТЕОРІЇ РИЗИКУ ДЛЯ ОЦІНКИ РІВНЯ БЕЗПЕКИ

3.1. Критерії прийнятного ризику

До недавнього часу Нормативи безпеки в усьому світі ґрунтувалися на концепції абсолютної безпеки. Для запобігання аваріям впроваджувалися інженерні системи безпеки, вживалися організаційні заходи, що забезпечують високий рівень дисципліни, суворий регламент роботи. Вважалося, що такий підхід дозволяє виключити будь-яку небезпеку для населення і навколишнього середовища.

Однак сьогодні через безпрецедентне ускладнення виробництв і появу принципово нових технологій, збільшеної мережі транспортних і енергетичних комунікацій, концепція абсолютної безпеки стала неадекватною внутрішнім законам техносфери і біосфери.

Ресурси будь-якого суспільства обмежені. А витрати на підвищення безпеки зростають експоненціально, тобто кожен наступний крок у напрямку підвищення безпеки обходиться суспільству все дорожче і дорожче. Тому спільнота прийшла до розуміння неможливості створення абсолютної безпеки (нульового ризику). Прагнути слід до досягнення такого рівня ризику від впливу небезпечних факторів, який можна розглядати як «прийнятний». Його прийнятність повинна бути обґрунтована виходячи з економічних і соціальних міркувань. Необхідність формування концепції прийнятного (допустимого) ризику обумовлена неможливістю створення абсолютно безпечної діяльності (технологічного процесу).

Прийнятний ризик – ризик загибелі людини, який суспільство на даному етапі розвитку готове прийняти.

У всіх розвинених у промисловому відношенні країнах існує стійка тенденція застосування концепції прийнятного ризику.

Серед підходів, запропонованих для обґрунтування критеріальних значень ризику, слід відзначити метод економічного аналізу безпеки, заснований на обліку витрат на забезпечення безпеки і втрат від можливих аварій. Концепція нормування безпеки пропонує завдання ризику наступним чином:

– абсолютна безпека не може бути забезпечена, об'єкт може бути тільки відносно безпечний;

– вимоги до рівня безпеки формуються на основі «прийнятного ризику», пов'язані з соціально-економічним станом суспільства і є похідними цього стану;

– визначення ризику здійснюється шляхом виявлення різних факторів, що впливають на безпеку, та їх кількісної оцінки.

Існують і інші аспекти нормування безпеки:

– ризик не повинен перевищувати рівня, досягнутого для складних технічних об'єктів з урахуванням природних впливів;

– ризик повинен бути знижений настільки, наскільки це практично досяжне в рамках відповідних обмежень;

– не повинно бути складових ризику, різко перевищують інші (аналог принципу рівнонадійності, застосовуваного при забезпеченні надійності виробів).

Тому при оцінці прийнятності різних рівнів ризику можна обмежитися розглядом ризику лише тих шкідливих наслідків, які, в кінцевому рахунку, призводять до смертельних наслідків, оскільки для цього показника існують досить надійні статистичні дані. Тоді, наприклад, поняття «екологічний ризик» може бути сформульовано як відношення величини можливого збитку, вираженого в кількості смертельних випадків від

впливу шкідливого екологічного фактора за певний інтервал часу до нормованої величини інтенсивності цього фактора.

Таким чином, головна увага при визначенні технічного, екологічного і соціального ризику має бути спрямована на аналіз співвідношення можливого економічного збитку, шкідливих соціальних і екологічних наслідків, що закінчуються смертельними наслідками.

Суспільна прийнятність ризику пов'язана з різними видами діяльності і визначається економічними, соціальними та психологічними факторами.

У загальному випадку під прийнятним ризиком розуміється ризик, рівень якого допустимий і обґрунтований, виходячи з економічних і соціальних міркувань.

Приклад визначення прийнятного ризику представлений на рис. 3.1.

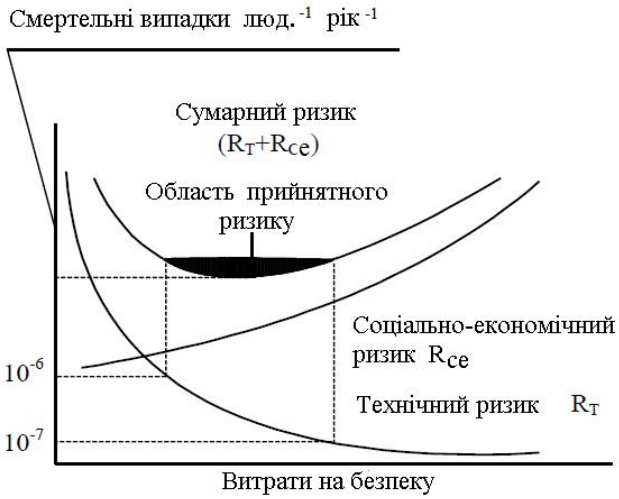


Рис. 3.1. Визначення прийнятного ризику

При збільшенні витрат на вдосконалення обладнання технічний ризик знижується, але зростає соціальний. Сумарний ризик має мінімум при певному співвідношенні між інвес-

тиціями в технічну та соціальну сферу. Цю обставину треба враховувати при виборі прийнятного ризику. При визначенні соціально прийнятного ризику зазвичай використовують дані про природну смертність людей.

Як реперне значення абсолютного ризику приймають величину летальних випадків (ЛВ):

$$R_А = 10^{-4} \text{ ЛВ/(чол. рік)}.$$

Як реперне значення допустимого (прийнятного) ризику при наявності окремо взятого джерела небезпеки приймають:

$$R_Д = 10^{-5} \text{ ЛВ/(чол. рік)};$$

$$R_Д = 10^{-4}…10^{-3} \text{ НЗ/(чол. рік)},$$

де НЗ – випадки непрацездатності.

Для населення величина додаткового ризику, викликаного техногенними причинами, не повинна перевищувати реперне значення абсолютного ризику:

$$R \le R_А.$$

Для окремо взятого джерела небезпеки, враховуючи, що індивідуальний ризик залежить від відстані R = R(r), умову безпеки можна записати у вигляді:

$$R\,(r) \le R_Д.$$

В даний час за міжнародною домовленістю прийнято вважати, що дія техногенних небезпек (технічний ризик) має знаходитися в межах $10^{-7}...10^{-6}$ (смертельних випадків $\text{чол}^{-1}/\text{рік}^{-1}$), а величина 10^{-6} є максимально прийнятним рівнем індивідуального ризику. У національних правилах ця величина використовується для оцінки пожежної безпеки та радіаційної безпеки.

Прийнятний ризик поєднує у собі технічні, екологічні, соціальні аспекти і являє певний компроміс між прийнятним

рівнем безпеки й економічними можливостями його досягнення, тобто можна говорити про зниження індивідуального, технічного або екологічного ризику, але не можна забувати про те, скільки за це доведеться заплатити і яким у результаті виявиться соціальний ризик.

У зв'язку зі складністю розрахунків показників ризику, недоліком вихідних даних (особливо за надійністю обладнання, людськими помилками) на практиці часто використовуються методи аналізу і критерії прийнятного ризику, засновані на результатах експертних оцінок фахівців. У цьому випадку розглянутий об'єкт зазвичай ранжується за ступенем ризику на чотири (або більше) групи з високим, проміжним, низьким або незначним рівнем ризику. При такому підході високий рівень ризику вважається, як правило, неприйнятним, проміжний вимагає виконання програми робіт зі зменшення рівня ризику, низький вважається прийнятним, а незначний взагалі не розглядається як такий, що заслуговує на увагу.

Таким чином, основними вимогами до вибору критерію прийнятного ризику при проведенні аналізу ризику є обґрунтованість і визначеність.

3.2. Управління ризиком

Відповідно до концепції безпеки населення і навколишнього середовища практична діяльність в області управління ризиком повинна бути побудована так, щоб суспільство в цілому отримувало найбільшу доступну суму благ.

Управління ризиком – це аналіз ризикової ситуації, розробка та обґрунтування управлінського рішення, нерідко у формі правового акта, спрямованого на мінімізацію ризику.

У принципах управління ризиком закладені стратегічні і тактичні цілі. У стратегічних цілях виражено прагнення до досягнення максимально можливого рівня добробуту су-

спільства в цілому, а в тактичних – прагнення до збільшення безпеки населення і тривалості життя. У них обумовлюються як інтереси груп населення, так і кожної людини при захисті від надмірного ризику.

Найважливішим принципом є положення про те, що в управління ризиком повинен бути включений весь спектр існуючих у суспільстві небезпек, і загальний ризик від них для будь-якої людини і для суспільства в цілому не може перевищувати «прийнятний» рівень.

Схема процесу управління ризиком представлена на рис. 3.2.

Для проведення аналізу ризику, встановлення його допустимих меж у зв'язку з вимогами безпеки і прийняття керуючих рішень необхідні:

– наявність інформаційної системи, що дозволяє оперативно контролювати існуючі джерела небезпеки і стан об'єктів можливого ураження;

– відомості про передбачувані напрямки господарської діяльності, проєкти і технічні рішення, які можуть впливати на рівень техногенної та екологічної безпеки, а також програми для ймовірнісної оцінки пов'язаного з ними ризику;

– експертиза безпеки і зіставлення альтернативних проєктів і технологій, що є джерелами ризику;

– розробка техніко-економічної стратегії збільшення безпеки і визначення оптимальної структури витрат для управління величиною ризику та її зниження до прийнятного рівня з економічної та екологічної точок зору;

– формування організаційних структур, експертних систем та нормативних документів, призначених для виконання зазначених функцій і процедури прийняття рішень;

– вплив на громадську думку та пропаганда наукових даних про рівні техногенного й екологічного ризиків з метою орієнтації на об'єктивні оцінки ризику.

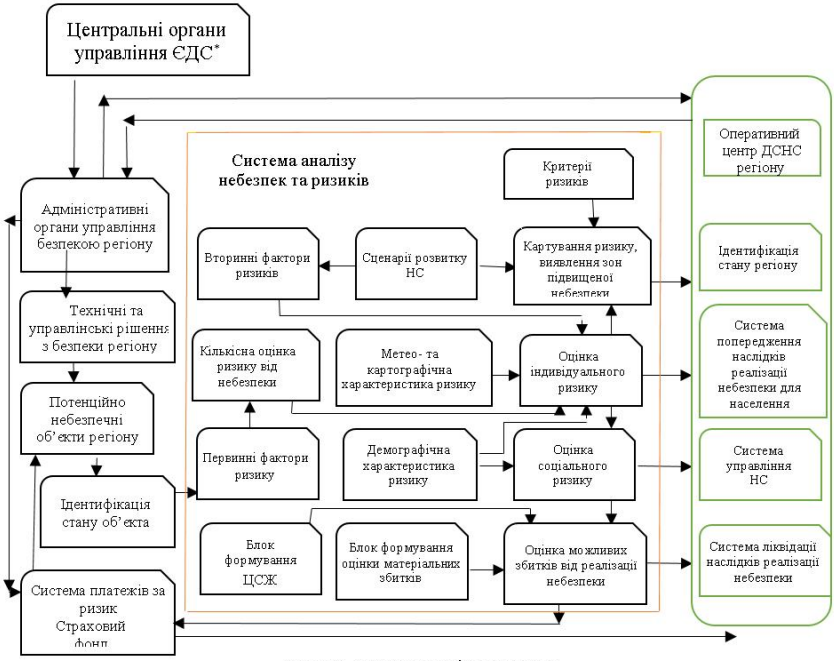


Рис. 3.2. Схема управління ризиком

Модель управління ризиком складається з чотирьох частин і етапів.

Перший етап пов'язаний з характеристикою ризику. На початковому етапі проводиться порівняльна характеристика ризиків з метою встановлення пріоритетів. На завершальній фазі оцінки ризику встановлюється ступінь небезпеки (шкідливості).

Другий етап – визначення прийнятності ризику. Ризик зіставляється з рядом соціально-економічних факторів:

– вигоди від того чи іншого виду господарської діяльності;

ЄДС* – єдина державна система цивільного захисту.

– втрати, обумовлені даними видами діяльності;

– наявність і можливості регулюючих заходів з метою зменшення негативного впливу на середовище і здоров'я людини.

Процес порівняння спирається на метод «витрати-вигоди».

У зіставленні «неризикових» факторів з «ризиковими» проявляється суть процесу управління ризиком.

Можливі три варіанти прийнятих рішень:

– ризик прийнятний повністю;

– ризик прийнятний частково;

– ризик неприйнятний повністю.

У даний час рівень знехтуваної межі ризику звичайно встановлюють як 1 % від максимально допустимого.

У двох останніх випадках необхідно встановити пропорції контролю, що входить у завдання третього етапу процедури управління ризиком.

Третій етап полягає у виборі одного з «типових» заходів, що сприяє зменшенню (в першому і другому випадку) або усуненню (в третьому випадку) ризику.

Четвертий етап – прийняття регулюючого рішення-визначення нормативних актів (законів, постанов, інструкцій) та їх положень, що відповідають реалізації тих «типових» заходів, які були встановлені на попередній стадії. Даний елемент, завершуючи процес управління ризиком, одночасно пов'язує всі його стадії, а також стадії оцінки ризику в єдиний процес прийняття рішень, в єдину концепцію ризику.

3.3. Застосування теорії ризику в технічних системах

Проєктування складних технічних систем і конструкцій виконується на основі чисельних методів з використанням комп'ютерів. Однак обчислені на основі таких розрахунків параметри і характеристики слід розглядати як наближені, які відрізняються від дійсних. Відхилення розрахункових

параметрів від дійсних являють собою випадкові величини, які залежать від умов завдання.

Шляхом застосування теорії ризику можна оцінити неточності, що виникають при розрахунку і проєктуванні конструкцій. Імовірнісний метод обчислення ризику дозволяє отримати нову інформацію про те, який вплив на величину ризику надають різні джерела невизначеності в процесі розрахунку і проєктування конструкції і як це відбивається на остаточному проєкті.

Однак при використанні чисельних методів виникають неточності розрахунку, оцінка яких набуває особливого значення при визначенні ймовірного ризику.

В інженерних задачах вихідні дані часто бувають далеко не повними. Так, наприклад, величина зовнішніх сил змінюється в часі; властивості матеріалу, з якого зроблена конструкція, також визначаються як середні і мають розкид. Виникають терміни «допустима межа», «інженерне рішення», які підтверджують відсутність достатньої точності у вихідних даних. У результаті для опису ймовірності руйнування конструкції виникає поняття «ризик», яким характеризують отримане рішення.

До складу великих споруд входять об'єкти, що мають різну ступінь відповідальності в забезпеченні безпеки, наприклад, у гідротехнічному вузлі найбільш відповідальним об'єктом є гребля, менш відповідальними – будівлі, трубопроводи і т. д. Однак бажано приймати для всіх об'єктів однакову міру ризику. Принцип збалансованого ризику вимагає, щоб усі об'єкти, які входять до складу споруди, проєктувалися на забезпечення однакового ступеня ризику.

При вирішенні багатьох інженерних завдань доводиться визначати ризик, який виникає як результат зниження витрат при виробництві та експлуатації технічної системи. Ризик визначається на основі обробки статистичними методами великого числа спостережень. Величина ризику залежить від

очікуваної вигоди. Як правило, підвищення величини ризику призводить до зниження витрат на створення технічної системи і збільшення очікуваної вигоди. Але разом з тим це підвищення може спричинити за собою руйнування технічної системи в більш короткий термін або з більшою часткою ймовірності. Тому визначення прийнятої величини ризику є досить відповідальним завданням, яке може бути правильно вирішене тільки шляхом проведення глибокого статистичного аналізу.

Функціональна залежність між величиною ризику й очікуваною вигодою виражається нелінійним законом, як це показано на рис. 3.3.

Побудована на цьому рисунку крива ділить координатну площину на дві частини. Праворуч від кривої розташовані значення, які можуть бути при відомих умовах прийняті (ця область заштрихована). Точки, розташовані зліва від кривої, відносяться до неприйнятних значень.

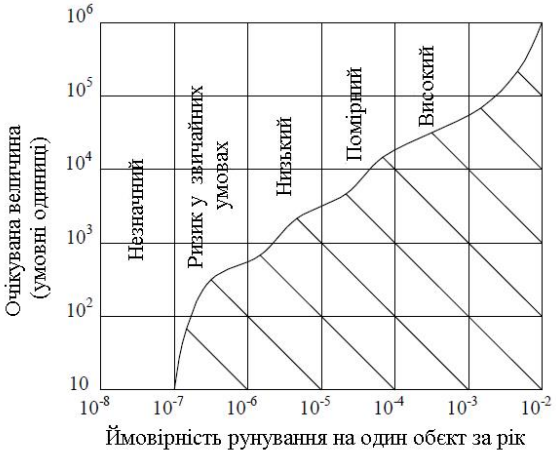


Рис. 3.3. Залежність величини ризику від витрат

Розглянемо докладніше фізичний сенс числового виразу ризику. Найбільш повні статистичні дані є для ризику,

яким характеризуються нещасні випадки в різних сферах виробництва. Так, наприклад, ризик, що характеризується числом 10^{-3} випадків на одну людину на рік, є абсолютно неприйнятним. Рівень ризику 10^{-4} вимагає вжиття заходів і може бути прийнятий тільки в тому випадку, якщо іншого виходу немає. Так, ризик в автомобільних аваріях в Україні досягає рівня $2 \cdot 10^{-4}$.

Рівень ризику 10^{-5} відповідає природним випадковим подіям, наприклад, нещасних випадків при купанні в морі, для яких ризик обчислюється як $3{,}7 \cdot 10^{-5}$.

Нещасні випадки, обумовлені ризиком 10^{-6}, відносяться до такого рівня, на який є більш спокійна реакція, оскільки вважається, що уникнути цього ризику може кожен, дотримуючись елементарних правил обережності.

Аналогічним чином величина ризику може бути встановлена і для кожної технічної системи з урахуванням терміну служби, її значення для загальної міцності всієї споруди, а також вартості, терміну відновлення і т. д.

Дуже часто для оцінки ризику приймається частота виникнення аварійних ситуацій, наприклад, число випадків руйнування гребель на рік і їх негативні наслідки – число нещасних випадків, які викликані цією аварією.

При проєктуванні приймаються рішення, які можуть збільшити або зменшити величину ризику в процесі експлуатації конструкції. Для того щоб оцінити вплив неточностей, допущених при проєктуванні, слід для даної конструкції оцінити ймовірні шляхи, в результаті яких може відбутися руйнування. Для найпростішої конструкції дуже часто можна передбачити єдиний шлях ймовірного руйнування і тоді завдання спрощується. Однак для складних конструкцій і споруд руйнування може розвиватися різними шляхами, що мають різну ймовірність.

Коефіцієнт надійності обчислюється для кожної наміченої схеми руйнування за такою формулою:

$$F_{rf} = \prod_{i=1}^{n}(R_i), \quad (3.1)$$

де R_i – множник, що характеризує коефіцієнт надійності для кожної схеми.

Залежність між ймовірністю P руйнування, вираженою у відсотках, і коефіцієнтом надійності F виходить у вигляді: $P = 10\ \% – F = 3{,}5$; $P = 1\ \% – F = 10$; $P = 0{,}1\ \% – F = 20$.

Імовірність того, що руйнування відбудеться за обраною послідовністю подій D, обчислюється за формулою

$$P_D = 1 - \prod_{i=1}^{n}(1 - P_i)^{mj}, \quad (3.2)$$

де m_j – число ділянок для обраної схеми руйнування.

Вирішуючи технічні завдання, необхідно враховувати ризик, який виникає в результаті невизначеностей при виборі вихідних даних для розрахунків. При визначенні допустимого ризику необхідно враховувати ймовірність сприятливого і несприятливого результату при експлуатації проєктованої технічної системи. Величина ризику визначається на основі загальних математичних методів: теорії ймовірностей, математичної статистики та теорії ігор. Для вимірювання величини ризику, відповідного даному варіанту рішення, проєктувальник повинен дослідити вплив усіх факторів.

Визначення ризику особливого значення набуває при проєктуванні нових споруд і складних технічних систем. Правильне використання теорії ризику дуже часто призводить до того, що проєктована технічна система може обійтися дешевше.

Дуже часто поняття ризику пов’язують з оцінкою можливих збитків. Для правильного розуміння суті питання доцільно визначати ризик як можливість відхилення прийнятого рішення від тієї величини, яка відповідає оптимальним умовам експлуатації об’єкта.

Витрати на виробництво технічних систем пов’язані з прийнятою при проєктуванні величиною ризику. При

великому ризику знижується вартість первинних витрат, однак надалі, при несприятливому збігу обставин, у технічній системі можуть виникнути пошкодження, ліквідація яких пов'язана з додатковими витратами. Мала величина ризику, прийнята при проєктуванні, зажадає збільшення міцності і надійності елементів технічної системи, а це підвищує вартість її виробництва. Якщо в процесі подальшої експлуатації не відбудеться несприятливого збігу обставин, то первісне подорожчання виробництва технічної системи для збільшення міцності і надійності її елементів виявляється не потрібним. Таким чином, збільшення ризику призводить до здешевлення виробництва, а зниження ризику викликає подорожчання виробництва.

3.4. Оцінка ризику аварій

Порядок розробки Декларації безпеки небезпечних виробничих об'єктів враховує аналіз умов виникнення і розвитку аварій, який включає:

– виявлення можливих причин виникнення і розвитку аварійних ситуацій з урахуванням відмов і неполадок обладнання, можливих помилкових дій персоналу, зовнішніх впливів природного і технічного характеру;

– визначення сценаріїв можливих аварій;

– оцінку кількості небезпечних речовин, здатних брати участь в аварії;

– обґрунтування застосовуваних для оцінки небезпек моделей і методів розрахунку.

Наведені дані причин пожеж (табл. 3.1) сприяють проведенню ідентифікації небезпечних і шкідливих факторів на об'єктах зберігання нафтопродуктів. Можна виділити наступні небезпеки: вибух (В), пожежа (П), отруєння (О) персоналу токсичними речовинами, забруднення (З) навколишнього природного середовища (НПС). Усі ці небажані події можуть наступати в разі порушення технологічного регламенту робіт

на об'єктах або відступу від інструкцій. Можна обґрунтовано вважати, що значною мірою зазначені небезпеки будуть проявлятися спільно, тобто вибух супроводжуватиметься пожежею, отруєнням персоналу та забрудненням НПС. У свою чергу, пожежа може призвести до вибуху і подальшого впливу на персонал і НПС. Забруднення середовища світлими нафтопродуктами (СНП) – бензином і гасом – у ряді випадку може супроводжуватися вибухом і пожежею. В табл. 3.2 наведені ці небезпеки залежно від стадії технологічного процесу та обладнання.

При аналізі ризику небезпечних промислових об'єктів допускаються найрізноманітніші методи, в тому числі й експертні процедури. В основі останніх лежать суб'єктивні оцінки, що спираються на відому експерту інформацію. Робота з апріорною інформацією являє собою особливий різновид імовірнісних процедур, включаючи суб'єктивні (персональні) ймовірності.

Таблиця 3.1. **Причини пожеж на об'єктах зберігання нафтопродуктів**

Причини пожежі	Кількість пожеж	Відсоток від загальної кількості пожеж	Число загиблих	Відсоток від загальної кількості загиблих
Визначені підпали	7	3,10	0	0
Несправність обладнання	58	25,66	6	
ППЕ – електрообладнання – печей – теплогенеруючих установок – побутових газових пристроїв	 17 1 0 0	 7,52 0,44 0 0	 3 0 0 0	 15,78 0 0 0

Продовж. табл. 3.1

Причини пожежі	Кількість пожеж	Відсоток від загальної кількості пожеж	Число загиблих	Відсоток від загальної кількості загиблих
ППБ електрогазових робіт	25	11,06	0	0
Вибухи	1	0,44	0	0
Самозаймання речовин та матеріалів	6	2,65	0	0
Необережне поводження з вогнем	86	38,05	9	47,37
Грози	1	0,44	9	0
Невстановлені	6	2,65	1	5,26
Інші	18	7,96	0	0

Примітка: ППБЕ – порушення правил будови та експлуатації пристрою; ППБ – порушення правил пожежної безпеки.

Таблиця 3.2. **Небезпеки технологічного процесу та обладнання**

Технологічна операція	Функціональний блок (споруда, обладнання, приміщення)					
	ЗНЕ	ПНС	ТТ	РП	Л	ПХ
Злив, зачистка, наливання (залізничні цистерни)	В,П,О,З					
Перекачування (СНП)		В,П,О,З	В,П,О,З			
Зберігання СНП				В,П,О,З		
Ремонт резервуарів				В,О		
Відбір проб, проведення замірів рівня СНП	В,П,О,З			В,П,О	В,П,О	В,П,О,З

Примітка: ЗНЕ – зливно-наливна естакада; ПНС – продуктово-насосна станція; ТТ – технологічний трубопровід (для перекачування СНП); РП – резервуарний парк; Л – лабораторія; ПЗ – приміщення для зберігання СНП, відібраних для аналізу.

Для визначення ймовірності настання несприятливої події, наприклад вибуху в Q_B, треба знати ймовірності вихідних подій – утворення парогазової суміші $Q_{2.1}$ і появи джерела займання $Q_{2.2}$. Для визначення ймовірності першої вихідної події $Q_{2.1}$ можна використовувати дані для показників, що формують коефіцієнт $К_1$ (приватні фактори вибухонебезпечності), наведені в табл. 3.3.

Аналіз специфічних властивостей гасу різних марок і бензинів показав відсутність у них принципових відмінностей. Обидва вони є легкозаймистими рідинами (ЛЗР), але пружність парів бензину значно (в середньому на 1–2 порядки) вище пружності парів гасу. Тому в умовах виробництва при нормальній температурі у закритих обсягах бензин може утворювати пароповітряні суміші, здатні до вибуху від зовнішніх джерел, у той час як гас практично їх не утворює.

Таблиця 3.3. **Вибухопожежонебезпечні властивості бензину і гасу**

Показники, які формують коефіцієнт $К_1$	Бензин БР-1	Гас
Діапазон концентраційних меж займання	0,02	0,02
Нижня концентраційна межа займання	0,13	0,13
Мінімальна енергія запалення	0,09	0,09
Температура середовища	0,01	0,01
Тиск середовища (надлишок)	0	0
Густина газу (пару) по відношенню до густини повітря	0,10	0,10
Об'ємний електричний опір	0,06	0,06
Особливо небезпечні характеристики	0	0

Коефіцієнт $К_1$, що має досить високе значення (0,41), можна пов'язати з імовірнісною складовою, приймаючи суб'єктивну імовірність утворення пароповітряної суміші бензину близькою до 0,4. Що стосується гасу, то ця величина значною мірою залежить від його складу. Для авіаційних палив вона

наближається до 0,4, а для освітлювального гасу може бути прийнята на порядок нижче, тобто 0,04.

Статистика пожеж і вибухів свідчить про те, що джерела займання проявляються досить часто. Тому на етапі оцінки небезпеки можна прийняти суб'єктивну ймовірність появи джерела запалювання (займання) $Q_{2.2}$ дорівнює 0,4 (такий же, як $Q_{3.13}$ = 0,40). В цьому випадку для моделі оцінки ймовірності вибуху бензину він складе 0,4 · 0,4 = 0,16. Інакше кажучи, один випадок з шести може закінчитися вибухом. Для освітлювального гасу ця величина на порядок менше (0,016), тобто тільки один випадок з 60 буде супроводжуватися вибухом.

Найбільш значущим є аналіз джерел займання. Свій внесок вносять апаратура з вогневим обігрівом, іскріння і перегрів струмоведучих систем, удар і тертя. Аналіз реальних випадків дозволив оцінити внесок джерел займання, рівний 0,14. З цієї величини 0,12 припадає на іскріння і перегрів струмоведучих частин. Ймовірність прояву інших джерел займання наступна:

електрика (блискавка, грозові розряди), $Q_{3.10}$ = 0,05; розряд статистичної електрики, $Q_{3.11}$ = 0,09; тліюче полум'я (транспорт), $Q_{3.12}$ = 0,02; відкрите полум'я (необережне поводження з вогнем), $Q_{3.13}$ = 0,40; інші джерела, $Q_{3.14}$ = 0,10. Складові ймовірності нижчого рівня на даному етапі не аналізуються.

Для аналізу ризику стосовно до небезпечних факторів «вибух» і «пожежа» використовували дані про 226 пожеж на складах ЛЗР і ГР, мали як джерело загоряння ЛЗР. Ці пожежі супроводжувалися загибеллю 19 осіб. Звідси можна в першому наближенні визначити, що один загиблий припадає на 12 пожеж.

Вважаючи, що ймовірність вибухів і пожеж за участю бензину дорівнює 0,16, отримуємо ймовірність смертельного травмування, рівну 0,013.

Проведений аналіз показав, що потенційна ймовірність аварії на об'єктах зі зберігання нафти і нафтопродуктів досить висока.

Істотний внесок у цю складову вносять помилки персоналу. Причинами помилок персоналу можуть бути неуважність, звичні асоціації, низька пильність, помилки альтернативного вибору, неадекватний облік побічних ефектів і неявних умов, мала точність, слабке топографічне та просторове орієнтування.

Важливим засобом запобігання аварій у даному випадку є чітке дотримання галузевих правил, норм та інструкцій.

Контрольні питання

1. Яким чином визначаються критерії прийнятного ризику?
2. У чому полягає процес управління ризиком?
3. Яка існує залежність між величиною ризику й очікуваною вигодою?
4. Який взаємозв'язок між витратами на виробництво технічних систем з прийнятою при проєктуванні величиною ризику?
5. У чому полягає аналіз умов виникнення і розвитку аварій?
6. Якими можуть бути причини помилок персоналу?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності та визначається періодичність здійснення планових заходів державного нагляду (контролю) у сфері техногенної та пожежної безпеки Державною службою з надзвичайних ситуацій : Постанова КМУ № 715 [Текст] // Офіційний вісник України від 05.09.2018 р.

2. Про затвердження Положення про Державну службу України з надзвичайних ситуацій : Постанова Кабінету Міністрів України від 16.01.2015 № 1052 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1052-2015-п.

3. Державна служба України з надзвичайних ситуацій [Електронний ресурс]. – Режим доступу : http://www.dsns.gov.ua

4. Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями : Постанова Кабінету Міністрів України від 24.03.2004 № 368 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/368-2004-п.

5. Про Концепцію Національної програми інформатизації : Закон України від 04.02.1998 № 75/98-ВР [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/75/98-вр.

6. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19.

7. Про об’єкти підвищеної небезпеки : Закон України від 18.01.2001 № 2245-III [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2245-14.

8. Про оборону України : Закон України від 06.12.1991 № 1932-XII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1932-12.

9. Про основи національної безпеки України : Закон України від 19.06.2003 № 964-IV [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/964-15.

10. Арламов О. Ю. Безпека життєдіяльності та цивільний захист. Конспект лекцій / О. Ю. Арламов. К., 2018. 93 с.

11. Атаманчук П. Безпека життєдіяльності (теоретичні основи) : навчальний посібник / П. Атаманчук. Київ : Центр навчальної літератури, 2017. 276 с.

12. Безпека життєдіяльності: навч. посіб. / В. В. Зацарний, Н. А. Праховнік, О. В. Землянська, О. В. Зацарна. Київ : НТУУ «КПІ» ІЕЕ, 2016. 417 с.

13. Зеркалов Д. В. Безпека життєдіяльності : навчальний посібник / Д. В. Зеркалов. К. : Основа, 2016. 267 с.

14. Безпека життєдіяльності : навч. посіб. / Т. Є. Стиценко, Г. В. Пронюк, Н. М. Сердюк, І. І. Хондак. Харків : ХНУРЕ, 2018. 336 с.

15. Методи і засоби оцінки ризику здоров’я населення від забруднення атмосферного повітря [Електронний ресурс] : навч. посіб. для студ. спец. 122 «Комп’ютерні науки та інформаційні технології», спеціалізації «Інформаційні технології моніторингу довкілля» / Н. В. Караєва, І. В. Варава ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 4,38 Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2018. 56 с.

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

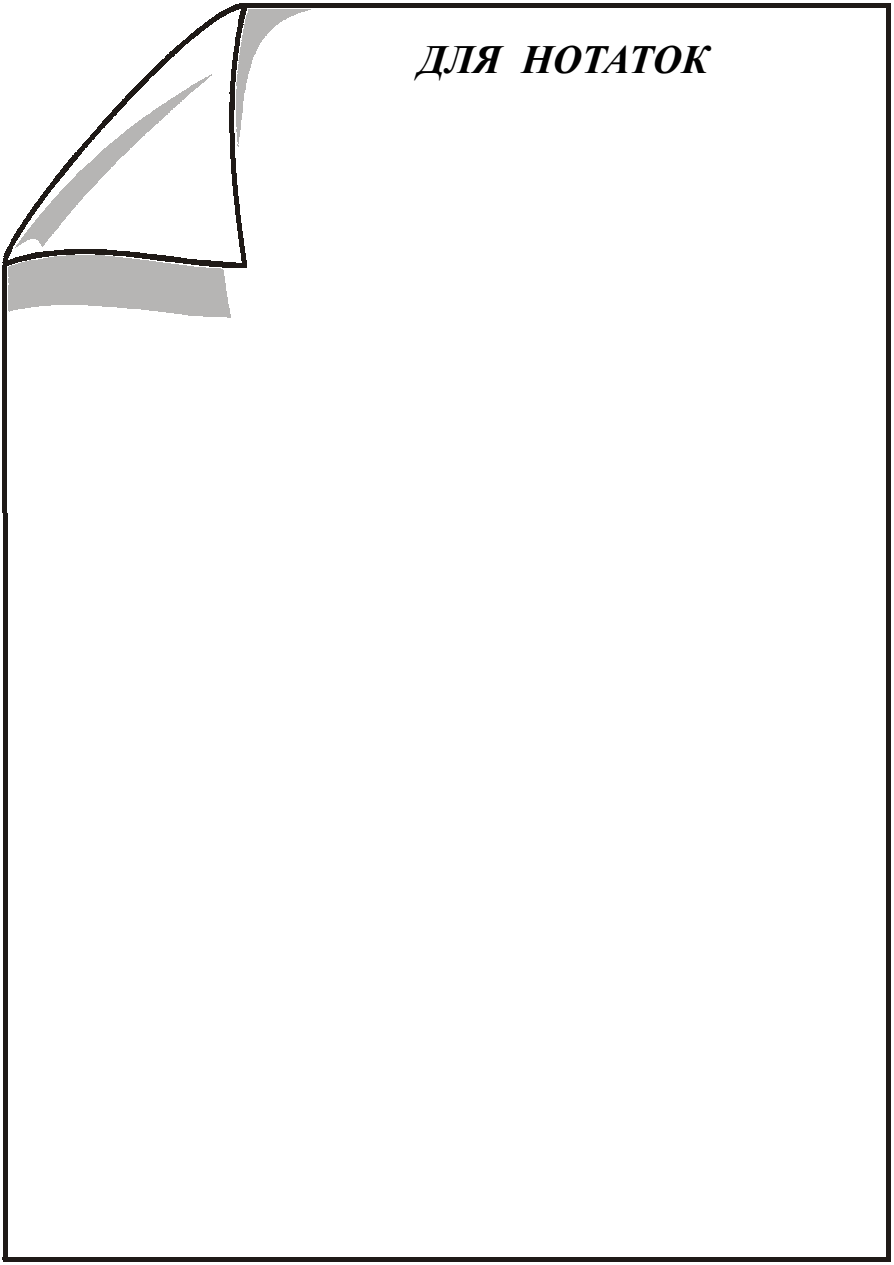
17. Старостіна А. О. Ризик-менеджмент: теорія та практика [Текст] : навч. посіб. / А. О. Старостіна, В. А. Кравченко. Київ : ІВЦ «Видавництво «Політехніка», 2018. 200 с.

18. Гречанінов В. Ф., Бєгун В. В. Функції управління і нагляду в ризик-орієнтованому підході до управління безпекою. Математичні машини і системи. 2014. № 1. С. 159–170.

19. Ткачук А. І. Цивільний захист. Курс лекцій : навч. посіб. / А. І. Ткачук, О. В. Пуляк. // Перевид., доп. та перероб. Кропивницький : Авангард, 2017. 144 с.

20. Глобальні енерго-еколого-кліматичні проблеми та невідкладність їх вирішення : підручник / П. М. Каніло, Н. В. Внукова, А. М. Туренко, А. В. Гриценко. Харків : ХНАДУ, 2020. 388 с.

21. Стешенко О. Д. Ризикологія : навч. посібник. Харків: УкрДУЗТ, 2019. 180 с.


ДЛЯ НОТАТОК

Навчальне видання

ДУБІНІН Віктор Андрійович
МАРКІНА Людмила Миколаївна
УШКАЦ Світлана Юріївна
ЖОЛОБЕНКО Наталія Юріївна
ВЛАСЕНКО Олег Васильович

МЕТОДИЧНІ ВКАЗІВКИ

до виконання практичних робіт за темою: «Ризик-стратегія в управлінні безпекою суб'єкта господарювання у надзвичайних ситуаціях»

Комп'ютерне верстання *В. В. Москаленко*
Коректор *О. Є. Вакула*

Формат 60×84/16. Ум. друк. арк. 3,7. Тираж 100 прим. Вид. № 4. Зам. № 0202-05.
Видавець і виготівник Національний університет кораблебудування
імені адмірала Макарова
просп. Героїв України, 9, м. Миколаїв, 54025
E-mail : publishing@nuos.edu.ua
Свідоцтво суб'єкта видавничої справи ДК № 6402 від 19.09.2018 р.