МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

В.В. Березуцький

М.І. Адаменко

НЕБЕЗПЕЧНІ ВИРОБНИЧІ РИЗИКИ ТА НАДІЙНІСТЬ

Навчальний посібник

для студентів за напрямком підготовки 6.170202 – Цивільна безпека, спеціальність – Цивільна безпека, спеціалізація - Охорона праці

Харків
НТУ «ХПІ»
2016

УДК 658:382.3
ББК 65.247
Б 48

Рецензенти:

Ворожбіян М.І. - д-р техн. наук, проф., завідувач кафедри безпеки життєдіяльності, ХНУЗТ;

Логвінков С.М. – д-р техн. наук, проф., завідувач кафедри технології, екології та безпеки життєдіяльності, ХНЕУ ім. С. Кузнеця;

Хворост М.В. - д-р техн. наук, проф., завідувач кафедри безпеки життєдіяльності, ХНАМГ

Затверджено
Редакційно-видавничою радою
Національного технічного університету «ХПІ», як навчальний посібник
для студентів спеціальності 6.170202 «Цивільна безпека»,
спеціалізації – охорона праці, протокол №2 від 24.12.2015

Березуцький В.В. , Адаменко М.І.

Б 48 Небезпечні виробничі ризики та надійність: навчальний посібник для студентів за напрямком підготовки 6.170202 «Цивільна безпека»/ В.В. Березуцький, М.І. Адаменко – Харків. : ФОП Панов А. М., 2016. – 385 с.

ISBN 978-617-7293-90-2

Розглянуто основні теорії і питання ризиків та надійності системи «людина – машина», за навчальною програмою «Теорія ризиків», також основні етапи розвитку науки про ризики та надійність технічних систем і людини.

Призначено для студентів спеціальностей з охорони праці, інженерно-технічних працівників, науковців, аспірантів.

Табл.16. Іл.39. Бібліогр.12/30 назв.

УДК 652.382.3
ББК 65.247

ISBN 978-617-7293-90-2

ЗМІСТ

Вступ 5

Тема 1. Суть та види ризиків 12

1.1. Теорія ризиків. 12

1.2. Поняття та види ризиків. Фактори ризику. 19

1.3. Страховий ризик і с траховий випадок 58

1.4. Світова інформаційна база ризиків 63

1.5. Досвід зарубіжних країн у сфері управління професійними ризиками 65

Тема 2. Методика визначення ризиків та їх прийнятних рівнів для декларування безпеки об'єктів підвищеної небезпеки 77

2.1. Методика визначення ризиків Міністерства праці та соціальної політики України 04.12.2002 № 637. 77

2.2. Об'єкти підвищеної небезпеки 95

Тема 3. Управління ризиками. Міжнародний стандарт ISO 31000:2009. 111

3.1. «П'яти крокова система» оцінки професійних ризиків 111

3.2. Міжнародний стандарт ISO 31000:2009 112

Тема 4. Менеджмент ризику. Методи оцінки ризику 152

4.1. Сфера застосування Міжнародного стандарту ISO / IEC 31010 152

4.2. Процес оцінки ризику 163

Тема 5. Вибір методів оцінки ризику 173

5.1. Стислий опис методів оцінки ризику 173

5.2. Методи оцінки ризику 180

Тема 6. Системний аналіз системи « людина – техніка – середовище» 301

6.1. Методичні засади визначення небезпечності об'єктів та процесів 301

6.2. Надійність технічних систем 308

6.3. Глобальний (загальносистемний) ризик відмови системи після

модернізації 315
6.4. Надійність оператора 320
6.5. Фактори надійності оператора 326
6.6. Фактори середовища 328
6.7. Ергономічні фактори 337
7. Аналіз аварійного ризику. План ліквідації аварійних ситуацій 342
7.1. Види техногенних небезпек 342
7.2. Етапи аналізу аварійного ризику 346
7.3. Попередній аналіз небезпек (ПАН) 347
7.4. План ліквідації аварійних ситуацій (ПЛАС) 350
Додаток 375
Список джерел інформації 385

Вступ

Ризик властивий будь–якій формі людської діяльності, це пов’язано з безліччю умов і факторів, що впливають на позитивний результат прийнятих людьми рішень. Історичний досвід показує, що ризик недоотримання намічених результатів особливо проявляється при спільності товарно–грошових відносин, конкуренції учасників господарського обороту. Актуальність теми визначається процесами, що відбуваються в економіці. У подібній ситуації прагнення економічного суб’єкта стабільно й успішно розвиватися стикається з апаратом управління його діяльністю, що тільки формується.

Незважаючи на високий технічний рівень виробництва і науки щорічно в Україні та за її межами травмується і гине велика кількість людей. Щорічно у світі нещасні випадки відбуваються більш ніж з 10 млн людей, причому понад 600 тис. чоловік гине. У США від нещасних випадків щорічно гине понад 55 і більше людей, 8500 чоловік стають інвалідами. У Німеччині кожні 13 секунд відбувається нещасний випадок, кожні 3 хвилини одна людина стає інвалідом, кожні 2,5 години відбувається нещасний випадок зі смертельним результатом. Сьогодні щорічно на виробництві в Україні травмується близько 120 тис. чоловік, з яких 2,5 тис. гине, більше 10 тис. осіб отримують професійні захворювання. Настав час робити висновки – людство не може вирішити проблему збереження життя і здоров’я людей шляхом вдосконалення техніки та розвитку науки. Рішення цього питання пов’язане з людиною або, як прийнято сьогодні називати, людським фактором у виробництві, а тому необхідно зайнятися ним дуже серйозно.

Аналіз нещасних випадків дозволяє виділити три основні ланки : небезпечну поведінку; небезпечну ситуацію; травму. Необхідно звернути увагу на напрямок розвитку подій, який може йти й у зворотню сторону. Тобто людина, яка отримала травму, створює небезпечну ситуацію своєю небезпечною поведінкою. Перша ланка є однією з основних причин, що спричиняють травму або створюють небезпечну ситуацію, яка далі може призвести до нещасного випадку. У свою чергу, небезпечна поведінка – це наслідок психологічного характеру людини, який може бути обумовлений такими факторами:

1). еволюцією людського суспільства, яке за останні 20 – 30 років зазнало значних змін у сфері психіки та інтелекту, що визначило створення досконалих технологій і знарядь праці;

2). умовами праці, що стали більш жорсткими і в багатьох випадках більш небезпечними для життя і здоров'я робітників. Ціна помилки при виконанні виробничих операцій стала більш високою – життя;

3). адаптацею людини до небезпек, що є серйозним ризиком. Ми живемо у світі потенційних загроз і потроху звикаємо до них;

4). ілюзією безкарності, що з'являється як наслідок розглянутого вище. Додаток до цього – повна впевненість у безаварійный та безпечный роботі атомних електростанцій, до аварії на Чорнобильській АЕС, свого часу впевненість у непотоплюваності «Титаніка» та ін.;

5). відсутністю бажання навчатися або зниженням інтенсивності навчання і самонавчання. Сучасне виробництво вимагає від робітників високої кваліфікації;

6). навмисним завищенням вимог безпеки, в результаті чого виконання їх стає неможливим, і у робітників (співробітників) створюється думка про неможливість їх досягнення, а отже, і відсутність необхідності їх виконання;

7). конфліктом безпеки і продуктивності праці.

Про життя людини в умовах потенційної загрози багато написано колегами з інших країн: проф. Л.Ф. Корженьовським [1,2] (Польща), проф.

Л.Хофрейтором [3] (Словаччина), проф. О.І. Запорожцем [4] (Україна) та ін. Людський фактор присутній постійно в техносфері – людина «створює» вироби, починаючи від проектування до виготовлення; «експлуатує» готове обладнання і «споживає» те, що створено іншими; «експлуатує» природу і «перетворює» навколишнє середовище; «формує» відносини в соціумі і між окремими людьми та інше.

На зламі 20 століття вчені психологи встановили, що практично в 80 – 90% випадків аварій та катастроф на виробництві домінуючою причиною є людський фактор.

Виробничі небезпеки завжди мають складну будову, і тому їх можна віднести до складних техніко-ергатичних систем, в яких завжди є потенційна небезпека, що полягає в присутності людини, з повним її набором психофізіологічних особливостей організму і поточного його стану як ланки контролю та (або) управління. Наявність потенційної небезпеки створює ризик. Ризик, поза визначенням, – це дія, спрямована на досягнення бажаної мети в умовах наявності загрози неуспіху або отримання небажаного результату. В англійській термінології застосовують поняття «виробничий ризик», а у французькій – «професійний ризик». Величина ризику визначається за методиками як надійність людини в системі «людина–машина».

Для визначення надійності людини проводять дослідження з метою виявлення її помилок при виконанні певних операцій у заданій послідовності за якийсь відрізок часу.

1. Korzeniowski Leszek. Menedzment. Podstawy zarzadzania / Leszek Korzeniowski. – Krakow. EAS, 2005. – 425 str.;

2. Korzeniowski F. Leszek. Securitologia. Nauka o bezpieczenstwie czlowieka i organizcji spolecznych [Monografia naukowa] /Leszek F. Korzeniowski. – EAS, Krakow, 2008. – 311str.

3. Hofreiter Ladislav,. Zdroje a oblasti konfliktov sucasneho sveta /Ladislav Hofreiter, Juraj Simko. – Akademia ozbrojenych sil generala Milana Rastislava Stefanika, Liptovsky Mikulas, 2007. – 95 str.

4. Запорожець О.І. Щодо проекту концепції управління ризиками надзвичайних ситуацій техногенного і природного характеру./ Запорожець О.І //Безпека життя і діяльності людини – освіта, наука, практика. – К.:Самміт–Книга, – 2007. – С. 10–12.

Сьогодні ці дослідження в Україні практично не проводяться, а тому й навести дані з такого системного аналізу практично неможливо.

Банки даних про помилки людини є основою для виконання досліджень за ризиком, який визначається людським фактором. Банки даних про помилки людства можна розділити на такі три категорії.

1. Банки експериментальних даних, що містять результати лабораторних експериментів і заслуговують більшої довіри, ніж банки даних іншого типу, оскільки меншою мірою можуть зазнавати впливу суб'єктивних оцінок, здатних призводити до помилок.

2. Банки експлуатаційних даних, що є більш реальними, ніж банки експериментальних даних, однак сформувати такий банк достатньо важко, оскільки для цього потрібна ретельна реєстрація дій у реальних умовах експлуатації.

3. Банки суб'єктивних даних, що складаються на основі експертних оцінок. Створення таких банків є порівняно дешевим і не викликає особливих труднощів, оскільки великий обсяг інформації може бути отриманий від невеликої кількості опитаних експертів.

Щоб банки суб'єктивних даних можна було використовувати при аналізі надійності роботи людини, необхідно:

• забезпечити необхідну точність даних (точність банків суб'єктивних даних завжди менша точності банків експериментальних даних);

• гарантувати вірогідність експертних оцінок, суб'єктивні дані повинні надходити тільки від тих осіб, які вважаються висококваліфікованими фахівцями;

• враховувати конкретний характер роботи (ретельно вибирати використовуваний метод оцінки з урахуванням характеру оцінюваної роботи);

• правильно встановити рівень експертного оцінювання. Фактори, що визначають якість оцінюваної роботи, повинні виявлятися на початковому етапі оціночної діяльності;

• чітко визначити процедури оцінювання (чітко описати застосовувану процедуру, метод Дельфі або метод парного порівняння).

Складанням банків даних в Україні практично не займаються, і необхідно цю прогалину заповнювати. Можливим є використання університетів як основних центрів накопичення інформації, для чого необхідно створити єдиний інформаційно-методичний центр.

На Заході, навіть у відносно стабільних економічних умовах, суб'єкти господарювання приділяють пильну увагу питанням управління ризиками. Водночас, в українській економіці, де фактори економічної нестабільності і без того ускладнюють ефективне управління підприємствами, проблемам аналізу та управління комплексом ризиків, що виникають у процесі їх економічної діяльності, приділяється явно недостатня увага.

До недавнього часу подібний підхід домінував не тільки на підприємствах реального сектора економіки, а й у фінансово–кредитних організаціях. Пильну увагу питанню управління ризиками стали приділяти тільки після фінансової кризи, яка чітко позначила всю гостроту цієї проблеми в Україні.

Поняття «ризик» відомо з давніх часів. У вітчизняній економіці дослідження питань теорії ризику було певною мірою затребуване лише до кінця 20–х років 20 століття. Надалі посилювалася роль командно–адміністративних методів управління. Все це в поєднанні з усуненням ринкової мотивації економіки призвело до заперечення проблеми господарського і соціального ризику. Окремі ж розробки з питань виробничих, господарських ризиків не могли претендувати на право вважатися науковим напрямом.

Аналіз опублікованих робіт свідчить про те, що проблема управління ризиками підприємства тією чи іншою мірою дістала відображення в порівняно невеликій кількості наукових праць.

Основна мета дослідження полягає у розкритті змісту проблеми управління ризиками підприємства і в розробці механізму управління ризиками підприємства в сучасних умовах господарювання.

Ризик, слід розуміти як міру небезпеки, що одночасно вказує і на можливість заподіяння шкоди протягом деякого часу, і на його величину. Вимірювати ж ризик у загальному випадку найкраще одиницями збитку, а якщо тяжкість конкретного збитку або характер небажаної події попередньо обговорено, то – безрозмірною ймовірністю або частотою прояву таких подій (наприклад, загибель людини, повне руйнування установки при аварії). Як основні методи безпеки можна рекомендувати: для дослідження – системну інженерію (системний аналіз і системний синтез), для вдосконалення – програмно–цільове планування і управління відповідним процесом. Використання першого методу включає: а) уточнення мети, а також структури й істотних властивостей об'єкта дослідження; б) проблемно–орієнтований емпіричний і теоретичний системний аналіз його життєстійкості з метою виявлення закономірностей появи і зниження можливого збитку; в) системний синтез методів прогнозування показників безпеки та заходів щодо їх забезпечення. Реалізація другого методу проводиться шляхом стратегічного планування (нормування показників безпеки, розробку цільових програм) й оперативного управління їх виконанням (контроль і підтримання цих показників у заданих межах).

Природність і безперервність існування численних небезпек вказують на необхідність у системі забезпечення безпеки : сукупності взаємопов'язаних нормативних актів, організаційно-технічних заходів і відповідних сил і засобів. Її цілями можуть бути: а) стратегічна – висока результативність функціонування відповідного об'єкта (система «людина–машина» чи її окремі компоненти); б) тактична – мінімізація збитку від об'єктивно існуючих для них небезпек. А основними завданнями – задоволення важливих для цього потреб і парирування природно–екологічних, антропогенно–соціальних та техногенно–виробничих загроз.

Критерієм оцінки ефективності цієї системи буде підтримка такого її рівня, який характеризується необхідною якістю або результативністю функціонування відповідного об'єкта, або мінімальними сумарними витратами

(витратами на парирування об’єктивно існуючих небезпек і збитком від їх можливого руйнівного впливу). Оптимальними ж мають вважатися цільові програми та заходи, що забезпечують максимальний приріст безпеки при виділених витратах, або потребують, мінімальних витрат для досягнення її заданого рівня або зниження ризику до певної величини.

Тема 1. СУТЬ ТА ВИДИ РИЗИКІВ

1.1. Теорія ризиків.

1.2. Поняття та види ризиків.

1.3. Страховий ризик і страховий випадок.

1.4. Світова інформаційна база ризиків.

1.5. Досвід зарубіжних країн у сфері управління професійними ризиками.

1.1.Теорія ризиків

Загальні поняття аналізу та оцінки ризиків

Джерелом небезпеки може бути все живе та неживе. Небезпеки не мають вибіркових властивостей, під час свого виникнення вони негативно діють на все оточуюче їх матеріальне середовище. Впливу небезпек зазнає людина, природне середовище, матеріальні цінності. Носіями небезпек є природні процеси та явища, техногенне середовище та дії людей. Небезпеки реалізуються у вигляді потоків речовини, енергії та інформації, вони існують у просторі та в часі.

Розрізняють небезпеки *природного, техногенного* та *антропогенного* походження.

Природні небезпеки обумовлюють стихійні явища, кліматичні умови, рельєф місцевості і ін. Землетруси, виверження вулканів, урагани, бурі та ін. часто супроводжуються травмами та загибеллю людей.

Людина, вирішуючи завдання свого матеріального забезпечення, безперервно діє на середовище проживання своєю діяльністю та продуктами діяльності (технічними засобами, викидами різних виробництв та ін.), генеруючи у середовищі проживання *антропогенні* та *техногенні небезпеки*.

Небезпеки, що створюються технічними засобами, називаються *техногенними*, а *антропогенні* небезпеки виникають у результаті помилкових та несанкціонованих дій людини чи групи людей.

Для зменшення впливу негативних факторів на людину, на природне середовище необхідне проведення ідентифікації та квантифікації небезпек.

Ідентифікація – процес виявлення та з'ясування кількісних, просторових, часових та інших характеристик, необхідних та достатніх для розролення заходів, направлених на забезпечення безпеки життєдіяльності.

Квантифікація – запровадження кількісних характеристик для оцінки складних, якісних понять. Квантифікація здійснюється у вигляді числових, балових прийомів. Наприклад, класи небезпек речовин (4 класи), шкала землетрусів MSK–64 (12 балів) та Ріхтера (9 балів).

Ризик – ймовірність, частота реалізації негативного впливу в зоні перебування людини.

Ризик може бути визначений як частота (розмірність – зворотна часова 1/с), або можливість виникнення події *A* (величина без розміру, знаходиться у межах 0 – 1). У розрахунках ризик прийнято позначати літерою *R* (від англ. слова risk – ризик).

Спеціалісти у галузі безпеки пропонують найбільш загальне визначення: ризик – якісне оцінювання небезпеки.

Якісна оцінка – це відношення кількості тих чи інших несприятливих наслідків *n* до їх імовірної кількості *N* за визначений період часу:

$$R = \frac{n}{N} \qquad (1.1)$$

де *R* – ризик несприятливих наслідків; *n* – кількість несприятливих подій;

N – загальна кількість імовірних подій.

Розрізняють ризик:

- індивідуальний;
- соціальний (далі).

Індивідуальний ризик – частота виникнення впливів певного виду, що уражують, виникають під час реалізації певних небезпек у певній точці простору.

Під час аналізу індивідуального ризику необхідно враховувати природу нещасного випадку, частку часу знаходження у зоні ризику та місце знаходження людини, що ризикує.

Розглянемо приклад ризику R впливу на людину небезпечного фактора.

П р и к л а д. Визначити ризик R загибелі людини на виробництві в Україні за рік, коли відомо, що щорічно гине n = 2,5 тис. людей, а чисельність працюючих становить N = 23 млн людей

$$R = \frac{2{,}5 \cdot 10^3}{23 \cdot 10^6} \approx 10^{-4}. \qquad (1.2)$$

П р и к л а д. Щорічно в Україні внаслідок різних небезпек неприродною смертю гине близько 75 тис. людей. Прийнявши чисельність населення країни близько 50,1 млн людей (1999 р.), визначимо ризик R загибелі людини, що проживає в країні, від небезпек:

$$R = \frac{75 \cdot 10^3}{50{,}1 \cdot 10^6} \approx 14{,}9^{-4}. \qquad (1.3)$$

П р и к л а д. Визначити ризик загибелі від проживання та роботи у м.Харкові, при чисельності 2 млн людей, якщо щорічно гине з різних причин близько 5 000 людей

$$R = \frac{5 \cdot 10^3}{2 \cdot 10^6} \approx 2{,}5 \cdot 10^{-4}. \qquad (1.4)$$

Важливо знати величину ризику під час вибору місця роботи, проживання, відпочинку. Відомо, що більшість туристів під час вибору відпочинку орієнтується якраз на ці показники. Бізнесмени, вибираючи країну для розширення свого бізнесу та направлення інвестицій, орієнтуються у тому числі і на показники безпеки життєдіяльності.

П р и к л а д: Визначити ризик для працівника А.

Нехай дехто А працює у невеликої фірмі, що налічує 100 працівників. Статистичні дані за 50 років, які ми маємо, інформують про те, що за цей час із

кількості працівників фірми двоє працівників загинуло та 50 постраждало від нещасного випадку. Чисельність працівників (загальна) за цей період майже не змінювалася.

Працівник А цієї фірми на 4 тижні за рік знаходиться на відпочинку, 2 тижні кожного року проводить у відрядженнях, а решту часу знаходиться у своєму помешканні або відпочиває поза роботою. Працівник працює по 8 годин в одну зміну.

Індивідуальний ризик загибелі для працівника А можна визначити за формулою:

$$R_3 = \frac{N_n \cdot D \cdot t}{T \cdot N_0 \cdot d \cdot t_d} \ , \qquad (1.5)$$

де N_n – чисельність загиблих працівників фірми (N_n = 5,0); d – кількість тижнів у році (d = 52); t_d – кількість годин за тиждень ($24 \cdot 7 = 168$); T – відрізок часу обліку статистичних даних; t – кількість годин у тиждень, коли працівник А знаходиться небезпеці (на роботі): $8 \cdot 6 = 48$; N_0 – чисельність працюючих на фірмі (100); D – кількість тижнів, які житель проводить на роботі: 52 – 4 – 2 = 46.

Індивідуальний ризик стати жертвою нещасного випадку будь–якого ступеня тяжкості для працівника А можна визначити там:

$$R_{ж} = \frac{\left(N_n + N_{тр}\right) \cdot D \cdot t}{T \cdot N_0 d \cdot t_d} \ , \qquad (1.6)$$

де R – ризик отримання травми ($2{,}63 \cdot 10^{-3}$); N – кількість постраждалих від нещасного випадку (N = 150 працівників).

Можна окремо порівняти ризики загибелі працівника $R_{зА}$ та ризик травмування $R_{трА}$.

Знання індивідуального ризику не дозволяє зробити висновок про масштаб катастроф, тому це розглядається у соціальному (груповому) ризику.

Допустимий рівень ризику

Схильність людей до ризикованої для свого життя поведінки пояснюється з еволюційної точки зору, тобто у боротьбі за своє існування людина як вид повинна була дотримуватися деякого допустимого порога ризикованої поведінки, у протилежному випадку вона була б знищена ворожим для неї оточенням, або виродилася б у результаті пасивної поведінки.

Допустимий рівень ризику відображується у багатьох прислів'ях різних народів. Прислів'я «Боягуз не ризикує» вказує на те, що у різних людей різний рівень ризику. У прислів'ї «Вовків боятися – до лісу не ходити» достатньо стисло позначені два види ризику, поміж якими людині у повсякденному житті часто доводиться робити вибір. Перший ризик – стати жертвою вовка, другий – жертвою голоду та холоду. Припустимим вважається перший ризик, а неприпустимим – другий.

Необхідність зниження ризику до деякого допустимого рівня є прямим наслідком неможливості забезпечення нульового рівня ризику.

Припустимий рівень ризику – це імовірність події, негативними наслідками якої на даному етапі розвитку можна знехтувати.

Допустимий рівень ризику формується індивідуальною та суспільною свідомістю та є функцією соціального, економічного і культурного рівня розвитку суспільства.

Розрізняють індивідуальний допустимий рівень ризику та соціальний допустимий рівень ризику.

Кожна окремо узята людина на виробництві та в побуті щоденно та погодинно змушена оцінювати ризик для свого власного життя під час досягнення певної мети. При цьому однією метою нехтують як недопустимою внаслідок того, що її досягнення супроводжується надто великим з точки зору людини, ризиком власної загибелі, іншу ж мають на меті, оскільки ризик

власної загибелі розглядається у цьому випадку як такий, яким можна знехтувати.

Індивідуальний припустимий рівень ризику власної загибелі формується з дитинства та залежить від *виховання, освіти, власної психіки, професії, статі, віку, місця проживання та ін*.

Зрозуміло, що кожен має свої власні поняття про рівень допустимого ризику, які протягом життя змінюються. У явному вигляді це можна спостерігати на пішохідному переході через автомобільну дорогу з інтенсивним рухом, де пішоходи зупиняються на різній відстані від потоку машин, у різні моменти часу та з різною швидкістю починають переходити вулицю.

Ризик загибелі людей під час нещасних випадків, аварій, катастроф, стихійних лих, а також ризик померти від хвороби, що є визначеним у цей момент часу, називається *ризиком, що спостерігається*.

Вважається, що якщо суспільство (держава) не вживає ніяких заходів щодо зниження рівня *ризику, що спостерігається*, то такий ризик є *соціально припустимим.*

Критерієм допустимості можуть служити *асигнування (кошти)*, що виділяються на *охорону здоров'я та забезпечення безпеки людей у широкому розумінні (охорона праці, аварійно–рятувальна служба та ін.).*

Якщо *чисельність* населення країни *збільшується та асигнування* на вказані цілі також *зростають пропорційно чисельності населення*, то рівень ризику смерті людей у цій країні вважається *соціально допустимим*. *Соціально недопустимий рівень ризику* смерті людей спостерігається тоді, коли держава *нарощує асигнування* на забезпечення безпеки людей *більш швидкими темпами*, аніж збільшується чисельність населення.

Соціальний допустимий рівень ризику (допустимий ризик) є деяким компромісом між рівнем безпеки та можливостями її досягнення.

Концепція допустимого ризику – досягнення такого малого ризику, який, з одного боку є технічно можливим, а з іншого боку, – допустимим суспільством у цей час.

Концепція допустимого ризику тісно пов’язана з економічним аспектом у діяльності конкретного промислового підприємства, тому що вона не може підвищуватися до нескінченності. Допустимий ризик має певні обмеження. Для того щоб пояснити сказане вище, розглянемо залежність ризику загибелі людини на підприємстві за рік залежно від фінансових затрат на забезпечення її безпеки (рис. 1.1).

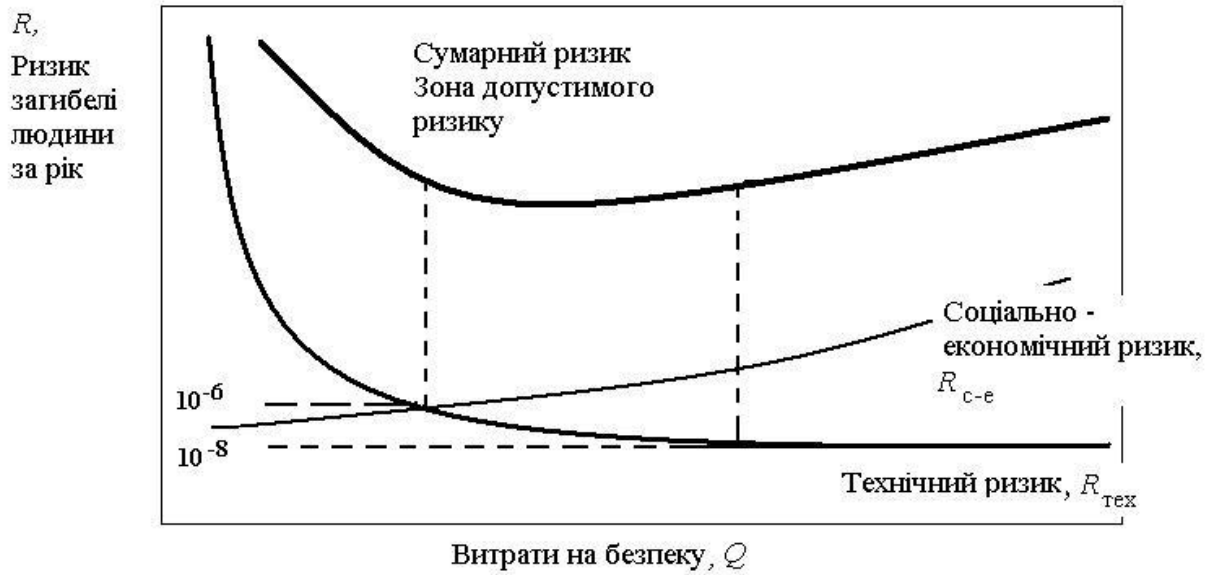

Рисунок 1. 1 – Схема визначення величини допустимого ризику

З підвищенням затрат на безпеку Q спостерігаємо зменшення $R_{тех}$, але зниження технічного ризику $R_{тех}$ відбувається з усе меншою інтенсивністю, а соціально–економічний ризик $R_{с–е}$ підвищується у зв’язку з переведенням коштів із соціальної сфери в технічну. Соціально–економічний ризик $R_{с–е}$ визначається, перш за все, збитками у здоров’ї людини через погіршення стану природного середовища та медичної допомоги. Враховуючи закономірність зміни технічного ризику $R_{тех}$ та соціально–економічного ризику $R_{с–е}$, знаходимо оптимальну зону допустимого ризику.

Допустимі рівні розрізняють для ризиків вимушеного (професійного) та добровільного.

Шкалу небезпек життєдіяльності людини наведено в табл.. 1.1.

Таблиця 1.1 – Класифікація оцінки допустимості ризику

Характеристика умов праці	Рівень ризику смерті за рік	Оцінка допустимості ризику
безпечні	нижче і 10^{-9}, 10^{-8}, 10^{-7}	дуже малий
відносно безпечні	10^{-6}, 10^{-5}, 10^{-4}	відносно невисокий – допустимий
небезпечні	10^{-3}, 10^{-2} і більше	високий, необхідні засоби захисту

Таким чином, індивідуальний допустимий рівень ризику має складати $10^{-9} – 10^{-7}$.

Допустимий ризик у професійній сфері зазвичай беруть $10^{-6} – 10^{-4}$ і недопустимим вважають ризик 10^{-3}, 10^{-2} і більше.

Значення величин ймовірності загибелі людини за рік на виробництві, що знаходиться у межах $10^{-6} – 10^{-4}$, називають зоною оптимізації допустимого професійного ризику, у якій міра захисту від конкретних небезпек повинна братися з урахуванням економічного обґрунтування та доцільності.

1.2. Поняття та види ризиків. Фактори ризику.

Ризик – можлива небезпека будь–якого несприятливого результату.

Ризик–менеджмент, *управління ризиками* – процес прийняття і виконання управлінських рішень, спрямованих на зниження ймовірності виникнення несприятливого результату і мінімізацію можливих втрат, спричинених його реалізацією.

Екологічний ризик – ймовірність виникнення негативних змін у навколишньому природному середовищі, або віддалених несприятливих наслідків цих змін, що виникають внаслідок негативного впливу на довкілля.

Екологічний ризик розуміють як ймовірність несприятливих для навколишнього середовища наслідків будь–яких змін природних об’єктів і факторів. Ризик розглядається як ймовірність виникнення надзвичайних подій у певний проміжок часу, виражена кількісними параметрами. Частіше розглядається техногенний аспект екологічного ризику – ймовірність виникнення техногенних аварій, шо здатні завдати істотної шкоди навколишньому середовищу або здоров’ю людей. Одні ризики конкретні, інші не можуть бути конкретно визначені. Існують професійні ризики – небезпека професійних захворювань.

Екологічний ризик часто розглядають у двох аспектах – потенційний і реальний ризики. Потенційний екологічний ризик – це явище небезпеки порушення відносин живих організмів із навколишнім середовищем внаслідок дії природних чи антропогенних чинників. Реальний екологічний ризик утворюється потенційним з урахуванням ймовірної частоти його реалізації. За характером прояву екологічний ризик може бути раптовим (техногенна аварія, землетрус тощо) і повільним (зсув, підтоплення, ерозія тощо).

Оцінка ризику – це аналіз причин його виникнення і масштабів прояву в конкретній ситуації. Небезпеку виникнення техногенних аварій, значних за своїми наслідками, більше пов’язують із хімічними та нафтохімічними підприємствами, атомними і тепловими електростанціями, шахтами, каналізаційними спорудами. Ймовірність виникнення техногенних аварій значною мірою визначається ефективністю природоохоронної діяльності. Вітчизняні експерти вважають, що для України ризик виникнення аварій безпосередньо залежить від трьох груп чинників і описується регресійним рівнянням:

$$R = 6{,}77 - 0{,}56X_1 - 0{,}43X_2 - 0{,}27X_3 \qquad (1.7)$$

де X_1 – ефективність екологічної політики місцевих органів влади; X_2 – капітальні вкладання в ресурсозберігаюче та природоохоронне устаткування; X_3 – ефективність реалізації екологічних державних програм.

Отже, дієвість такої політики (X_1) обумовлюється перш за все прийняттям місцевими радами ефективних нормативних рішень, що регулюють питання охорони навколишнього середовища. У групі чинників X_2 основна функція, це забезпечення економічного стимулювання екологічних заходів.

Для оцінки екологічного ризику часто використовують технологію «нейронних мереж», яка дає можливість забезпечувати аналітичну підтримку рішень, коли використання традиційних статистичних методів спричиняє труднощі. Важливою властивістю нейронних мереж є здатність до самонавчання з метою поліпшення якості функціонування, що досягається за допомогою алгоритмів, які навчають і визначають, як мають змінюватися зв'язки у відповідь на вхідну дію.

Моделювання з використанням реальних емпіричних даних дозволило визначити мінімально та максимально можливі рівні ризику виникнення техногенних аварій у регіонах України. Оцінка рівня ризику здійснювалася за 7 – баловою шкалою (табл. 1.2).

Таблиця 1.2 – Шкала оцінки техногенного ризику

Рівень	Низький	Незначний	Помірний	Середній	Підвищений	Значний	Високий
Оцінка (бали)	1	2	3	4	5	6	7

З'ясувалося, що для зменшення існуючого показника середнього рівня виникнення аварій (3,8 бала) до мінімально можливого (2,17 бала) необхідне підвищення ефективності основних чинників (табл. 1.3).

За оцінкою експертів, ризик виникнення техногенних аварій по регіонах України сильно відрізняється – від 5,5 для Одеської області до 2,1 для Чернігівської. У більшості областей він перевищує 4 і лише в Полтавській, Кіровоградській і Чернігівській – трохи менше 3,0.

Підприємницький ризик – узагальнюючий термін для групи ризиків, що виникають на різних етапах обігу капіталу в результаті дій конкурентів,

постачальників сировини і матеріалів, зміни кон'юнктури, технологічних помилок та ін.

Таблиця 1.3 – Значення чинників

Чинник	Ефективність (бали)	
	Існуюча	Необхідна
Екологічна політика місцевої влади	2,65	4,37
Капітальні вкладення в охорону природи	1,68	2,28
Капітальні вкладення в ресурсо – та енергозбереження	1,67	2,16
Реалізація програми охорони НПС України	2,83	4,37
Реалізація програми запобігання і реагування на аварії та інші надзвичайні ситуації	3,39	4,42
Реалізація програми охорони земель	2,44	3,0

У межах управлінського ризику виділяють особливий вид ризику – підприємницький.

Господарський (підприємницький) ризик слід розуміти як ризик, що виникає при будь–яких видах діяльності, пов'язаних із виробництвом продукції, товарів, послуг, їх операціями, комерцією, здійсненням соціально–економічних і науково–технічних проектів. Виходячи з цього визначення господарський ризик – це явище, ознака і властивість діяльності, а не тільки поняття [5].

5. Осадець С.С. Страхування : підручник / С.С. Осадець; Керівник авт. колективу і наук. ред. С.С. Осадець. – Вид. 2–ге, перероб. і доп. – К. : КНЕУ, 2002. – 599 с.

Причини, що зумовлюють підприємницький ризик, можна згрупувати за сферою прояву:

1) внутрішні

- недоліки у системі управління;
- недоліки організації процесу виробництва;

2) зовнішні

- поведінка контрагентів;
- похибки у визначенні попиту;
- природно–кліматичні умови;
- зміни ринкової кон'юнктури;
- зміни економічних факторів;
- політичні.

Підприємницький ризик характеризується як небезпека потенційно можливої, ймовірної втрати ресурсів чи недоотримання доходу порівняно з варіантом, розрахованим на раціональне використання ресурсів. Іншими словами, ризик – це погроза того, що підприємець зазнає втрат у вигляді додаткових витрат, понад передбачених прогнозом, програмою його дій або отримає доходи нижчі за ті, на які він розраховував.

Політичний ризик (англ. *Political risk*) – це міра очікуваної невдачі політичної діяльності, що визначається як співвідношення ймовірності неуспіху вжитих заходів та ступеня несприятливих наслідків, зумовлених втіленням прийнятих політичних рішень.

Страховий ризик – певна подія, на випадок якої проводиться *страхування* і яка має ознаки *ймовірності* та випадковості настання.

Страховий ризик – це ймовірність зазнати втрат очікуваної економічної (фінансової) користі або прямих збитків через появу невизначіної (випадкової) події, що стосується майнового інтересу членів суспільства.

Страховий ризик – це обставина, внаслідок якої застрахована *особа* або члени її сім'ї можуть втратити тимчасово засоби існування та потребувати

матеріального забезпечення або надання соціальних послуг за загальнообов'язковим державним соціальним страхуванням у зв'язку з тимчасовою втратою працездатності та витратами, зумовленими народженням та похованням[6].

Страховий ризик не повинен бути:

- неминучим;
- невідворотним [7].

Класифікація страхових ризиків:

- чисті – здійснюється *страхове відшкодування*;
- спекулятивні – переважно виникають при азартних іграх, лотереях, які не потребують страхового захисту, адже передбачають як втрати, так і прибутки (виграш).

1. Залежно від джерела небезпеки (походження):

- природні (об'єктивні) – зумовлені проявом стихійних сил природи. Природне походження ризиків характеризується цілковитою незалежністю причин їх виникнення від суб'єкта (випадкова подія, стихійне явище);
- антропогенні (суб'єктивні) – виникають як наслідок діяльності людей. Вони є похідною економічних, технологічних та організаційних змін, що являють собою необхідну умову розвитку суспільства.

2. З огляду на ризикогенні об'єкти:

- майнові – виявляються на майнових об'єктах та у майнових інтересах власників певних видів майна;
- особисті – притаманні людям. Це ризики фізичного, фізіологічного та соціального походження.

3. За об'ємом відповідальності:

- індивідуальні ризики характерні для окремих особливих предметів, таких як антикваріат, твори мистецтва тощо;

6. Закон України «Про загальнообов'язкове державне соціальне страхування» [Електроний ресурс] – режим доступу: http://zakon4.rada.gov.ua/laws/show/1105-14

7. Заіка Ю.О. Українське цивільне право: навч. посіб/ Ю.О. Заіка ─ К. : Істина, 2005. ─ 312 с.

• універсальні ризики входять до об'єму відповідальності страховика за більшістю договорів страхування.

4. За кількісними параметрами (величина збитка):

- катастрофічні;
- великі;
- середні;
- малі;
- незначні;
- звичайні.

5. У загальному розмежуванні ризиків виділяють такі їх групи:

• *політичні ризики* пов'язані з непередбачуваними діями, заходами чи акціями законодавчих або виконавчих органів влади, іноземних держав щодо конкретної суверенної держави, підприємств або приватних осіб цієї держави;

• *екологічні ризики* пов'язані зі забрудненням довкілля і зумовлені діяльністю людини у виробництві;

• *транспортні ризики* поділяють на

ризики *каско* (*страхування* різноманітних транспортних засобів) і

ризики *карго* (*страхування* вантажів, що перевозяться різними видами транспортних засобів);

• *технічні ризики* проявляються як аварії внаслідок раптового виходу з ладу машин, обладнання, збою в технології виробництва. Вони мають універсальний характер, можуть завдати *збитків* майну, життю, здоров'ю людей та майновим інтересам юридичних осіб. Технічні ризики можуть проявлятися як *промислові ризики*, будівельно – монтажні тощо [1].

Основними характеристиками ризику, які мають велике значення для *страхування*, є:

• частота настання події щодо місця та часу – визначає ступінь настання страхових випадків за тим чи іншим видом *страхування*. Розраховується як

відношення кількості страхових випадків до кількості договорів страхування або кількості застрахованих об'єктів за певним видом страхування. Об'єкти, що пропонуються на страхування, відрізняються різним ступенем небезпеки. На практиці спостерігаються періоди часу різкого підвищення страхового ризику, коли значно зростає кількість несприятливих подій із негативними наслідками;

- важкість наслідків (величина збитку) визначається як матеріальний збиток, завданий страхувальнику внаслідок страхового випадку. На основі величини збитку (з урахуванням системи страхового забезпечення) виконуються розрахунки страхового відшкодування [8].

Ризик – можливість того, що все відбуватиметься не так, як очікується, можливість припуститися помилки.

Вивчення, оцінка і зменшення ризиків завжди мали велике значення у господарській діяльності. Оскільки знання кожної людини і людства в цілому обмежені, а життя має безліч проявів, ризики завжди будуть присутні в людській діяльності (старовинне формулювання – «всі люди грішні»).

Кількісні методи оцінки, прогнозування і роботи з ризиками почали з'являтись відносно недавно, у зв'язку з розвитком математики починаючи з XVII ст.

Напрям у математиці, який безпосередньо присвячений вивченню і оцінці ризиків – *актуарна математика*. Також до вивчення ризиків мають відношення страхова математика, фінансова математика, теорія ймовірностей та математична статистика.

Актуарна математика – напрям у математиці, який вивчає питання, пов'язані з оцінкою ризиків у різних сферах людської діяльності.

Теорія ймовірності вивчає ризики у маркетингу (рис. 1.2).

8. Вовчак О.Д. Страхова справа : підручник/О.Д. Вовчак. – К. : Знання, 2009. – 425 с

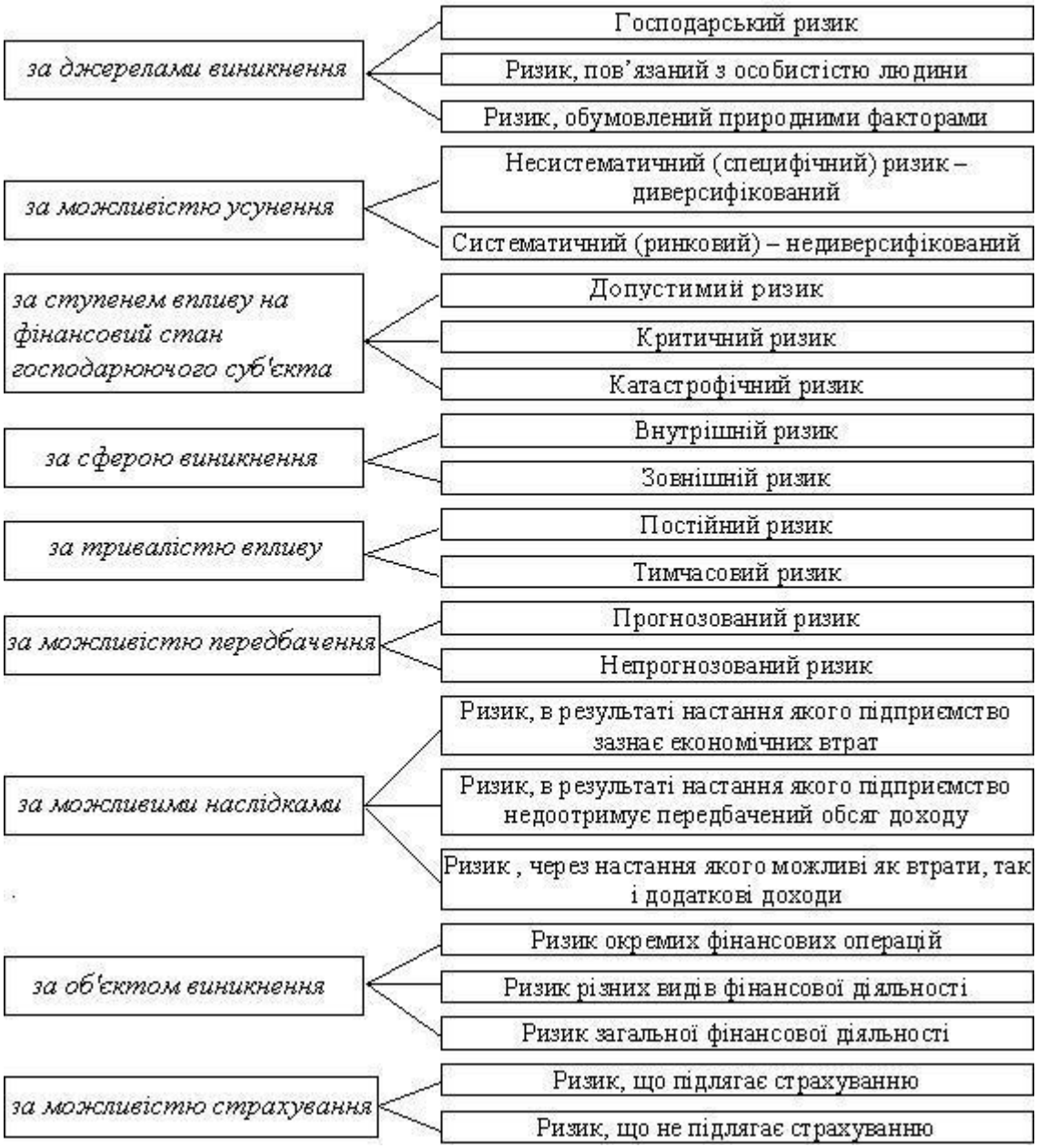

Рисунок 1.2 – Класифікація ризиків

Діяльність – це процес взаємодії людини з довкіллям, завдяки чому вона досягає свідомо поставленої мети, яка виникла внаслідок появи потреби.

Усі види діяльності поділяються умовно на такі:

- Архітектурна діяльність;
- Аудиторська діяльність;

- Безумовно рефлекторна діяльність;
- Благодійна діяльність;
- Видавнича діяльність;
- Вища нервова діяльність;
- Геологічна діяльність;
- Господарська діяльність;
- Девелоперська діяльність;
- Депозитарна діяльність;
- Діяльність з розповсюдження християнства;
- Діяльність людська;
- Зовнішньоекономічна діяльність;
- Інвестиційна діяльність банку;
- Інноваційна діяльність;
- Комерційна діяльність з цінних паперів;
- Комісійна діяльність з цінних паперів;
- Метрологічна діяльність;
- Миротворча діяльність;
- Містобудівна діяльність;
- Монопольна діяльність
- Наукова діяльність;
- Науково–інформаційна діяльність;
- Незаконна торговельна діяльність;
- Основна діяльність неприбуткових організацій;
- Періодична діяльність травної системи;
- Періодична моторна діяльність шлунка;
- Політична діяльність;
- Професійна діяльність;
- Психологія діяльності в особливих умовах;

- Спільна підприємницька діяльність;
- Топографо–геодезична і картографічна діяльність.

Ризик властивий будь–якій сфері людської діяльності, що пов’язано з безліччю умов і факторів, які впливають на позитивний результат прийнятих людьми рішень. Історичний досвід показує, що ризик недоотримання намічених результатів особливо став виявлятися при спільності товарно–грошових відносин, конкуренції учасників господарського обороту. Тому з виникненням і розвитком капіталістичних відносин з’являються різні теорії ризику, а класики економічної теорії приділяють велику увагу дослідженню проблем ризику у підприємницькій діяльності.

Не можна сказати, що у вітчизняній економіці проблема ризику нова. У 20–х роках, ще у СРСР, було прийнято низку законодавчих актів, що містили поняття виробничо–господарського ризику. У виступах господарських керівників того часу лунали думки про те, що від дозволу питання про ризик залежатимуть темпи розвитку економіки країни. Проте вже до середини 30–х років категорія «ризик» була оголошена буржуазним поняттям.

З ідеологічної точки зору ризик ніяк не поєднувався з проголошеним плановим характером розвитку економіки. Адміністративно–командна система прагнула до знищення реальної підприємливості разом з неминучою її умовою – ризиком.

Ризик становить об’єктивно неминучий елемент прийняття будь – якого господарського рішення через те, що невизначеність – неминуча характеристика умов господарювання. В економічній літературі часто не розрізняють поняття «ризик» і «невизначеність». Насправді перше характеризує таку ситуацію, коли настання невідомих подій дуже ймовірно і може бути оцінено кількісно, а друге – коли ймовірність настання таких подій оцінити заздалегідь неможливо. У реальній ситуації рішення, прийняте підприємцем, майже завжди пов’язане з ризиком, обумовленим наявністю низки чинників невизначеності, заздалегідь непередбачуваних.

Для розуміння природи підприємницького ризику фундаментальне значення має зв'язок ризику і прибутку. Адам Сміт у своїй роботі «Дослідження про природу і причини багатства народів» відзначав, що досягнення навіть звичайної норми прибутку завжди пов'язане з більшим чи меншим ризиком. Відомо, що отримання прибутку підприємцеві не гарантовано винагородою за витрачений ним час, зусилля, і здібності можуть виявитися як прибутком, так і збитками. Однак підприємець виявляє готовність йти на ризик в умовах невизначеності, оскільки поряд із ризиком втрат існує можливість додаткових доходів. І. Шум Петер у книзі «Теорія економічного розвитку (Дослідження підприємницького прибутку, капіталу, відсотка і циклу кон'юнктури) » пише про те, що якщо ризики не враховуються в господарському плані, тоді вони стають джерелом, з одного боку, збитків, а з іншого – прибутків. Можна вибрати рішення, що містять менше ризику, але при цьому менше буде і прибуток.

Слід зауважити, що підприємець має право частково перекласти ризик на інших суб'єктів економіки, але повністю уникнути його він не може. Справедливо вважається: хто не ризикує, той не виграє. Іншими словами, для отримання економічного прибутку підприємець повинен усвідомлено піти на прийняття ризикового рішення.

Ризик характеризується як небезпека виникнення непередбачених втрат очікуваного прибутку, доходу або майна, коштів у зв'язку з випадковою зміною умов економічної діяльності, несприятливими обставинами. Його величина вимірюється частотою, ймовірністю виникнення того чи іншого рівня втрат.

Невизначеність і ризик у підприємницькій діяльності виконують дуже важливу функцію, укладаючи в собі протиріччя між запланованим та дійсним, тобто є джерелом розвитку підприємницької діяльності. Підприємницький ризик має об'єктивну основу через невизначеність зовнішнього середовища щодо відношенню до підприємництва. Зовнішнє середовище включає в себе об'єктивні – *економічні, соціальні та політичні* умови, в рамках яких фірма здійснює свою діяльність і до динаміки яких вона змушена пристосовуватися.

Невизначеність ситуації зумовлюється тим, що вона залежить від багатьох змінних, – контрагентів та осіб, поведінку яких не завжди можна передбачити з прийнятною точністю. Позначається також і відсутність чіткості у визначенні цілей, критеріїв та показників їх оцінки (зсуви у суспільних потребах і споживчому попиті, поява технічних і технологічних нововведень, зміна кон'юнктури ринку, непередбачувані природні явища).

Господарські, фінансові та інвестиційні ризики є обов'язковими атрибутами. В цей час прийнято ділити всі ризики на *дві великі групи*. Ризики поділяються на *зовнішні і внутрішні*.

До зовнішніх ризиків належать: природні (ризик стихійних лих та екологічні ризики); загальноекономічні (ризик зміни економічної ситуації, ризик несприятливої кон'юнктури ринку, ризик посилення конкуренції і галузевий ризик); політичні (ризик націоналізації і експропріації, ризик трансферту, ризик розриву контракту, ризик військових дій і громадянських заворушень); фінансові ризики, пов'язані з купівельною спроможністю грошей (інфляційні і дефляційні ризики, валютні ризики, ризики ліквідності, ризик зміни загальноринкової ставки відсотка).

До внутрішніх ризиків належать: виробничі (ризики зниження продуктивності праці, втрат робочого часу або перевитрати; відсутність необхідних матеріалів); технічні (ризики при впровадженні нових технологій або інноваційні ризики; ризики втрат при негативних результатах НДДКР; ризики втрат у результаті збоїв та поломки обладнання); комерційні (ризики, пов'язані з реалізацією товару на ринку; транспортні ризики; ризик, пов'язаний з прийманням товару покупцем; з його платоспроможністю; інвестиційні (ризик упущеної вигоди; процентний ризик; кредитний ризик; біржові ризики; селективний ризик; ризик банкрутства).

Ризики можуть бути класифіковані і за іншими ознаками. Так, наприклад, виділяють ризики чисті та спекулятивні, динамічні і статичні, абсолютні й відносні. Чисті ризики означають можливість одержання збитків або нульового результату. Зазвичай до них належать виробничі та інвестиційні ризики.

Спекулятивні ризики виражаються в ймовірності отримання як позитивного, так і негативного результату. Фінансові ризики, наприклад, вважаються спекулятивними ризиками.

Динамічний ризик – це ризик непередбачених змін внаслідок прийняття управлінських рішень або змін, що відбулися в економічній, політичній та інших сферах суспільного життя. Такі зміни можуть призвести як до втрат, так і до додаткових доходів.

Статичний ризик – це ризик втрат внаслідок заподіяння шкоди власності, а також втрат доходу через недієздатність організації. Цей ризик може призвести лише до втрат.

Абсолютний ризик – ризик, який можна оцінити в грошових одиницях (гривнях, доларах та ін); відносний ризик – у частках одиниці або у відсотках. Наприклад, ризик у підприємництві можна виміряти абсолютною величиною – сумою збитків та втрат і відносною величиною – ступенем ризику, тобто мірою ймовірності нездійснення наміченого заходу або недосягнення запланованого рівня прибутку, доходу, ціни. Обидва показники необхідні і мають відповідну інформацію абсолютного і відносного ризику.

Крім усього іншого, потрібно враховувати *інфляційний ризик* (спричинений непередбаченим зростанням витрат виробництва внаслідок інфляційного процесу); ризик *незбалансованої ліквідності* (небезпека втрат у разі неспроможності банківської установи покрити свої зобов'язання по пасивах банку вимог за активами); *ризик цінової зміни* (ризик зміни ціни боргового зобов'язання унаслідок зростання або падіння поточного рівня процентних ставок).

З безлічі ризиків особливо потрібно звернути увагу на *господарський* або *підприємницький* ризик. Це ризик, що виникає при будь–яких видах діяльності, пов'язаний з виробництвом продукції, товарів, послуг, їх реалізацією, комерцією, фінансовими операціями та здійсненням різних проектів.

При визначенні ризику не варто плутати поняття «витрати», «збитки» і «втрати». Будь–яка підприємницька діяльність неминуче пов'язана з

витратами, тоді як збитки мають місце при несприятливому збігу обставин, прорахунки і становлять додаткові витрати понад намічених. До збитків належать і будь–які витрати, що не приносять ефекту, доцільного результату.

Існує також вид економічних втрат, які іменують «втраченими можливостями». Наприклад, гонщик вирішив брати участь у ралі Великобританії і для цього придбав спеціальні грязьові покришки, але, приїхавши на гонку, виявив, що покришки з дефектами і брати участь у ралі на них не можна. Таким чином, гонщик повернувся додому без золотого кубка. У даному випадку це і є втрачені можливості.

Фактори ризику

Підприємницький ризик складається під впливом об'єктивних (***зовнішніх***) і суб'єктивних (***внутрішніх***) чинників.

До найбільш важливих зовнішніх факторів належать: інфляція (значне і нерівномірне зростання цін на сировину, матеріали, паливо, енергоносії, комплектуючі вироби, транспортні та інші послуги, а також на продукцію та послуги підприємства); зміна банківських процентних ставок та умов кредитування, податкових ставок і митних зборів; зміни у відносинах власності та оренди, у трудовому законодавстві та ін. Не менш небезпечним для діяльності підприємства є вплив внутрішніх факторів, пов'язаних із помилками й упущеннями керівництва та персоналу. Так, за оцінками зарубіжних експертів, 90 % різних невдач малих фірм пов'язано з недосвідченістю керівництва, його невмінням адаптуватися до мінливих умов, консерватизмом мислення, що призводить до неефективного управління підприємством, до прийняття помилкових рішень, втрати позицій на ринку.

Економічна поведінка підприємця при ринкових відносинах заснована на виборі на свій ризик, реалізується індивідуальною програмою підприємницької діяльності в рамках можливостей, які випливають із законодавчих актів. Кожний учасник ринкових відносин спочатку позбавлений заздалегідь відомих, однозначно заданих параметрів, гарантій успіху, забезпеченої частки участі в ринку, доступності до виробничих ресурсів за фіксованими цінами,

стабільності купівельної спроможності грошових одиниць, незмінності норм і нормативів та інших інструментів економічного управління.

Наявність підприємницького ризику – це, по суті зворотна сторона економічної свободи, своєрідна плата за неї. Отже, в міру розвитку ринкових відносин у нашій країні буде посилюватися невизначеність і підприємницький ризик.

Усунути невизначеність майбутнього у підприємницькій діяльності неможливо, тому що вона є елементом об'єктивної дійсності. Ризик властивий підприємництву і є невід'ємною частиною його економічного життя. До сьогодні ми звертали увагу тільки на об'єктивну сторону підприємницького ризику. Дійсно, ризик пов'язаний із реальними процесами в економіці. Об'єктивність ризику обумовлена наявністю факторів, існування яких, зрештою, не залежить від дії підприємців.

Тим не менше, деякими вченими розглядається суб'єктивна сторона ризику. Така точка зору не позбавлена сенсу. Сприйняття ризику залежить від кожної конкретної людини з її характером, складом розуму, психологічними особливостями, рівнем знань у галузі її діяльності. Для одного підприємця певна величина ризику є допустимою, тоді як для іншого – недопустимою.

За американськими стандартами всі люди поділяються на дві категорії: ризикованих і більш обережних, що йдуть на прийняття рішень тільки з мінімальними шансами на ризик. Для підприємця важливо знати, до якої групи він належить, тому для визначення схильності до ризику психологами розроблено різні тести.

У цей час можна виділити дві форми підприємництва. Передусім це комерційні організації, засновані на старих господарських зв'язках. У ситуації невизначеності такі підприємці прагнуть уникати ризику, намагаючись пристосовуватися до умов господарювання, що змінюються. Друга форма – це новостворені підприємницькі структури, які характеризуються розвинутими горизонтальними зв'язками, широкою спеціалізацією. Такі підприємці готові

ризикувати, в ризиковій ситуації вони маневрують ресурсами, здатні дуже швидко знаходити нових партнерів.

У прийнятті підприємцем рішення, пов'язаного з ризиком, важливим є його проінформованість, досвід, кваліфікація, ділові якості. Підприємець схильний до ризикованих рішень в тому випадку, якщо упевнений у професіоналізмі виконавців. Також готовність йти на ризик значною мірою визначається під впливом результатів реалізації попередніх рішень, прийнятих у тих самих умовах. Помилки, допущені раніше в аналогічній ситуації, диктують вибір більш обережної стратегії. Принципове рішення про прийняття ризикового проекту залежить від переваг підприємця, що приймає це рішення, між очікуваною прибутковістю (рентабельністю) вкладених у цей проект коштів (у середньому за значний період часу) та їх надійністю, що, у свою чергу, розуміється як неризикованість, ймовірність отримання доходів.

Види втрат

Оцінка величини ризику та його допустимості потребує, перш за все, знання основних видів втрат. Кожному з таких видів властива своя шкала можливості виникнення тієї чи іншої величини втрат. Тому у всіх випадках, коли заздалегідь не відомо, який з видів втрат має визначальний характер і з рештою яким слід знехтувати, необхідно аналізувати різні види втрат. До речі, саме такий аналіз і дозволяє частіше за все встановити, який вид втрат є найбільш небезпечним.

Потрібно ще раз нагадати, що аналізувати можна випадкові, непередбачені, але потенційно можливі втрати, які виникають внаслідок відхилення реального перебігу підприємництва від задуманого сценарію, а не витрату ресурсів, пов'язану з видом і характером підприємницької діяльності.

Відповідно втратами будемо вважати зниження прибутку, доходу порівняно з очікуваними величинами. Підприємницькі втрати – це насамперед чергу випадкове зниження підприємницького прибутку.

Щоб оцінити ймовірність тих чи інших втрат, зумовлених розвитком подій з непередбаченого варіанта, необхідно, перш за все, знати всі види втрат, пов'язаних із підприємництвом, і вміти заздалегідь обчислити їх або виміряти як ймовірні прогнозні величини. При цьому природним є бажання оцінити кожний з видів втрат у кількісному вимірі і вміти звести їх воєдино, що, на жаль, далеко не завжди вдається зробити.

В абсолютному вираженні ризик може визначатися величиною можливих втрат у матеріальному (фізичному) або вартісному (грошовому) вимірі в гривнях, якщо тільки збиток можна так виміряти. При такому підході кажуть: «Є ризик залишитися голодним» або «Перед нами ризик втратити весь наш вклад ».

У відносному вираженні ризик визначається як величина можливих втрат, що належить до деякої бази, у вигляді якої найбільш зручно приймати або майновий стан підприємця, або загальні витрати ресурсів на цей вид підприємницької діяльності, або очікуваний дохід (прибуток) від підприємництва. При такому підході кажуть: «Існує ризик втрати половини прибутку».

Тільки через недосконалість використовуваних методів розрахунку підприємницької діяльності або недостатньо глибоке опрацювання підприємцем бізнес–плану систематичні помилки можуть розглядатися як втрати в тому сенсі, що вони здатні погіршити очікуваний результат.

Отже, перш ніж оцінювати ризик, обумовлений дією суто випадкових факторів, вкрай бажано відокремити систематичну складову втрати від випадкових. Це необхідно і з позицій математичної коректності, тому що процедури дій з випадковими величинами істотно відрізняються від процедур дій з детермінованими величинами.

Аналіз ризику і методи його оцінки. Ризик, якого зазнає підприємство, – це ймовірна загроза розорення або несення таких фінансових втрат, які можуть зупинити всі справи. Оскільки ймовірність невдачі присутня завжди, постає питання про методи зниження ризику. Для відповіді на це запитання необхідно

кількісно визначити ризик, що дозволить порівняти величину ризику різних варіантів рішення і вибрати з них той, який найбільше відповідає вибраній підприємством стратегії ризику.

При аналізі ризику зазвичай використовуються допущення, запропоновані відомим американським експертом Б. Берлімером:

- втрати від ризику незалежні один від одного;
- втрата за одним напрямком діяльності не обов'язково збільшує ймовірність втрати за іншим, за винятком форс–мажорних обставин;
- максимально можливий збиток не повинен перевищувати фінансових можливостей учасника.

Аналіз ризиків можна підрозділити на два доповнюючі один одного види: *якісний* і *кількісний.*

Якісний аналіз дозволяє визначити фактори і потенційні сфери ризику, виявити можливі його види. *Кількісний аналіз* спрямований на те, щоб кількісно виразити ризики, провести їх аналіз та порівняння. При кількісному аналізі ризику використовуються різні методи. Сьогодні найбільш поширеними є:

- статистичний метод;
- аналіз доцільності витрат;
- метод експертних оцінок;
- метод аналогій.

Кількісна оцінка ризику. Безсумнівно, що ризик є ймовірною категорією, і в цьому сенсі найбільш обґрунтовано з наукових позицій характеризувати і виміряти його як ймовірність виникнення певного рівня втрат.

Строго кажучи, за всебічної оцінки ризику слід потрібно б встановлювати для кожного абсолютного або відносного значення величини можливих втрат відповідною ймовірність виникнення такої величини.

Вся система соціального забезпечення створюється і функціонує в державі для захисту населення від соціального ризику. Саме соціальні ризики є наріжним каменем всього соціального забезпечення (не слід плутати із

визначенням соціального ризику в аналізі травматизму).

Соціальний ризик – частота виникнення подій, існуючих у поразках певної кількості людей, що підлягають уражаючим діям певного виду, під час реалізації певних небезпек.

Соціальний ризик характеризує масштаб катастрофічності небезпек відповідно до виробництва. Наприклад: 10 смертельних випадків могли статися під час 5 аварій на підприємстві, у кожному з них могло бути по дві жертви, але 10 чоловік могло б загинути і під час однієї аварії на підприємстві. Соціальний ризик допомагає оцінити *F–N* діаграма (рис. 1.3).

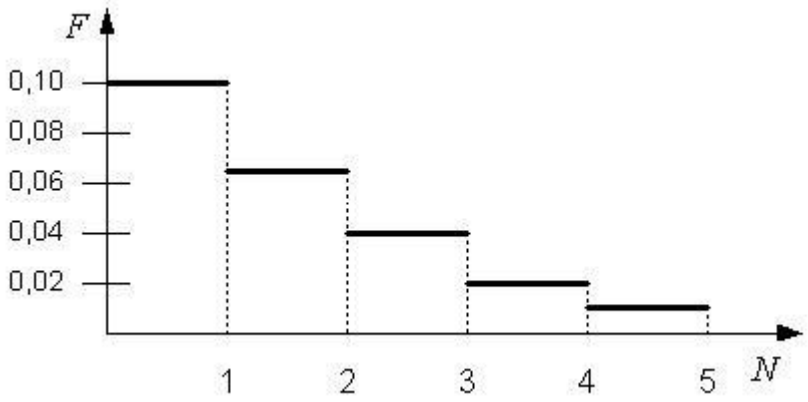

Рисунок 1.3 – Діаграма залежності частоти реалізації небезпеки від її масштабу

На підставі статистичних даних збирається інформація: кількість загиблих *N*, кількість подій, в яких загинуло *N* працівників, частота подій (кількість випадків за рік) *F*, в яких загинуло *N* працівників. За цими даними будується графік залежності *F–N*.

Діаграму використовують для показу залежності частоти реалізації небезпеки від її масштабу (масштаб небезпеки – наприклад, об’єм газу, що вибухає).

Теорію «соціальних ризиків» почали інтенсивно розробляти ще в 20 – 30 – ті рр. минулого століття. Згідно із цією теорією, соціальне забезпечення надається членам суспільства в зв’язку із настанням різних обставин, так званих соціальних ризиків, а соціальний ризик автори розуміють як ризик втрати заробітку. Матеріальний рівень у сучасному суспільстві залежить від заробітку. Будь–кому, хто живе за рахунок продажу своєї робочої сили,

загрожує дві небезпеки – втрата працездатності, з одного боку, і безробіття, з іншого. І в тому, і в іншому випадку особа втрачає заробіток. Саме цей ризик втрати заробітку і є соціальним ризиком.

Соціальний ризик сьогодні також слід розуміти як ймовірні події, що породжуються об'єктивними соціально–значущими причинами і призводять до втрати заробітку особи, зниження доходів нижче прожиткового мінімуму, необхідності в медичній допомозі та інших соціальних послугах.

Ознаки соціального ризику:

– мають об'єктивний характер, наступають незалежно від волі особи;

– виникнення цих обставин завжди впливає на матеріальний, життєвий рівень особи;

– закріплені у законодавстві, їх перелік вичерпний, тобто розширеному тлумаченню не підлягає;

– є підставою для призначення того чи іншого виду соціального забезпечення, тобто є обов'язковою частиною юридичного складу, який спричиняє виникнення, зміну або припинення соціально–забезпечувальних правовідносин.

Класифікація соціальних ризиків може проводитись із різними критеріями. Так, *за критерієм організаційно–правової* форми розрізняють ***страхові*** та ***нестрахові*** соціальні ризики.

За змістом можна виділити такі основні соціальні ризики: *непрацездатність, безробіття, малозабезпеченість, втрата годувальника.*

В Конституції України окреслюється менш вузьке коло соціальних ризиків, ніж передбачено іншими нормативно–правовими документами. Так, у Конституції йдеться про втрату працездатності, старість, втрату годувальника, безробіття. Проаналізувавши сучасне соціально–забезпечувальне законодавство, можна зобразити таку систему соціальних ризиків:

1) безробіття;

2) малозабезпеченість;

3) втрата працездатності: постійна і тимчасова;

4) втрата годувальника (смерть).

Безробіття як соціальний ризик

Законодавчого тлумачення терміна безробіття немає, проте у Законі України «Про зайнятість населення» є визначення безробітного (безробітними визнаються працездатні громадяни працездатного віку, які через відсутність роботи не мають заробітку або інших передбачених законодавством доходів і зареєстровані у державній службі зайнятості як такі, що шукають роботу, готові та здатні приступити до підходящої роботи). Крім того, в Законі України «Про загальнообов'язкове державне соціальне страхування на випадок безробіття» є поняття «втрати роботи з незалежних від застрахованих осіб обставин».

Безробіття – втрата працездатною особою працездатного віку роботи з об'єктивних чи суб'єктивних причин, яка призвела до втрати заробітної плати або інших, передбачених законом доходів.

Факт безробіття встановлюється на підставі Положення про порядок реєстрації, затвердженого Постановою Кабінету Міністрів України від 27 квітня 1998 р. N 578, перереєстрації та ведення обліку громадян, які шукають роботу, і безробітних, виплати допомоги у зв'язку з безробіттям, а також визначають умови подання матеріальної допомоги в період професійної підготовки та перепідготовки.

Реєстрація та облік громадян, які звертаються за сприянням у працевлаштуванні, здійснюється державною службою зайнятості за місцем постійного проживання за умови пред'явлення паспорта і трудової книжки, а у разі потреби – військового квитка, документа про освіту або документів, які їх замінюють.

Незайняті громадяни підлягають реєстрації у цій службі. Під час реєстрації кожна особа самостійно або із застосуванням автоматизованої системи за допомогою працівника державної служби зайнятості заповнює картку персонального обліку громадянина, який шукає роботу (безробітного), і особистим підписом підтверджує достовірність внесених до неї даних.

Зайняті громадяни, які бажають змінити професію або місце роботи, працевлаштуватися за сумісництвом чи у вільний від навчання час і звернулися до державної служби зайнятості, підлягають обліку.

Не можуть бути визнані безробітними громадяни:

а) віком до 16 років, за винятком тих, які працювали і були звільнені у зв'язку із змінами в організації виробництва і праці, реорганізацією, перепрофілюванням і ліквідацією підприємства, установи і організації або скороченням чисельності (штату);

б) які вперше шукають роботу і не мають професії (спеціальності), в тому числі випускники загальноосвітніх шкіл, у разі відмови їх від проходження професійної підготовки або від оплачуваної роботи, включаючи роботу тимчасового характеру, яка не потребує професійної підготовки;

в) які відмовились від двох пропозицій підходящої роботи з моменту реєстрації їх у службі зайнятості як осіб, які шукають роботу;

г) які мають право на пенсію відповідно до законодавства України.

У разі відсутності трудової книжки громадянин, який вперше шукає роботу, повинен пред'явити паспорт, диплом або інший документ про освіту чи професійну підготовку, а звільнені військовослужбовці – військовий квиток.

Крім цих документів окремі категорії громадян під час реєстрації повинні пред'явити також такі документи:

а) громадяни, які втратили роботу внаслідок нещасного випадку на виробництві або настання професійного захворювання і через це потребують професійної підготовки, перепідготовки чи підвищення кваліфікації – довідку медико-соціальної експертної комісії щодо професійної придатності;

б) випускники вищих навчальних закладів, підготовка яких здійснювалась за державним замовленням, яким відмовлено у прийнятті на роботу за місцем призначення, – направлення на роботу і скріплену

печаткою замовника довідку про відмову в працевлаштуванні або довідку про самостійне працевлаштування;

в) особи, які отримують пенсію відповідно до законодавства України, – пенсійне посвідчення або посвідчення інваліда.

Громадянам, зареєстрованим у державній службі зайнятості як таким, що шукають роботу, протягом семи календарних днів з моменту реєстрації підбирається підходяща робота. Семиденний строк підбору підходящої роботи розпочинається з дня реєстрації громадянина як такого, що шукає роботу.

Громадяни, які зареєстровані на загальних підставах у державній службі зайнятості як такі, що шукають роботу, і відмовилися в період пошуку роботи від двох пропозицій підходящої роботи, не можуть бути визнані безробітними. Такі особи знімаються з обліку і їм протягом шести місяців надаються консультаційні послуги. Після закінчення шести місяців з дня зняття з обліку вони можуть зареєструватися повторно у державній службі зайнятості як такі, що шукають роботу.

Неповнолітні, які досягли 15 – ти років і звернулися до державної служби зайнятості за сприянням у працевлаштуванні, можуть як виняток бути зареєстровані як такі, що шукають роботу, за згодою одного з батьків або осіб, що їх замінюють.

Громадяни, зареєстровані у державній службі зайнятості як такі, що шукають роботу, і безробітні зобов’язані сприяти своєму працевлаштуванню, виконувати всі рекомендації центру зайнятості, відвідувати центр зайнятості у строки, встановлені працівником цієї служби.

Для одержання статусу безробітного з призначенням допомоги у зв’язку з безробіттям громадянин повинен наступного дня після встановленого строку підбору підходящої роботи (тобто з восьмого дня після реєстрації) особисто подати до державної служби зайнятості письмову заяву про надання статусу безробітного та заяву про те, що він не має заробітку або інших передбачених законодавством доходів.

Малозабезпеченість як соціальний ризик

Малозабезпеченість – це неспроможність особи чи сім'ї з огляду на об'єктивні чинники забезпечити середньомісячний сукупний дохід на рівні прожиткового мінімуму. У законодавстві є термін «малозабезпечена сім'я». Такою називають сім'ю, яка з поважних або незалежних від неї причин має середньомісячний сукупний дохід, нижчий від прожиткового мінімуму для сім'ї.

Середньомісячний сукупний дохід сім'ї – це обчислений у середньому за місяць дохід усіх членів сім'ї з усіх джерел надходжень протягом шести місяців, що передують місяцю звернення за призначенням державної соціальної допомоги.

Втрата працездатності як соціальний ризик

Втрата працездатності може бути постійна і тимчасова. Постійна втрата працездатності буває повна і часткова. Повна втрата працездатності – настання пенсійного віку (старість). Пенсійний вік в Україні становить 60 років для жінок, 60 років для чоловіків.

Прикладом часткової втрати працездатності є інвалідність. Існує два критерії інвалідності – медичний та економічний. З медичної точки зору – це розлад функцій організму. З економічної точки зору – це таке порушення, яке призводить до втрати працездатності: професійної чи загальної.

Інвалідність – це стійкий розлад функцій організму, зумовлений захворюванням, наслідком травм або вродженим дефектом, який призводить до обмеження життєдіяльності, до необхідності в соціальній допомозі і захисті. Обмеження життєдіяльності – це повна або часткова втрата здатності обслуговувати себе, самостійно пересуватись, орієнтуватись, спілкуватись, контролювати свою поведінку, вчитись, займатись трудовою діяльністю.

Причинами інвалідності можуть бути:

1) трудове каліцтво;
2) професійне захворювання;
3) загальне захворювання;

4) вроджені дефекти.

Інвалідність вважається такою, що настала внаслідок *трудового каліцтва*, якщо нещасний випадок настав:

– під час виконання трудових обов'язків (в тому числі і під час відрядження);

– по дорозі на роботу, або з роботи;

– на території підприємства, установи, організації протягом робочого часу (вкл. перерви);

– поблизу підприємства протягом робочого часу, якщо перебування там не суперечило правилам внутрішнього трудового розпорядку;

– у разі виконання державних або громадських обов'язків;

– у разі виконання дій з урятування людського життя, охорони державної чи приватної власності, охорони правопорядку.

Порядок розслідування та обліку нещасних випадків на виробництві закріплено в Положенні про розслідування та ведення обліку нещасних випадків, професійних захворювань та аварій на виробництві, затвердженому Постановою Кабінету Міністрів від 21 серпня 2001 року.

Інвалідність внаслідок *професійного захворювання* встановлюється на підставі висновку спеціалізованого медичного закладу про наявність професійного захворювання. Перелік таких захворювань закріплений у Постанові Кабінету Міністрів України «Про затвердження переліку професійних захворювань» від 8.11.2000 р.

Професійне захворювання – захворювання, яке виникло внаслідок професійної діяльності застрахованого та зумовлене дією на організм виключно або переважно факторів виробництва, характерних для конкретної професії.

Професійні захворювання можуть бути спричинені виключно дією несприятливих виробничо–професійних факторів, а можуть бути і такими, у розвитку яких встановлено причинний зв'язок впливу певного несприятливого виробничо–професійного фактора та виключено явний вплив інших непрофесійних факторів, що викликають аналогічні зміни в організмі. Крім

того, необхідно враховувати можливість розвитку професійного захворювання через тривалий термін після припинення впливу шкідливих факторів виробництва.

Загальне захворювання як причина інвалідності визначається за залишковим принципом, тобто якщо інвалідність не спричинена нещасним випадком на виробництві чи професійним захворюванням, то її причиною визнається загальне захворювання. До загального захворювання прирівнюють нещасний випадок невиробничого характеру.

Показаннями для встановлення *інвалідності у дітей* є патологічні стани, що виникають при вроджених, спадкових, набутих захворюваннях та після травм.

Тимчасову втрату працездатності розуміють як неспроможність особи виконувати свої трудові обов'язки внаслідок короткотривалих обставин об'єктивного характеру. Тимчасова непрацездатність може бути спричинена:

1) фізичною нездатністю особи здійснювати трудову діяльність (хвороба, травма, вагітність та пологи);

2) неможливістю працювати у зв'язку із необхідністю здійснювати догляд за іншим членом сім'ї (хворою дитиною; хворим членом сім'ї; за дитиною до трьох років; за дитиною до досягнення трьох річного віку або дитиною–інвалідом до 16 років у разі хвороби матері або іншої особи, яка доглядає за цією дитиною);

3) неможливістю працювати у зв'язку із настанням обставин, спричинених діями державних органів (карантин, накладений органами санітарно–епідеміологічної служби).

Порядок видачі документів, які засвідчують тимчасову, затверджено Наказом МОЗ України від 13.11.2001 р.

Втрата годувальника як соціальний ризик

Втрата годувальника є підставою для призначення пенсії в разі втрати годувальника та щомісячних страхових виплат, якщо годувальник помер внаслідок нещасного випадку на виробництві чи професійного захворювання.

Втрату годувальника розуміють як його смерть або безвісну відсутність. Факт смерті підтверджується свідоцтвом або встановлюється судом. Оголошення померлим у судовому порядку проводиться, якщо в місці постійного проживання не має відомостей про перебування особи протягом трьох років, а якщо вона пропала безвісти за обставин, що загрожують смертю або дають підстави припускати загибель від певного нещасного випадку – протягом місяців. Військовослужбовець або інший громадянин, який пропав безвісти у зв'язку із воєнними діями, може бути оголошений померлим не раніше, ніж через два роки з дня закінчення воєнних дій. Оголошення безвісно відсутнім у судовому порядку здійснюється, якщо протягом одного року в місці його постійного проживання не має відомостей про перебування.

Право на отримання певних видів соціального забезпечення мають непрацездатні члени сім'ї померлого годувальника, якщо вони знаходились на його повному утриманні або отримували від нього допомогу, що була постійним і основним джерелом засобів до існування. Непрацездатними членами сім'ї визнаються:

1) діти, які не досягли 16 років; діти з 16 до 18 років, які не працюють; діти, які є учнями, студентами денної форми навчання –до завершення навчання, але не більш як до досягнення ними 23 років;

2) жінки і чоловіки пенсійного віку, якщо вони не працюють;

3) неповнолітні діти, на утримання яких померлий виплачував або зобов'язаний був виплачувати аліменти;

4) дружина (чоловік), або один із батьків померлого чи інший член сім'ї, якщо він не працює та доглядає дітей, сестер, братів або онуків потерпілого, які не досягли 8 - річного віку.

Фактори ризику

Небезпеки впливають на людину завдяки своїм специфічним факторам. Небезпеки класифікують:

- за природою походження – природні, технічні, антропогенні, змішані;

- за часом виявлення негативних наслідків – імпульсивні, кумулятивні;
- за локалізацією – пов’язані з літосферою, атмосферою, космосом;
- за спричиненими наслідками – захворювання, травми, аварії, пожежі, фатальні наслідки та ін.;
- за завданними збитками – технічні, екологічні, соціальні і т.д.;
- за сферами прояву небезпек – побутова, спортивна, дорожньо–транспортна, виробнича, військова та ін.;
- за структурою (будовою) – прості та складні, породжені взаємодією простих;
- за характером впливу – активні та пасивні;
- за здатністю людини ідентифікувати небезпеку органами чуття – відчутні та невідчутні.

Небезпека реалізується вражаючим фактором, а вражаючі фактори можна класифікувати, взявши за основу відомий ГОСТ 12.0.003–74*ССБТ, на фізичні, хімічні, біологічні та психофізіологічні фактори.

Фізичні небезпеки та шкідливі фактори середовища проживання підрозділяються на такі:

- рухомі машини та механізми; рухливі частини устаткування, пересувні вироби, заготовки, матеріали; гострі кромки, нерівність поверхні заготівок, інструментів та устаткування;
- гірські породи, що обвалюються;
- підвищена запиленість і загазованість повітря;
- зони дихання людини нетоксичними речовинами;
- підвищена або понижена температура поверхонь устаткування, матеріалів;
- підвищені або понижені температури, вологість і рухливість повітря, а також підвищений або понижений барометричний тиск та його різкі зміни у робочій зоні;
- підвищені рівні шуму, вібрації, інфразвуку, ультразвуку в місцях знаходження людини;

- підвищена або понижена іонізація повітря; наявність випромінювань із підвищеними рівнями (іонізуючих, лазерних, електромагнітних, ультрафіолетових, інфрачервоних та ін.);
- підвищене значення напруги в електричному колі, замикання якого може виникнути через тіло людини;
- підвищений рівень статичної електрики;
- підвищена напруга електричного та магнітного поля;
- відсутність або недостача природного світла, недостатня освітленість; підвищена яскравість світла, знижена контрастність, пряме та відбите блискотіння, підвищена пульсація світлового потоку;
- розташування місця знаходження людини на значній висоті відносно землі (підлоги).

Хімічні небезпечні та шкідливі фактори середовища існування класифікують *за характером впливу та за шляхом проникнення в організм людини*.

За характером впливу на організм людини їх поділяють на такі види:

- токсичні – окис вуглецю, плюмбум, гідраргіум та ін.;
- сенсибілізуючі (алергени) – антибіотики, натуральні та синтетичні смоли, пил та ін.;
- мутагенні, що впливають на спадковість – радіоактивні речовини, плюмбум, марганець та ін.;
- ті, що впливають на репродуктивну функцію – плюмбум, радій та ін.

За шляхом проникнення в організм людини:

- через органи дихання;
- через шкіру та слизові оболонки;
- через шлунково–кишковий тракт.

За ступенем небезпеки шкідливих речовин хімічні небезпечні та шкідливі фактори середовища проживання підрозділяють на:

- надзвичайно небезпечні;

- високо небезпечні;
- помірно небезпечні;
- мало небезпечні.

Біологічні небезпечні та шкідливі фактори середовища проживання включають такі біологічні об’єкти:

- патогенні мікроорганізми (бактерії, віруси, спірохети, гриби, найпростіші) та продукти їх життєдіяльності;
- мікроорганізми (рослини та тварини).

Психофізіологічні небезпечні та шкідливі фактори середовища проживання за характером впливу поділяють на такі:

- Фізичне перевантаження;
- Нервово–психічні перевантаження.

Фізичні перевантаження підрозділяють на статичні, динамічні, гіподинамічні.

Нервово–психічні перевантаження підрозділяють на розумове перенапруження, перенапруження аналізаторів, монотонність праці, емоційне перевантаження.

Один і той самий небезпечний та шкідливий фактор за природою своєї дії може належити одночасно до різних груп, наведених вище. Тому дуже важливо вірно ідентифікувати фактор навколишнього середовища, тобто визначити його тип та величину.

Хімічні фактори ризику

У цьому підрозділі наведено дослідження Ulrike Tittelbach, Wolfram Dietmar Schneider. Незважаючи на численні дослідження, значення хімічних факторів у розвитку серцево–судинних захворювань хоча і залишається спірним, мабуть, відносно невелике. При підрахуванні частки хімічних професійних факторів в етіології серцево–судинних захворювань у населення Данії, вона становила менше 1 % (Kristensen 1994). Вплив на серцево–судинну систему деяких хімічних речовин, таких, як дисульфід вуглецю й органічні

сполуки азоту, є загальновизнаним (Kristensen 1994). Свинець, як виявилося, впливає на артеріальний тиск і розвиток цереброваскулярної патології. Монооксид вуглецю (Weir і Fabiano 1982), поза всяким сумнівом, має могутній вплив, провокуючи напад стенокардії на фоні вже існуючої ішемії, але, ймовірно, не збільшує ризик розвитку, є в основі ішемічної хвороби атеросклерозу, як це довгий час передбачалося. Роль інших речовин, таких, як кадмій, кобальт, миш'як, сурма, берилій, фосфорорганічні сполуки та розчинники, обговорюється, але до теперішнього часу кількість документальних даних недостатня. Критичний огляд матеріалів пропонує Kristensen (1989, 1994). Підбірку з відповідних видів діяльності та промислових галузей подано в табл. 1.4.

Дані найважливіших досліджень про результати впливу дисульфіду вуглецю, моно оксиду вуглецю і нітрогліцерину подано в розділі Енциклопедії, присвяченому хімії. Цей перелік робить зрозумілим, що проблеми включення комбінованих впливів, розбіжність поглядів при вивчені комплексних факторів, зміна масштабів цілей та оціночних стратегій мають важливе значення при розгляді результатів досліджень, тому висновки, зроблені на підставі цих епідеміологічних досліджень, залишаються не цілком визначеними.

У подібній ситуації наявні патогенетичні концепції та наукові дані можуть свідчити на користь припущенням про існуючі взаємозв'язки і тим самим сприяти з'ясуванню та обґрунтуванню наслідків, включаючи профілактичні заходи. Відомо вплив дисульфіду вуглецю на ліпідний і вуглецевий обміни, на функцію щитовидної залози (пусковий механізм гіпотиреозу) і на механізми згортання крові (сприяє агрегації тромбоцитів, інгібує активність плазміногену).

Таблиця 1.4 – Група видів діяльності і промислових галузей, які можуть бути пов’язані з професійними шкідливостями, що впливають на серцево–судинну систему

Шкідливі матеріали	Промислові галузі, схильні до дії / використовують
Дисульфід вуглецю (CS_2)	Виробництво віскози і синтетичних волокон; галузі, що виробляють гуму, сірники, вибухові речовини і целюлозу. Використовується як розчинник у фармацевтичній та косметичній промисловості, виробництві інсектицидів
Органічні нітро – сполуки	Виробництво вибухових речовин, військова промисловість, фармацевтична промисловість
ооксид вуглецю (CO)	Робітники великих промислових підприємств, що використовують горіння в технологічному процесі (доменні печі, коксові печі). Виробництво та утилізація газових сумішей, що містять CO (виробники газового обладнання). Ремонт газопроводів. Робітники ливарного виробництва, пожежники, автомеханіки (особливо працюючі в погано вентильованих приміщеннях). Нещасні випадки (гази від вибуху, пожежи в тунелях або підземні роботи)

Продовження табл.1.4

Свинець	Плавлення свинцевої руди або вторинної сировини, що містить свинець. Металургійна промисловість (виробництво різних сплавів), різання і зварювання металів, що містять свинець або матеріалів із покриттям, що містить свинець. Заводи з виробництва акумуляторів. Виробництво кераміки й порцеляни (глазурі що містить свинець). Виробництво скла що містить свинець. Виробництво барвників, використання та видалення фарб що містять свинець.
Вуглеводні, галогенні вуглеводні	розчинники (фарби, лаки); різні клеї (взуттєва, гумова промисловість); миючі та чистячі засоби; основні матеріали для хімічного синтезу; охолоджувачі; медикаменти (наркотики); вплив метилхлориду при застосуванні розчинників.

Зміни артеріального тиску, зокрема гіпертензія, найбільш часто призводять до судинних уражень нирок, при цьому до сьогодні повністю не виключено прямий причинно–наслідковий зв’язок між впливом дисульфіду вуглецю і підвищенням артеріального тиску, передбачається так само прямий (оборотний) токсичний вплив на міокард і втручання в метаболізм катехоламінів. В одному з кращих досліджень – «інтервенцій» (Nurminen і Hernberg 1985), що проводилося протягом 15–ти років, наведено документальні дані, що підтверджують оборотний характер впливу на серце: зменшення

впливу супроводжувалося майже одночасним зниженням смертності від серцево–судинних захворювань. Крім очевидного прямого кардіотоксичного ефекту, серед тих, хто зазнавав впливу дисульфіду вуглецю, було підтверджено розвиток артеріосклеротічних змін мозку, очного дна, нирок і коронарних судин, що можна розглядати як основу для виникнення енцефалопатії, аневризм судин сітківки, нефропатії та хронічної ішемічної хвороби серця. На патологічний механізм впливають етнічні чинники та особливості харчування; це було ясно подано в порівняльних дослідженнях, що проводилися серед робітників, зайнятих у виробництві хімічних віскозних волокон у Фінляндії та Японії. Так, в Японії були виявлені зміни судин сітківки, тоді як у Фінляндії переважало ураження серцево–судинної системи. Аневрізматичні зміни судин сітківки спостерігалися при концентрації дисульфіду вуглецю нижче 3 ppm (Fajen, Albright і Leffingwell 1981). Безумовно, зниження концентрації діоксиду вуглецю до 10 ppm приводить до зниження смертності від серцево–судинних захворювань. Однак поки остаточно неясно, чи може бути кардіотоксичний ефект діоксиду вуглецю однозначно виключений при його концентрації нижче 10 ppm.

Гостре отруєння органічними нітратами спричиняє розширення судин, яке супроводжується падінням артеріального тиску, збільшенням частоти серцевих скорочень, плямистою еритемою (почервоніння обличчя, шиї), ортостатичним запамороченням і головним болем. Оскільки період напіврозпаду органічних нітратів короткий, то симптоми, що виникли незабаром проходять. Зазвичай гострі отруєння серйозного значення для здоров’я не мають. Так званий синдром відміни, з латентним періодом від 36 до 72 годин, розвивається в тих випадках, коли після тривалого контакту з органічними нітратами їх вплив раптово припиняється. Його прояви варіюють від нападу стенокардії до гострого інфаркту міокарда та випадків раптової смерті. У всіх вивчених випадках смертей склеротичні зміни коронарних судин зареєстровані не були. Тому, передбачається, що причиною послужив синдром «рикошету». Коли припиняється ефект вазодилятації, спричинений нітратами,

включається механізм саморегуляції, спрямований на підвищення судинного опору, в тому числі і в коронарних артеріях, що і призводить до згаданого вище результату. У деяких епідеміологічних дослідженнях висловлюються сумніви про існування зв'язку між тривалістю й інтенсивністю дії органічних нітратів та ішемічною хворобою серця, патогенетична ймовірність цього зв'язку невелика.

Щодо свинцю, то металевий свинець у формі пилу, солей двовалентного свинцю та органічні сполуки свинцю є важливими з точки зору токсикології. Свинець впливає на механізм скорочення м'язових клітин судин і спричиняє спазм судин, що проявляється у вигляді цілого ряду симптомів, характерних для інтоксикації свинцем. Серед них нетривала гіпертензія в поєднанні зі свинцевими коліками. Тривало існуюча гіпертензія як результат хронічної свинцевої інтоксикації може пояснюватися спазмом судин, а також змінами в нирках. В епідеміологічних дослідженнях у результаті спостереження випадків більш тривалого впливу свинцю на організм був виявлений зв'язок між тривалістю цього впливу і підвищенням артеріального тиску, також збільшення кількості цереброваскулярних захворювань, тоді як серйозних доказів збільшення кількості серцево–судинних захворювань виявлено не було.

До теперішнього часу епідеміологічні дані і патогенетичні дослідження не дали ясних результатів щодо токсичності для серцево–судинної системи таких металів, як кадмій, кобальт і миш'як. Однак існує цілком достовірна гіпотеза про те, що вуглеводні, які містять галоген діють як засоби, що збуджують міокард. Пусковим механізмом спричиненої цими речовинами аритмії, яка в ряді випадків може становити загрозу для життя, ймовірно, служить чутливість міокарда до адреналіну (епінефрину), що є природним медіатором нейронів вегетативної нервової системи. Досі дискутується питання про існування прямої дії на міокард, що проявляється у зниженні скорочуваності, придушенні збудливості і провідності міокарда, а так само погіршенні рефлекторної діяльності через потрапляння цих речовин у верхні дихальні шляхи. Здатність вуглеводнів викликати сенсибілізацію організму, мабуть, залежить від ступеня галогенізації і від того, який саме галоген вони

містять, тому хлорвміщуючі вуглеводні, імовірно володіють сильнішим сенсибілізуючим ефектом, ніж фтористі сполуки. Максимальний вплив на міокард надають хлорвміщуючі вуглеводні з чотирма атомами хлору в молекулі. Незаміщені вуглеводні з коротким ланцюжком мають більшу токсичність, ніж вуглеводи з більш довгим ланцюжком. Мало відомостей про мінімальну дозу, що викликає аритмію, для кожної окремої речовини, оскільки переважна більшість повідомлень про вплив на людину описують вплив високих концентрацій (випадковий контакт або вдихання). Згідно з Reinhardt та ін. (1971), бензин, гептан, хлороформ і трихлоретилен надають особливо сильну сенсибілізуючу дію, тоді як тетрахлорид вуглецю і галотан мають менший аритмогенний ефект.

Токсичні ефекти монооксиду вуглецю розвиваються в результаті гіпоксемії тканин, що, в свою чергу, є наслідком його поєднання з гемоглобіном – CO-Hb (CO має в 200 разів більшу спорідненість до гемоглобіну, ніж кисень) і зменшення внаслідок цього вивільнення кисню в тканинах. Крім нервів, серце – ще один орган, для якого така гіпоксія є надзвичайно небезпечною. Розвинуті в результаті цього ознаки гострого ураження міокарда були неодноразово вивчені й описані з урахуванням тривалості впливу, частоти дихання, віку і перенесених раніше захворювань. У той час як у здорових спостережуваних перші ознаки впливу на серцево–судинну систему з’являлися при концентрації CO-Hb від 35 до 40 %, то у пацієнтів з ішемічною хворобою серця, в умовах експерименту, симптоми стенокардії були викликані вже при концентрації CO-Hb у межах від 2 до 5 % (Kleinman та ін. 1989; Hinderliter та ін. 1989). Інфаркти міокарда зі смертельним результатом спостерігалися серед пацієнтів з інфарктами в анамнезі при концентрації CO-Hb близько 20 % (Atkins Baker 1985).

Ефект тривалого впливу низьких концентрацій CO досі залишається предметом суперечок. У той час як експериментальні дослідження на тваринах показують ймовірність атерогенного ефекту, або за рахунок гіпоксії судинної стінки, або за рахунок прямої пошкоджуючої дії CO на судинну стінку

(підвищення проникності судинної стінки), за рахунок впливу на властивості кровотоку (посилення агрегації тромбоцитів) або на ліпідний обмін, то відповідних даних для людини недостатньо. Зростаючу смертність від серцево–судинних захворювань серед робітників тунелів (SMR 1.35, 95 % Cl 1.09 -1.68) можна швидше пояснити гострим отруєнням CO, ніж його хронічними впливом (Stern та ін. 1988). Роль CO в поєднанні з впливом куріння на серцево–судинну систему так само залишається неясною.

Біологічні фактори ризику

«Біологічний фактор ризику може бути визначений як біологічна матерія, здатна до самореплікації, і така, що може чинити шкідливу дію на інші організми, і особливо на людину» (American Industrial Hygiene Association 1986). Regina Jackel, Ulrike Tittelbach, Wolfram Dietmar Schneider.

На першому місці серед біологічних факторів ризику знаходяться бактерії, віруси, гриби та найпростіші, які можуть пошкоджувати серцево–судинну систему при безпосередньому контакті: навмисному (використання біологічних матеріалів у технологічному процесі), або ненавмисному (що не належить до технологічного процесу зараження виробничих матеріалів) . На додаток до інвазивних властивостей мікроорганізму, певну функцію можуть виконувати ендо– та мікотоксини. Вони самі по собі можуть бути безпосередньою причиною або чинником, що сприяє розвитку захворювання.

Відповідна реакція серцево–судинної системи може бути двох типів. По–перше, реакція з обмеженим залученням окремих органів і розглянута як ускладнення інфекційного захворювання – васкуліт (запалення кровоносних судин), ендокардит (запалення ендокарда, найчастіше спричинене бактеріями, хоча зустрічаються так само грибкові ендокардити і ендокардити, викликані найпростішими; гостра форма може розвиватися в результаті сепсису, підгостра форма поєднується з генералізацією інфекції); міокардити (запалення серцевого м’яза, спричинене бактеріями, вірусами або найпростішими); перикардит (запалення перикарда, зазвичай супроводжує міокардит) або панкардит

(генералізоване ураження серця з одночасним розвитком ендокардиту, міокардиту і перикардиту). І по-друге, реакція, пов’язана із залученням всієї системи в цілому до системного генералізованого патологічного процесу (сепсис, септичний або токсичний шок).

Серце може бути залучено в патологічний процес як під час, так і після фактичної інфекції. Провідними механізмами патогенезу слід вважати пряму мікробну колонізацію, токсичну або алергічну реакції. Крім того, відповідна реакція серця на інфекцію залежить від типу і вірулентності патологічного агента, ефективності імунної системи. Так, наявність інфікованих ран може призвести до розвитку міо– або ендокардиту, наприклад, стафілококової або стрептококової природи. До цього можуть бути схильні фактично всі професійні групи в разі виробничої травми.

Дев’яносто відсотків усіх простежених випадків ендокардиту можна приписати стрептококову або стафілококову інфекції, але тільки дуже невелика частка захворювань має зв’язок із посттравматичною інфекцією.

Професійні групи ризику

Відповідно до виконуваної роботи за фахом, усі працівники поділяються на певні групи за ризиком.

1. Персонал медичних і соціальних служб.

2. Фермери.

3. Робітники-пакувальники м’яса, зайняті розведенням тварин, ветеринари.

4. Виїжджаючі у бізнес-поїздки в Центральну і Південну Америку.

5. Робітники, які обслуговують каналізаційні системи та системи стічних вод, боєнь.

6. Персонал, що працює з дітьми (особливо з маленькими дітьми), у відділеннях діалізу та трансплантації.

7. Персонал, що працює з дітьми і в медичних установах.

8. Робітники лісової промисловості та садівничих господарств.

9. Робітники упукування м’яса, переробки риби, рибалки, ветеринари.

10. Виїжджаючі в ділові поїздки в ендемічні райони.

11. Співробітники медичних служб заражених районів і спеціальних лабораторій, робітники, що займаються розведенням тварин.

12. Обслуговуючий персонал систем кондиціонування повітря, зволоження, водопостачання, персонал з догляду.

13. Особи, які займаються розведенням декоративної і свійської птиці, працівники зоомагазинів.

14. Працівники програм розвитку та допомоги в тропіках і субтропіках.

15. Виїжджаючі в ділові поїздки в африканські регіони, розташовані між 20° Південної та Північної паралелі.

16. Люди, що мають професійний контакт із тваринами.

17. Співробітники програм допомоги і розвитку, персонал мікробіологічних лабораторій (особливо ті, що роблять аналіз калу).

Таблиця Д.1 (додатка) дає уявлення про можливі інфекційніх захворювання, пов’язаніх з професійною діяльністю, що вражають серцево–судинну систему.

1.3. Страховий ризик і страховий випадок

Відповідно до Закону України «Про загальнообов’язкове державне страхування від нещасних випадків на виробництві і профзахворювань, що призвели до втрати працездатності» страховий ризик – це обставини, внаслідок яких може виникнути страховий випадок.

Страховий випадок – це нещасний випадок на виробництві чи професійне захворювання, що заподіяло застрахованому працівнику професійно зумовлену фізичну або психічну травму при виконанні трудових обов’язків у результаті професійної діяльності, з настанням яких виникає право застрахованої особи на одержання матеріального забезпечення і (або) соціальних послуг.

Професійне захворювання вважається страховим випадком також при встановленні або його виявленні в період, коли потерпілий не перебуває у виробничих відносинах із підприємством, на якому він захворів.

Нещасний випадок чи професійне захворювання, що відбулися внаслідок порушення нормативних актів з охорони праці застрахованим, також є страховим випадком.

Порушення правил охорони праці застрахованим, що призвело до нещасного випадку чи професійного захворювання, не звільняє страховика від виконання зобов'язань перед потерпілим. Але в цих випадках сума страхових виплат потерпілому може бути зменшена до 50 %.

Підставою для сплати потерпілому витрат на медичну допомогу, проведення медичної, професійної і соціальної реабілітації, а також для страхових виплат є акт розслідування нещасного випадку або акт розслідування професійного захворювання (отруєння) у встановлених нормах.

Виробничі ризики

Для аналізу і профілактики травматизму важливе значення має класифікація причин та відповідно ризиків. При цьому необхідно враховувати комплекс факторів, що визначають безпечні та нешкідливі умови праці на виробництві, які обумовлюють виробничі ризики.

При встановленні причин (ризиків) нещасного випадку зазначаються і кодуються три групи причин відповідно до класифікатора.

І – технічні:

•конструктивні недоліки, недосконаліть, недостатня надійність засобів виробництва;

•конструктивні недоліки, недосконаліть, недостатня надійність транспортних засобів;

•неякісна розробка або відсутність проектної документації на будівництво, реконструкцію виробничих об'єктів, будівель, споруд, обладнання тощо;

• неякісне виконання будівельних робіт;

•недосконаліть, невідповідність вимогам безпеки технологічного процесу;

• незадовільний технічний стан:

– виробничих об’єктів, будинків, споруд, території;

– засобів виробництва;

– транспортних засобів;

•незадовільний стан виробничого середовища (несприятливі метеорологічні умови, підвищена концентрація шкідливих речовин у повітрі робочої зони; наявність шкідливих опромінень (випромінювань); незадовільна освітленість, підвищений рівень шуму і вібрації та ін.);

ІІ – організаційні (що залежать від рівня організації праці на виробництві та діяльності самої людини):

• незадовільне функціонування, недосконаліть або відсутність системи управління охороною праці;

• недоліки під час навчання безпечним прийомам праці, у тому числі:

– відсутність або неякісне проведення інструктажу;

– допуск до роботи без навчання та перевірки знань з охорони праці;

• неякісна розробка, недосконаліть інструкцій з охорони праці або їх відсутність;

• відсутність у посадових інструкціях функціональних обов’язків з питань охорони праці;

• порушення режиму праці та відпочинку;

•відсутність або неякісне проведення медичного обстеження (професійного відбору);

• невикористання засобів індивідуального захисту через незабезпеченість ними;

• виконання робіт із відключеними, несправними засобами колективного захисту, системами сигналізації, вентиляції, освітлення тощо;

• залучення до роботи працівників не за спеціальністю (професією);

• порушення технологічного процесу;

• порушення вимог безпеки під час експлуатації транспортних засобів;

• порушення правил дорожнього руху;

• незастосування засобів колективного захисту (за їх наявності);

• незастосування засобів індивідуального захисту (за їх наявності);

• порушення трудової і виробничої дисципліни, в тому числі:

– невиконання посадових обов'язків;

– невиконання вимог інструкцій з охорони праці;

III – психофізіологічні (пов'язані з несприятливою особливістю людського фактора; невідповідність анатомо–фізіологічних і психологічних особливостей організму людини умовам праці):

• алкогольне, наркотичне сп'яніння, токсикологічне отруєння;

• незадовільні фізичні дані або стан здоров'я;

• незадовільний психологічний клімат у колективі;

• травмування внаслідок протиправних дій інших осіб, інші причини.

Серед причин, не внесених до класифікатора, слід також враховувати соціальні причини, зумовлені станом людини в певний момент, якостями особи:

• недостатня ефективність норм трудового права;

• побутові умови;

• рівень доходу в родині;

• рівень освіти;

• належність до тих чи інших соціальних верств тощо.

При розгляді нещасного випадку зазначається основна причина і супутня. Як свідчать статистичні дані, психофізіологічним (людським) факторам приділяється другорядна (супутня) роль, незважаючи на те, що, як свідчить міжнародна статистика, через вину людини відбувається близько 90 % нещасних випадків. Це пояснюється недосконалістю об'єктивних методів оцінки впливу цих причин на виникнення нещасного випадку.

При з’ясуванні причин (ризиків) професійного захворювання зазначаються виробничі фактори, які призвели до захворювання:

• запиленість повітря робочої зони (концентрація пилу);

• загазованість повітря робочої зони шкідливими речовинами (концентрація речовин та їх гранично допустима концентрація);

• підвищені та знижені температури, температура поверхні устаткування, матеріалів, повітря робочої зони;

• рівень шуму, загальної та локальної вібрації;

• рівень інфразвукового коливання, ультразвуку;

• рівень електромагнітного випромінювання;

• рівень вологості та швидкості руху повітря;

• рівень іонізуючого випромінювання;

• рівень фізичного перевантаження (параметри, ступінь, важкість роботи),%;

• інші виробничі фактори за гігієнічною класифікацією праці.

Аналіз виробничого травматизму за запропонованою класифікацією дає можливість вирішувати завдання профілактики нещасних випадків і професійних захворювань у тісному взаємозв’язку з іншими завданнями управління і виробництва.

1.4. Світова інформаційна база ризиків

Аналіз інформаційної бази за ризиками База токсикологічних даних Канадського центру з професійної безпеки і здоров’я (CCOHS) [9] містить такі розділи: ідентифікація речовини, опис зовнішнього вигляду, ідентифікації небезпеки, заходи першої допомоги, протипожежні заходи, зберігання і

9. Canadian Centre for Occupational Health and Safety: Comprehensive, Practical occupational health and safety information on chemicals: [Електроний ресурс]. – 2010. – режим доступу: http://www.ccohs.ca/products/ databases/ cheminfo.html *(База токсикологических данных Канадского центра по профессиональной безопасности и здоровью (CCOHS) http://www.ccohs.ca/products/databases/cheminfo.html)*

.

поводження, контроль експозиції / персонального захисту, фізичні та хімічні властивості, стабільність і реактивність, токсикологічна інформація, екологічна інформація, видалення та зберігання відходів, транспортування, регулювання обігу та нормативи, додаткова інформація.

У Вермонтському університеті (Vermont SIRI MSDS Collection) є електронна колекція карт безпеки для близько 180 тисяч хімічних речовин[10]. А в Корнельському університеті (Cornell MSDS Search) зберігаються відомості про понад 250 тисяч хімічних речовин[11]. Посилання на пріоритетні джерела з хімії та токсикології можна знайти в хімічній та інженерній бібліотеці (Science and Engineering Library), Chemistry Data Sets[1]. Міжнародні карти хімічної безпеки є на сайті в Інтернеті[12]. Національний інститут США з професійної безпеки і здоров'я (NIOSH homepage) також володіє всією необхідною інформацією з токсичної дії інгредієнтів, що входять до складу СОТС[13]. Центр оцінки хімічних речовин та ризику RIVM Centre for Substances & Risk Assessment (Нідерланди) наводить інформацію про токсичність речовин, а також методику розрахунку ризиків для людей[14]. Інформаційна система Міністерства енергетики США (Risk Assessment Information System (RAIS)) містить відомості про фізико–хімічні властивості, фактори канцерогенного потенціалу, референтні дози і концентрації пріоритетних хімічних речовин.

10. Vermont Safety Information Resources, Inc.: Chemical toxicity data: [Електроний ресурс]. – 2011. - Режим доступу: http://hazard.com/msds/ *(Вермонтский университет (Vermont SIRI MSDS Collection). Электрона колекція карт безпеки. http://hazard.com/msds/index.html)*

11. Cornell University: Environmental Health & Safety: NYSAES: [Електроний ресурс]. – 2011. -Режим доступу: http://www.ehs.cornell.edu/NYSAES/default.cfm *(Корнелььский університет (Cornell MSDS Search). Відомості про хімічні речовини. http://MSDS.PDC.CORNELL.EDU/msdssrch.asp.)*

12. UCSD Libraries' internal business network: [Електроний ресурс]. – 2011. - Режим доступу: https://libnet.ucsd.edu/ *(Хімічна й інженерна бібліотека (Science and Engineering Library), Chemistry Data Sets. http://libnet.ucsd.edu/se/ list_bytype.html?subject=3&t=2)*

13. NIOSH: National Institute for Occupational Safety and Health: International chemical safety cards (ICSC): [Електроний ресурс]. – 2011. - Режим доступу: http://www.cdc.gov/niosh/ipcs/icstart.html *(Міжнародні карти хімічної безпеки. http://www.cdc.gov/niosh/ipcs/ipcs0000.html)*

До складу системи входить блок для розрахунку концентрацій, заснованих на ризику і які враховують множинність шляхів надходження хімічних речовин до організму людини.

Містить посилання на багато сайтів окремих штатів і нормативно–методичні документи [15]. Наведено також публікації з деяких методичних аспектів оцінки ризику[14]. Рівні мінімального ризику для гострих, підгострих і хронічних впливів рекомендовані Агентством США з реєстрації токсичних сполук і захворювань[15].

Найбільшої популярності набула Risk Assessment Information System (RAIS), інформаційна система Міністерства енергетики США, забезпечена програмою розрахунку величини ризику з урахуванням інформації, яка є в банку даних США та інших країн. Основним показником у цих технологіях є те, що всі показники ризиків мають не перевищувати ризик рівня 10^{-6} [16,17]. Аналізуючи ситуацію в Україні з базою даних і доступними методиками розрахунків ризиків, слід відзначити їх практично повну відсутність і орієнтацію на особливо небезпечні об’єкти.

14.CDC: Centers for Disease Control and Prevention: The national institute for occupational safety and health (NIOSH): Providing National and World Leadership to Prevent Workplace Illnesses and Injuries: [Електроний ресурс]. – 2010. - Режим доступу: http://www.cdc.gov/niosh/homepage.html *(Національний інститут США з професіональної безпеки і здоров’я (NIOSH). http://www.cdc.gov/niosh/homepage.html)*

15. National institute for public health and the environment (RIVM): Research for man and environment: [Електроний ресурс]. – 2010. - Режим доступу : http://www.rivm.nl/en/ *(Центр оцінки хімічних речовин і ризику RIVM Centre for Substances & Risk Assessment (Нидерланды). http://www.rivm.nl/csr/)*

16.RAIS: The Risk Assessment Information System: [Електроний ресурс]. – 2009. - Режим доступу: http://rais.ornl.gov/ *(Інформаційна система Міністерства енергетики США (Risk Assessment Information System (RAIS)) http://risk.lsd.ornl. gov/rap_hp.shtml)*

17.United States Environmental Protection Agency: region 3 risk assessment: [Електроний ресурс]. – 2011. - Режим доступу : http://www.epa.gov/ *(Методичні аспекти оцінки ризику (US EPA Region 3 Risk Assessment). http://www.epa.gov/ reg3hwmd/risk/riskmenu.htm)*

1.5. Досвід зарубіжних країн у сфері управління професійними ризиками.

Розглянемо досвід втілення систем управління ризиками у країнах Європи та світу.

Польща

Польща – одна з небагатьох країн, яка законодавчо закріпила оцінку та управління професійними ризиками. Відповідно до вимог польського законодавства, оцінка ризиків є одним з основних зобов'язань роботодавця.

Це зобов'язання було введено законодавством Польщі більше 10 років тому в процесі зближення польського законодавства з правовою системою Європейського співтовариства.

У польському трудовому законодавстві (Глава 10, ст. 226 «Профілактична охорона здоров'я») говориться про те, що роботодавець зобов'язаний оцінити і задокументувати професійні ризики, пов'язані з виконуваною роботою, вжити необхідних заходів, спрямованих на зниження ризиків, інформувати працівників про ризики, пов'язані з роботою, що виконують, а також про заходи, що вживаються з метою зниження цих ризиків.

Оцінка ризиків має відбуватися за участю працівників. Відповідно до законодавства, роботодавець повинен консультуватися з працівниками або їх представникам всіх дій, пов'язаних з їх здоров'ям і безпекою, зокрема: щодо змін в організації роботи, в технології та застосуванні хімічних речовин – якщо вони можуть привести до загрози безпеці або життю працівників; з оцінки та інформування про ризики.

Критерії, що застосовуються в оцінці професійних ризиків, містяться в різних правових актах, наприклад, у Постанові Міністра праці та соціальної політики Польщі «Щодо мінімально допустимих концентрацій і інтенсивності впливу шкідливих чинників на здоров'я працівників у робочому середовищі». Законодавчо не встановлюється регламент (правила, процедури) оцінки професійних ризиків і не визначаються деталі, що стосуються форми

документування ризиків. Тому після введення в законодавство зобов'язання проведення оцінки ризиків було здійснено ряд заходів, спрямованих на підтримку практичного застосування оцінки ризиків у компаніях, переважно в рамках урядової стратегічної програми «Охорона праці та здоров'я людини в робочому середовищі», розпочатої з ініціативи Уряду Польщі в 1995 році .

Розроблені в Польщі стандарти призначені для добровільного виконання. Стандарт PN-N18002 «Системи управління сферою здоров'я та безпеки працівників. Загальне керівництво з оцінки професійних ризиків» містить положення щодо оцінки професійних ризиків в організаціях. Цей стандарт покладений в основу концепцій інших стандартів, зокрема PN-IEC 300-3-9, BS 8800 і PN-EN 1050. Стандарт роз'яснює цілі оцінки професійних ризиків, питання організації оцінки ризиків у компанії, включаючи суб'єкти оцінювання професійних ризиків і те, як правильно оцінювати ризики. У стандарті наведено також приклади того, як робити оцінку ризиків, що виникають у зв'язку з можливим впливом на працівників хімічних речовин і шуму. Стандарт формує основу для оцінки ризиків у польських компаніях.

Слід зазначити, що допомога роботодавцям у проведенні оцінки професійних ризиків покладена і на трудову інспекцію. Діяльність трудової інспекції в сфері оцінки ризиків, зокрема, включає: забезпечення інформації про передовий досвід у галузі оцінки ризиків та управління ризиками в сфері забезпечення здоров'я та безпеки працівників; підтримку застосування систем управління здоров'ям та безпекою на робочому місці (ЗБР); здійснення перевірки виконання оцінки ризиків у компаніях.

Є програми і заходи сприяння, спрямовані на підтримку малих і середніх підприємств в оцінці ризиків. Потрібно зауважити, що правові вимоги до оцінки професійних ризиків та управління ризиками однакові як для великих, так і для малих компаній, однак ресурси малих і середніх підприємств зазвичай обмежені. Методи, що застосовуються для оцінки професійних ризиків, є схожими як у великих компаніях, так і в малих і середніх. Малі та середні підприємства можуть застосовувати спеціальні керівництва і листи

контрольних запитань для оцінки ризиків. У більшості випадків малі та середні підприємства користуються зовнішніми консалтинговими послугами з метою проведення оцінки ризиків.

Нідерланди

Оцінка ризиків (у Голландії цю процедуру називають облік / інвентаризація ризиків і аналіз ризиків) є інструментом роботодавців і працівників, який служить для ідентифікації ризиків, що існують на підприємстві. Обов'язковість проведення оцінки ризиків закріплена в законі про умови праці 1998 р., у статтях 3.1 і 5.

Відповідно до статті 3.1 Закону про умови праці, роботодавець повинен проводити політику, спрямовану на поліпшення умов праці, яка має бути «настільки ґрунтовної, наскільки це можливо». Він також має дотримуватися таких вимог: робота повинна бути організована таким чином, щоб вона не чинила ніякого негативного впливу на здоров'я та безпеку працівників; небезпеки і ризики, що загрожують здоров'ю та безпеці працівників, мають бути усунені або скорочені на ранніх стадіях; оснащення робочого місця, методи роботи, використовувані для роботи ресурси, а також зміст роботи повинні бути пристосовані до особистих якостей конкретних працівників; необхідно уникати виконання працівниками монотонної роботи і такої, що часто повторюється в короткий проміжок часу, а також роботи в контрольованому темпі, на який сам працівник не може вплинути.

Відповідно до статті 5 Закону про умови праці, політика роботодавця, спрямована на поліпшення умов праці, повинна передбачати складання «реєстру» ризиків і аналіз ризиків (оцінку ризиків), властивих тій роботі, яка виконується працівниками. Оцінка ризиків має включати також опис небезпек і заходів, спрямованих на скорочення ризиків, а також ризиків, властивих окремим категоріям працівників. Як невід'ємну частину оцінки ризиків роботодавець також зобов'язаний вести реєстр нещасних випадків, що сталися

на робочому місці і призвели до невиходу працівників на роботу з причини порушення здоров'я.

План дій, що містить заходи, спрямовані на усунення та скорочення ризиків, і розкриває їх взаємозв'язок, має бути частиною оцінки ризиків. План дій, про виконання якого складається щорічний письмовий звіт, повинен містити терміни виконання запланованих заходів. Роботодавець зобов'язаний проводити попередні консультації з щорічним звітом із радою підприємства, з представниками працівників, а за відсутності таких – з уповноваженими працівниками.

Коригування «реєстру» ризиків і результатів їх аналізу як наслідок накопиченого досвіду, зміни в методах роботи і умовах праці, навчання співробітників можуть проводитися так часто, як це необхідно.

У Голландії не існує спеціального стандарту, що встановлює, як необхідно проводити оцінку ризиків на робочому місці. Соціальні партнери самі розробили спеціальні галузеві форми, що допомагають роботодавцю проводити оцінку ризиків. Контроль за проведенням оцінки ризику здійснюється інспекцією праці. У разі виявлення трудовим інспектором порушень закону про умови праці, інспектор проводить перевірку того, чи була цим роботодавцем проведена оцінка ризиків і чи була вона перевірена.

Уряд Голландії стимулює інвестиції комерційного та некомерційного сектора в засоби, що дозволяють удосконалити сферу ЗБР. З цією метою було розроблено схему субсидування. Щороку Міністерство соціальних питань та зайнятості складає список інновацій, засобів, що дозволяють удосконалити сферу ЗБР, скорочують ступінь навантаження фізичного стресу, шуму, впливу шкідливих речовин. Роботодавці, які закуповують засоби та обладнання (машини, системи, засоби транспорту й інструменти, що застосовуються на місці роботи), які перераховані у переліку ЗБР, можуть отримати субсидію на придбання цього обладнання у розмірі до 10 % його первісної вартості, на загальну суму не більше € 25.000.

Великобританія

Великобританія, мабуть, найбільш широко представлена з точки зору різного роду рекомендацій з оцінки ризику. У законі «Про здоров'я і безпеку на роботі» від 1974 р., у главі 2 частини 3 містяться загальні обов'язки роботодавця в галузі забезпечення здоров'я та безпеки на робочому місці. Серед них:

– заходи, що дозволяють забезпечити, наскільки це можливо, безпеку та відсутність ризиків для здоров'я у зв'язку з використанням, обробкою, зберіганням і транспортуванням матеріалів і речовин;

– забезпечення інформацією та інструкціями, проведення навчання, необхідного для забезпечення здоров'я і безпеки працівників;

– підтримання на будь–якому робочому місці, що знаходиться під контролем роботодавця, умов, що забезпечують безпеку і відсутність ризиків для здоров'я, а також без ризиків для здоров'я доступ до робочого місця;

– забезпечення і підтримка прийнятного рівня безпеки робочого середовища для працівників, включаючи забезпечення адекватними засобами і заходами.

Згідно з цим законом, суб'єктами забезпечення безпечних і здорових умов праці, крім роботодавців і працівників, є Комісія з питань здоров'я та безпеки і Виконавчий орган з питань здоров'я і безпеки. При цьому Комісія з питань здоров'я та безпеки (далі – Комісія) створюється з урахуванням консультацій:

– з організаціями, що представляють роботодавців (вибір організацій – на розсуд міністра);

– з організаціями, що представляють працівників (вибір також на розсуд міністра), і

– з організаціями, що представляють місцеві влади, та іншими організаціями, включаючи професійні організації (вибір – на розсуд міністра).

До функцій Комісії належать: розробка заходів для проведення відповідних досліджень, публікація результатів досліджень, проведення навчання та інформування згідно з поставленими цілями; підготовка відповідних заходів для забезпечення надання інформації та консультативний супровід діяльності відомств, роботодавців, службовців, організацій, що представляють роботодавців і працівників та інших стейкхолдерів; звернення до органів, уповноважених на затвердження нормативних документів, з пропозиціями щодо прийняття правил, що стосуються застосування положень відповідного законодавства.

Наступний суб'єкт, який згадується в законодавстві – місцеві органи влади, які можуть бути уповноважені на здійснення ряду функцій з охорони праці.

Уповноважений орган влади має право призначити інспектора, який має відповідну кваліфікацію для здійснення перевірки з конкретного питання. Перевіряючий (або інспектор) має право здійснювати тільки ті повноваження, якими він наділений, і в рамках відповідальності яких призначив його орган влади. До конкретних повноважень інспекторів, зокрема, належать:

– право доступу в будь–який «розумний» час (або, в ситуації, яка, на його думку, є або може бути небезпечною, в будь–який час) в приміщення, яке, на його думку необхідно відвідати для досягнення цілей перевірки;

– залучення до проведення перевірки співробітника правоохоронних органів у разі, якщо є підозри, що перевірці можуть чинитися перешкоди, а також використання обладнання або матеріалів, необхідних для досягнення цілей перевірки;

– призупинення роботи в приміщенні, що перевіряється на строк, необхідний для проведення будь–яких експертиз і досліджень;

– проведення вимірювань, фотозйомки і ведення записів, необхідних для проведення експертизи або досліджень;

– забір зразків речовин, виявлених у приміщенні, що перевіряється, а також проб повітря;

– у разі виявлення обладнання або речовин, які на думку інспектора, становлять небезпеку, він має право вилучити їх зі виробничого процесу та призначити будь–який аналіз або тест (але не пошкоджувати або не руйнувати їх, якщо в цьому немає необхідності).

Канада

У Правилах промислової безпеки та здоров'я, прийнятих у Канаді в 1986р., наведено вимоги до оцінки ризиків для конкретних видів діяльності. Наприклад, у розділі «Готовність будівель, споруд, обладнання та майданчиків до аварійних ситуацій» в частині 4.13 зазначено таке:

– роботодавець повинен проводити оцінку ризику кожного робочого місця, на якому може виникнути необхідність евакуації працівника у разі аварійної ситуації;

– якщо оцінка ризику свідчить, що існує необхідність евакуації у разі аварійної ситуації, то має бути розроблена задокументована процедура, дотримання якої є обов'язком працівника.

У розділі «Робота поодинці або в ізоляції», в частині 4.20.2 наведено вимоги до виявлення небезпек, їх зниження і контролю.

У розділі «Зусилля на робочому місці» в частині 4.27 містяться вимоги до проведення оцінки ризику травми на будь–якому робочому місці, де може виникнути ризик травми в результаті докладання зусиль, пов'язаних із виконанням роботи. Оцінка ризиків у таких випадках обов'язково повинна включати розгляд попереднього досвіду роботи на цьому робочому місці, досвід роботи на подібних робочих місцях в інших підрозділах чи організаціях, а також умови, в яких ця робота буде виконуватися.

У розділі «Ергономічні вимоги» міститься опис процесу оцінки ризиків отримання м'язових травм.

Трудове законодавство Канади передбачає створення Ради зі зв'язків з промисловістю (далі – Рада), до складу якої включаються представники роботодавців і представники працівників.

Повноваження Ради, зокрема, полягають у праві викликати в суд і забезпечувати явку до суду жертв, а також добиватися від них усних або письмових свідоцтв під присягою, надання документів і речових доказів, необхідних Раді для проведення всебічного розслідування з питань, що знаходяться в юрисдикції Ради . Експерти Ради мають право відвідувати будь–яке приміщення, в якому виконувалася робота, яка є предметом слухання, а також інспектувати роботу, матеріали, обладнання або вироби і проводити опитування будь–яких осіб.

Загальним обов'язком роботодавця згідно з трудовим законодавством є гарантія того, що здоров'я і безпека кожного найнятого ним працівника на кожному робочому місці захищені, що передбачає рішення роботодавцем безлічі завдань – починаючи від розміщення текстів нормативних актів у галузі охорони праці та інших друкованих матеріалів у доступному для працівників місці і закінчуючи вимогою з установлення огорож, огороджувальних поручнів, барикадних загород і зборів згідно з чинними стандартами.

Як наступний суб'єкт, що бере участь у питаннях забезпечення здоров'я та безпеки, трудове законодавство Канади призначає комітети з політики безпеки та здоров'я. Ці комітети створюються для вирішення питань, пов'язаних із проблемами безпеки і здоров'я, що належать до роботи підприємств або бізнесу роботодавця. Кожному роботодавцю, де наймають безпосередньо триста і більше працівників, наказується створювати комітет з питань політики безпеки та здоров'я. Ця вимога є обов'язковою. За погодженням з представниками працівників, на одному підприємстві може бути створено кілька таких комітетів.

До обов'язків комітету з політики безпеки та здоров'я входить:

– участь у виробленні політики та програм у галузі безпеки і здоров'я;

– розгляд питань, що належать до забезпечення безпеки і здоров'я;

– участь у розробці та моніторингу програм щодо запобігання небезпек на робочих місцях, які (програми) передбачають навчання працівників питанням безпеки та здоров'я;

– участь у судових розглядах, розслідуваннях, перевірках та інспекціях, що належать до питань безпеки та здоров’я;

– участь у розробці та моніторингу програм, пов’язаних із наданням засобів індивідуального захисту, одягу, обладнання або матеріалів;

– проведення моніторингу даних про нещасні випадки, травми і шкідливі умови роботи;

– участь у плануванні та реалізації змін, які можуть торкнутися здоров’я та безпеки, включаючи зміни робочих процесів і методів роботи.

Далі як суб’єкт питань охорони праці фігурують комітети з питань безпеки та здоров’я на робочих місцях. Такі Комітети створюються роботодавцем для робочих місць, на яких зайнято двадцять і більше працівників. До обов’язків Комітетів з питань безпеки та здоров’я на робочих місцях належить:

– розгляд скарг та звернень працівників, що стосуються питань безпеки та здоров’я;

– участь у впровадженні та моніторингу програм щодо забезпечення безпеки і здоров’я на робочому місці;

– якщо зазначені вище програми не зачіпають специфічні для цього робочого місця небезпеки, то члени Комітету беруть участь у розробці, реалізації та моніторингу програм щодо запобігання цих небезпек, включаючи питання навчання працівників на цьому робочому місці з питань забезпечення безпечних умов праці;

– у разі відсутності Комітету з питань політики у галузі безпеки та здоров’я брати участь у розробці, реалізації та моніторингу програм щодо запобігання небезпек на робочих місцях;

– брати участь у судових розглядах, розслідуваннях, перевірках та інспекціях, що стосуються безпеки та здоров’я працівників, включаючи одержання консультацій від осіб, достатньо технічно або професійно кваліфікованих;

– брати участь у реалізації та моніторингу програм, пов’язаних із забезпеченням працівників засобами індивідуального захисту, спеціального одягу, обладнання та матеріалів і, у разі відсутності в організації Комітету з розробки політики, брати участь у розробці таких програм;

– контролювати і забезпечувати ведення записів про нещасні випадки, травмування і небезпечні чи шкідливі для здоров’я працівників фактори, а також проводити періодичний моніторинг даних, що належать до цих нещасних випадків, травм або небезпек;

– здійснювати взаємодію з інспекторами з безпеки і здоров’я;

– брати участь у проведенні змін, які можуть торкнутися здоров’я і безпеки працівників, включаючи робочі процеси, і, в разі їх відсутності, брати участь у плануванні та впровадженні таких змін;

– сприяти роботодавцю у виявленні та оцінці впливу на працівника шкідливих виробничих факторів;

– щомісяця проводити перевірку всіх або частини робочих місць так, щоб кожне робоче місце було перевірено щонайменше один раз на рік.

Японія

У 1972 р. в Японії був прийнятий закон про промислову безпеку і здоров’я, який був покликаний гарантувати здоров’я і безпеку працівників на робочих місцях, а також стимулювати створення комфортних умов праці за рахунок прийняття всебічних і систематичних заходів щодо запобігання виробничого травматизму. До таких заходів закон, зокрема, відносить розробку стандартів щодо запобігання різного роду небезпек, роз’яснення відповідальності за забезпечення безпеки та здоров’я на робочих місця, а також ініціативні добровільні заходи, що розробляються і реалізуються з метою запобігання нещасних випадків на виробництві.

Основні заходи щодо запобігання виробничого травматизму викладаються у Плані запобігання виробничого травматизму, який затверджується Міністерством охорони здоров’я, праці та соціального

забезпечення після отримання пропозицій від Комітету з питань трудової політики.

Відповідно до нормативних актів, кожен роботодавець зобов'язаний призначити залежно від виду діяльності та розміру організації керівника з питань безпеки та здоров'я для кожного робочого місця, фахівця з техніки безпеки для кожного робочого місця, санітарного інспектора (працівника, відповідального за питання безпеки та здоров'я, або тільки за питання здоров'я), виробничого терапевта з медичних працівників, який відповідатиме за надання медичної допомоги працівникам, спеціаліста з технічного обслуговування, працівника, який здійснює загальний контроль питань безпеки та здоров'я, головного контролера з питань безпеки та здоров'я, контролера ділянки з питань безпеки і здоров'я, або контролера з питань безпеки та здоров'я.

Роботодавець зобов'язаний проводити вимірювання умов праці у разі використання небезпечних видів робіт, а також вести необхідний облік результатів проведення вимірювань. На Міністерство охорони здоров'я, праці та соціального забезпечення покладаються обов'язки щодо видання керівних вказівок з проведення таких вимірювань.

На додаток до закону про промислову безпеку та здоров'я в 1975 р. був прийнятий Закон «Про оцінку умов праці», в якому прописані вимоги до кваліфікації експертів, необхідної для проведення відповідних вимірювань, і вимоги до організацій, що виробляють такі виміри з метою підтримки здоров'я працівника на робочому місці .

Служба з проведення вимірювань умов праці визначається законом як особа або організація, зареєстрована Міністерством охорони здоров'я, праці та соціального забезпечення або Генеральним директором Бюро праці префектури. Ця служба надає послуги з проведення вимірювань умов праці за запитом споживачів у порядку, затвердженому Міністерством охорони здоров'я, праці та соціального забезпечення.

Запитання для самоконтролю

1. Чи актуальна проблема травмування людей на виробництві? Рівень ризику на виробництві в Україні та у світі.

2. Банки даних про помилки людини. Призначення.

3. Що слід розуміти як ризик?

4. З чого складається механізм управління ризиком?

5. Якими показниками вимірюється ризик?

6. Види небезпек, що формують ризик людини.

7. Як визначається якісна оцінка рівня ризику?

8. Як визначити рівень ризику, яким можна знехтувати? Допустимий ризик.

9. З чого складається оцінка екологічного ризику?

10. Як пов’язані господарський ризик та ризик травмування робітника?

11. Чи можна віднести ризик гри у лотереї до страхових ризиків? Класифікація страхових ризиків.

12. Як математика пов’язана із ризиками? Актуарна математика.

13. Як види діяльності людини впливають на ризик травмування або іншого ушкодження здоров’я? Види небезпечної (ризикової) діяльності людини.

14. Який ризик показує масштабність подій та наслідків на виробництві? Соціальний ризик.

15. Види соціальних ризиків у суспільстві. Як вони впливають на ризики на виробництві?

16. Які небезпеки та їх фактори ви знаєте? Наведіть класифікацію небезпек та їх факторів.

17. Чи належать студенти та викладачі до професійних груп ризиків?

18. Який документ роз’яснює втілення у життя страхового ризику? Закон України «Про загальнообов’язкове державне страхування від нещасних випадків на виробництві і профзахворювань, що призвели до втрати працездатності».

19. Що ви знаєте про інформаційні бази ризиків у світі? Інформаційна система Міністерства енергетики США (Risk Assessment Information System (RAIS)).

Тема 2. МЕТОДИКА ВИЗНАЧЕННЯ РИЗИКІВ ТА ЇХ ПРИЙНЯТНИХ РІВНІВ ДЛЯ ДЕКЛАРУВАННЯ БЕЗПЕКИ ОБ'ЄКТІВ ПІДВИЩЕНОЇ НЕБЕЗПЕКИ

2.1. Методика визначення ризиків Міністерства праці та соціальної політики України 04.12.2002 № 637.

2.2. Об'єкти підвищеної небезпеки.

2.1. Методика визначення ризиків Міністерства праці та соціальної політики України 04.12.2002 № 637

Галузь застосування

Методика визначає порядок проведення аналізу небезпеки та оцінки ризику об'єктів підвищеної небезпеки, установлює методичні принципи, терміни і поняття аналізу ризику, визначає критерії прийнятних ризиків та їх рівні.

Методика призначена:

- для розробки декларації безпеки об'єктів підвищеної небезпеки;
- для прийняття рішень щодо розташування та експлуатації об'єктів підвищеної небезпеки;
- для розробки заходів щодо запобігання аварій та підготовки до реагування на них;

– для визначення обсягу відповідальності та страхових тарифів при страхуванні цивільної відповідальності суб’єктів господарської діяльності за шкоду, що може бути заподіяна аваріями на об’єктах підвищеної небезпеки відповідно до вимог Закону України «Про об’єкти підвищеної небезпеки» та Закону України «Про страхування».

Аналіз небезпеки й оцінка ризику виконується в повному обсязі, передбаченому цією Методикою, для об’єктів підвищеної небезпеки першого класу. Для об’єктів підвищеної небезпеки другого класу визначаються тільки масштаби небезпеки відповідно до вимог цієї Методики.

Методика може застосовуватися також для оцінки рівня ризику й експертизи рішень з безпеки потенційно небезпечних об’єктів, у тому числі під час:

– розробки нових технологій та конструювання обладнання;

– проектування та розташування нових виробництв;

– реконструкції діючих виробництв;

– експертизи діючих виробництв і тих, що реконструюються та проектуються;

– розробки планів локалізації та ліквідації аварій;

– організації страхового захисту майна підприємств;

– розгляду конфліктів між суб’єктом господарської діяльності, що експлуатує чи планує експлуатацію потенційно небезпечного об’єкта, та будь–якими зацікавленими сторонами, для яких аварії на об’єктах підвищеної небезпеки можуть мати негативні наслідки.

Методика призначена для фахівців у галузі промислової безпеки та охорони праці, керівників і фахівців підприємств, а також для фахівців органів виконавчої влади, що регулюють відносини в сфері діяльності об’єктів підвищеної небезпеки, відповідно до вимог Закону України «Про об’єкти підвищеної небезпеки». Методика є основою для розробки відомчих або галузевих керівних документів з проведення аналізу ризику об’єктів

підвищеної небезпеки відповідно до їх специфіки.

Результати аналізу ризику наводяться у декларації безпеки згідно з вимогами Порядку декларування безпеки об'єктів підвищеної небезпеки.

Терміни та визначення

У Методиці застосовуються такі терміни та їх визначення.

Аналіз ризику аварії – процес виявлення небезпек і оцінки ризику аварії на об'єктах підвищеної небезпеки для людей, їх майна та довкілля.

Громадськість – одна або декілька фізичних чи юридичних осіб.

Небезпека аварії – загроза, можливість заподіяння збитків людині, майну і (чи) довкіллю внаслідок аварії на об'єкті підвищеної небезпеки.

Об'єкт «турботи» – реципієнти, негативний вплив аварій на які створює небезпеку для життєдіяльності населення та для довкілля і торакється інтересів громадськості.

Оцінка ризику аварії – процес визначення ймовірності та вагомості наслідків реалізації небезпек аварій для здоров'я людини, майна і довкілля.

Прийнятний ризик – ризик, який не перевищує на території об'єкта підвищеної небезпеки і за його межами гранично допустимого рівня.

Ризик – ступінь імовірності певної негативної події, яка може відбутися в певний час або за певних обставин на території об'єкта підвищеної небезпеки та/або за його межами.

Основними кількісними показниками ризику аварії є:

- *індивідуальний ризик* – імовірність загибелі людини, що знаходиться в цьому регіоні, від можливих джерел небезпеки об'єкта підвищеної небезпеки протягом року з урахуванням імовірності її перебування в зоні ураження;
- *територіальний ризик* – імовірність загибелі протягом року людини, яка знаходиться в конкретному місці простору, від можливих джерел небезпеки об'єкта підвищеної небезпеки;
- *соціальний ризик* – імовірність загибелі людей понад певну кількість (або очікувана кількість загиблих) у цьому регіоні протягом року від можливих

джерел небезпеки об’єкта підвищеної небезпеки, з урахуванням імовірності їх перебування в зоні ураження.

Збитки від аварії – втрати (збитки) у виробничій і невиробничій сфері життєдіяльності людини, шкода довкіллю, заподіяні в результаті аварії на об’єкті підвищеної небезпеки що обчислюються в грошовому еквіваленті.

Крім термінів, наведених вище, вживаються терміни в значенні, що надається у таких законодавчих і нормативних актах:

– Закон України «Про об’єкти підвищеної небезпеки»;

– ДСТУ 2156–93. Безпека промислових підприємств. Терміни і визначення;

– ДСТУ 2960–94. Організація промислового виробництва. Основні поняття. Терміни і визначення.

Порядок здійснення аналізу небезпеки й оцінки ризику

Аналіз небезпеки та ризику аварій на об’єкті підвищеної небезпеки включає такі основні етапи:

– постановку завдання аналізу небезпеки та оцінки ризику;

– аналіз небезпеки та умов виникнення аварій;

– оцінку ризику (ймовірності) виникнення аварій;

– аналіз умов і оцінку ймовірності розвитку аварій;

– визначення масштабів наслідків;

– оцінку ймовірності наслідків аварій;

– оцінку прийнятності ризику та прийняття рішень щодо зменшення ризику.

Постановка завдання містить у собі такі основні етапи:

– визначення мети і завдань дослідження ризику;

– виділення об’єктів, для яких необхідно, виходячи з цілей і завдань дослідження, виконати аналіз небезпеки та ризику;

– визначення реципієнтів і виділення з них об’єктів «турботи» суспільства.

Завданнями дослідження ризику є:

– встановлення рівня ризику, що зумовлений експлуатацією об’єкта підвищеної небезпеки;

– управління ризиком шляхом зіставлення рівня ризику з прийнятним та вибір рішень щодо його зниження.

Для виділення об’єктів, для яких необхідно при виконанні дослідження ризику з метою розробки декларації виконати аналіз небезпеки та ризику, потрібно:

– визначити ті апарати чи установки, на яких можливі аварії з найбільшим викидом небезпечних речовин;

– визначити ті з них, на яких аварії з ураженням та завданням збитків можливі за межами підприємства;

– установити зони максимального ураження, вид і масштаб можливих наслідків негативних впливів;

– визначення реципієнтів, що потрапляють у зону ураження, та установити об’єкти «турботи».

Основним об’єктом «турботи» є людина. Необхідно визначити загрозу для людини, для чого виділити місця проживання, підприємства й організації, що потрапляють у зону ураження.

З урахуванням особливостей небезпечних речовин, що застосовуються на об’єкті підвищеної небезпеки, апаратурного та технологічного оформлення об’єкта підвищеної небезпеки, географічного розташування, рельєфу і кліматичних умов місцевості тощо, місцеві ради можуть встановлювати прийнятний ризик для інших об’єктів «турботи» (крім людини).

Як інші об’єкти «турботи» необхідно розглядати:

- соціально важливі об’єкти;
- елементи екосистеми;
- майно юридичних і фізичних осіб.

Як соціально важливі об’єкти слід розглядати:

- місця великого скупчення людей (стадіони, кінотеатри, лікарні тощо);
- природоохоронні об’єкти (заповідники, парки тощо);
- зони відпочинку (рекреаційні зони);
- об’єкти культури (музеї, палаци, пам’ятники архітектури тощо);
- об’єкти життєзабезпечення (станції водопідготовки, об’єкти енергопостачання, об’єкти комунального господарства, транспортні магістралі тощо);
- місця розташування органів місцевого самоврядування, державної адміністрації й інших органів управління життєдіяльністю.

Як елементи екосистеми, де можливий негативний вплив аварій, слід розглядати:

- флору і фауну;
- атмосферу;
- водне середовище (ріки, водойми, морська акваторія);
- землю, включаючи ґрунтові води;
- інші об’єкти впливу.

Як майно юридичних і фізичних осіб можуть розглядатися:

– житлові та господарські будівлі;
– транспортні засоби;
– дачні та садові ділянки;
– будівлі, споруди та устаткування підприємств;
– майно промислових підприємств, організацій та установ;
– орні землі, свійські тварини й інші сільськогосподарські об’єкти;
– сировина та продукти виробництва, у тому числі посіви та врожай;
– інше рухоме та нерухоме майно.

Крім цього, необхідно виділити інші об’єкти «турботи», що потрапляють у зону небезпечного впливу аварії.

Для кожного об’єкта аналізу оцінюється можливість впливу зовнішніх сил, виходячи з особливостей місця його розташування.

Зовнішні впливи та їх імовірність не залежать від умов експлуатації об’єкта підвищеної небезпеки. Тому визначається достатність заходів для забезпечення стійкості об’єкта до зовнішніх впливів і зменшення наслідків. Кількісна оцінка ризику при цьому не виконується.

Складається перелік можливих зовнішніх впливів.

Аналіз небезпеки та умов виникнення аварій виконується тільки для тих небезпек, що пов’язані з порушенням умов безпечної експлуатації об’єкта.

У кожному об’єкті підвищеної небезпеки аналізуються технологічне середовище і наявність у ньому небезпечних речовин, їх фізико–хімічні, хімічні, теплофізичні та інші властивості, наведені в науково–технічній, довідковій і нормативно–технічній літературі, що свідчать про їх небезпеку. При цьому розглядається не тільки можливість прояву небезпечних властивостей при виході речовин за межі апаратури та контакті з атмосферою, але й можливість небезпечних процесів в апаратах і трубопроводах, у тому числі можливість перебігу некерованих реакцій.

В усіх випадках виділяються речовини з небезпечними властивостями відповідно до категорій небезпечних речовин, встановлених «Нормативами порогових мас небезпечних речовин для ідентифікації об’єктів підвищеної небезпеки».

Визначаються режими та відхилення в технологічній системі, що є причиною виникнення умов, за яких можлива реалізація небезпечних властивостей речовин.

На підставі аналізу можливих відхилень виявляються небезпечні події, що призводять до виникнення та розвитку аварій (події, що ініціюють виникнення аварій). Складається перелік подій, що ініціюють виникнення аварії.

Для аналізу експлуатаційної небезпеки можуть використовуватися такі методи аналізу:

- «що буде, якщо»?;
- «перевірочний лист»;

– аналіз експлуатаційної небезпеки (HAZOP–аналіз);

– інші наведені в науково–технічній і нормативній літературі методи.

Для оцінки ризику (імовірності) виникнення аварій для кожної ініціюючої аварію події на потенційному джерелі аварії виконується оцінка імовірності її реалізації протягом одного року. Під час розгляду можливих відхилень параметрів процесу можуть використовуватися:

– дерево «відмов»;

– аналіз видів і наслідків відмов;

– обробка статистичних даних про аварійність технологічної системи, що відповідають специфіці об'єктів підвищеної небезпеки чи виду діяльності;

– експертні оцінки імовірності виникнення події, що розглядається, виконані за певною методикою;

– інші обґрунтовані методи оцінки.

Під час розгляду причин відхилень розглядаються відмови устаткування, арматури, поломки, можливі технологічні причини, обумовлені порушенням режимів роботи функціонально пов'язаних систем, а також помилки персоналу.

Якщо імовірність виникнення аварії є неприйнятною величиною, то відшуковуються рішення щодо її зниження.

Наступним етапом оцінки ризику є аналіз умов і оцінка імовірності та розвитку аварій.

У разі реалізації хоча б однієї із розглянутих ініціюючих аварію подій запобігти їй за допомогою контролю і регулювання параметрів технологічного процесу стає неможливим. Розвиток небезпечних неконтрольованих процесів може призвести до всіляких напрямів розвитку аварій з різними масштабами ураження і наслідками, залежно від того, які засоби стримування аварії (протиаварійного захисту та локалізації аварії) застосовуються, та від результатів їх реалізації.

На цьому етапі аналізу ризику на основі оцінки ймовірності спрацьовування і відмови засобів стримування аварії та помилок персоналу

визначається ймовірність різноманітних наслідків аварії. Для цього можна використовувати:

– дерево подій;

– аналіз видів і наслідків відмов;

– експертні оцінки імовірності виникнення події, що розглядається, виконані за певною методикою;

– інші обґрунтовані методи оцінки.

Для кожного результату визначаються можливі умови реалізації (параметри витікання чи інші умови викиду, час витікання чи викиду, маса викиду, площа протоки, погодні умови та ін.), за яких моделюються аварії та визначаються значення вражаючих факторів, зони їх дії та можливі наслідки у фізичному вираженні.

Визначення масштабів наслідків аварій включає аналіз можливих впливів на людей, майно і довкілля. Для оцінки можливих наслідків і наступної оцінки ризику необхідно моделювати аварії для кожного можливого її результату, визначеного при виконанні аналізу розвитку аварій.

Під час моделювання вибухів рекомендується розглядати:

– вибухи при руйнуванні оболонки чи апаратів трубопроводів у результаті підвищення тиску в устаткуванні внаслідок неконтрольованих фізичних чи хімічних процесів;

– вибухи при руйнуванні оболонки і скипанні зріджених газів, що знаходяться в апаратах під тиском, чи перегрітих рідин;

– вибухи конденсованих речовин в устаткуванні, в атмосфері при викидах;

– об’ємні вибухи газових і парових хмар при викидах стиснутих чи зріджених газів перегрітих рідин;

– інші вибухові явища, можливі на розглянутому об’єкті в разі виникнення аварійних ситуацій.

При моделюванні пожеж рекомендується розглядати:

– горіння вільних і обмежених розливів горючих і легкозаймистих рідин;

– дифузійне чи дефлаграційне згоряння незмішаних хмар при викидах зріджених газів під тиском і перегрітих рідин («вогняна куля»);

– факельне горіння струменя пари, газу або диспергованої рідини;

– інші види пожежі, можливі на розглянутому об’єкті в разі виникнення аварійних ситуацій.

При моделюванні викидів шкідливих і токсичних речовин в атмосферу враховуються погодні умови, стан атмосфери, напрямок і швидкість вітру, умови викиду й інші параметри.

У процесі аналізу виявляються інші небезпечні фізичні та хімічні процеси, що можуть реалізуватися при виникненні і розвитку аварії, та оцінюється їх негативний вплив на населення, соціально важливі об’єкти, елементи екосистеми, майно юридичних і фізичних осіб та інші об’єкти «турботи» суспільства.

Якщо на підприємстві є декілька об’єктів підвищеної небезпеки і на кожному об’єкті підвищеної небезпеки є декілька джерел (апаратів), на яких можливі аварії з виходом за межі території цього підприємства, повинні бути оцінені наслідки всіх можливих видів аварій на цих джерелах.

Для оцінки рівня ризику наслідків аварії необхідно визначати для виявлених у процесі аналізу напрямів і для кожного етапу її розвитку, чи може вона на цьому етапі бути локалізована і ліквідована.

Вплив вражаючих факторів на об’єкт «турботи» не означає неминучого настання негативних наслідків. На кожному етапі розвитку аварії має бути оцінена ймовірність наслідків. Виконується оцінка ризику наслідків тільки для тих об’єктів «турботи» (населення, соціально важливі об’єкти, елементи екосистеми, майно юридичних і фізичних осіб), на які за результатами розрахунків вражаючих факторів можливий негативний вплив.

Для оцінки територіального ризику за отриманим при моделюванні аварії значенням вражаючого фактора в певній точці простору визначається умовна

ймовірність летального результату для людини у випадку її перебування в цій точці. Якщо відома ймовірність появи людини в певній точці простору, то визначається індивідуальний ризик загибелі в цій точці людини, що проживає в розглянутому регіоні.

Підсумовуючи індивідуальні ризики по всій території розглянутого регіону, визначається індивідуальний ризик проживання в ньому, обумовлений можливими аваріями на об’єкті підвищеної небезпеки.

За значенням територіального ризику у виділеному регіоні та щільності населення в ньому визначається очікувана чисельність загиблих протягом одного року в розглянутому регіоні, чи ймовірність загибелі в регіоні протягом одного року більше певної кількості людей, обумовлені можливими аваріями на об’єкті підвищеної небезпеки.

Для інших об’єктів «турботи» здійснюється оцінка ризику, якщо для них місцевими органами виконавчої влади відповідно до вимог цієї Методики встановлені прийнятні ризики. Для обраного об’єкта «турботи» визначається сумарний ризик небажаних наслідків від впливу будь-яких вражаючих факторів аварій з різними наслідками всіх виділених джерел аварії.

У разі потреби розглядаються рішення щодо зниження оцінених ризиків до прийнятного рівня. Для визначення рівня ризику на всіх етапах його аналізу допускається застосування будь–яких відомих у науково–технічній, довідковій, нормативній і методичній літературі методів розрахунку й оцінок небезпек, наслідків і ризику для об’єктів «турботи» за умови наявності обґрунтування їх застосування відповідно до вимог цієї Методики.

Всі припущення під час оцінки масштабів аварії у випадку виникнення невизначеностей у процесі оцінки ризику повинні орієнтуватися на найгірші наслідки:

– якщо виникає невизначеність у можливих значеннях параметрів процесу, то для визначення умов виникнення аварій приймаються найгірші з можливих;

– якщо виникає невизначеність у можливих значеннях мас викиду небезпечних речовин, то в розрахунках приймається найбільша маса з можливих;

– щодо ймовірності погодних і кліматичних умов, то для оцінок ризику повинні вибиратися найбільш несприятливі;

– в разі здійснення статистичних оцінок вибирається найнесприятливіше відхилення від середньостатистичного значення при надійній імовірності, що дорівнює і більше 0,95;

– якщо є інші невизначеності, то приймаються інші найгірші припущення, за яких можливі найгірші наслідки з найбільшою ймовірністю.

Рекомендується для моделювання аварій, аналізу небезпеки й оцінки ризику застосовувати комп'ютерні програми та програмні засоби. Методи розрахунку й оцінок небезпек, наслідків і ризику, що застосовуються в комп'ютерних програмах і програмних засобах, мають бути обґрунтовані відповідно до вимог цієї Методики.

Один із методів, який рекомендується для застосування на підприємствах України, наведений у Настанові з дослідження небезпеки та кількісної оцінки ризику техногенних аварій.

Пріоритетними у використанні є методичні матеріали, погоджені чи затверджені Держгірпромнаглядохоронпраці, МНС, МОЗ, УПБМВС, Мінекоресурсів, Держбудом та іншими органами виконавчої влади.

Визначення прийнятного ризику

Прийнятний ризик для об'єктів «турботи», що визначені в процесі постановки завдання дослідження ризику, повинен встановлюватися місцевими органами виконавчої влади з урахуванням:

– чинних нормативних актів;

– угод між суб'єктом господарської діяльності, що є власником об'єкта підвищеної небезпеки, та зацікавленими сторонами;

– економічних і соціальних умов регіону;

– експертних оцінок;

– досвіду інших регіонів;

– інших обставин.

Для об’єкта підвищеної небезпеки прийнятний ризик встановлюється з урахуванням створюваного ним масштабу небезпеки та розташування в регіоні інших підприємств, що мають об’єкти підвищеної небезпеки, за умови, що сумарний ризик виникнення небажаних наслідків не перевищує встановленого цією Методикою.

Встановлюється значення, вище якого ризик вважається абсолютно неприйнятним (верхній рівень), і значення, нижче якого ризик вважається абсолютно прийнятним (нижній рівень).

Якщо місцевими радами не встановлений прийнятний ризик для визначених об’єктів «турботи», то для складання декларації безпеки об’єктів підвищеної небезпеки застосовуються рівні, наведені у цій Методиці.

Для життя людини рекомендується вважати неприйнятним:

$R_t > 10^{-5}$ – для територіального ризику за межами санітарно–захисної зони підприємства, що має у своєму складі хоча б один об’єкт підвищеної небезпеки,

$R_i > 10^{-6}$ – для індивідуального ризику – для людини, яка знаходиться в конкретному регіоні за межами санітарно-захисної зони підприємства, яке має у своєму складі хоча б один об’єкт підвищеної небезпеки (місті, селищі, селі, на території промислової зони підприємств і організацій тощо).

$R_s > 10^{-5}$ – для соціального ризику загибелі понад 10 чоловік протягом одного року у виділеному регіоні за межами санітарно–захисної зони підприємства, яке має у своєму складі хоча б один об’єкт підвищеної небезпеки (місті, селищі, селі, на території підприємств і організацій).

Як критерій соціального ризику може використовуватися також очікувана кількість загиблих у виділеному регіоні за межами санітарно–захисної зони підприємства (місті, селищі, селі, на території підприємств і організацій, що знаходяться у промисловій зоні тощо) на 1000 жителів $\dot{M}_D > 10^{-3}$.

В усіх випадках ризик аварій на об’єкті підвищеної небезпеки для населення рекомендується вважати абсолютно прийнятним при рівнях:

– територіального ризику $R_t \leq 10^{-7}$;

– індивідуального ризику $R_i \leq 10^{-8}$;

– соціального ризику $R_s \leq 10^{-7}$ чи $\dot{M}_D \leq 10^{-5}$.

Місцеві органи виконавчої влади з урахуванням особливостей регіону можуть встановлювати інші значення верхнього та нижнього рівнів ризику. Значення верхнього рівня кожного з перерахованих вище критеріїв прийнятного ризику можуть встановлюватися в 100 разів нижчими від їх аналогів, які пов’язані з небезпекою повсякденного життя та ризиком проживання в регіоні (дорожньо–транспортні пригоди, нещасні випадки в побуті, пожежі, вибухи газу тощо).

В усіх випадках прийнятний ризик, що встановлюється органами виконавчої влади у регіонах, не повинен перевищувати рівнів, установлених цією Методикою.

Для прийняття рішень щодо дозволів на експлуатацію, будівництво чи реконструкцію об’єктів підвищеної небезпеки, може використовуватися кожний з перерахованих вище критеріїв прийнятного ризику (територіальний, індивідуальний чи соціальний) або їх сукупність, залежно від специфіки об’єкта.

Для інших об’єктів «турботи» ризиками можуть бути:

- для соціально важливих об’єктів – імовірність аварій на об’єкті підвищеної небезпеки протягом одного року, які можуть призвести до припинення їх функціонування на термін, що перевищує встановлений нормами термін припинення їх життєдіяльності або вказаний у наступному пункті;
- для майна юридичних і фізичних осіб – імовірність аварії на об’єкті підвищеної небезпеки протягом одного року, яка призвела до ушкодження або

знищення майна фізичних чи юридичних осіб у розмірах, що перевищують вказані у наступному пункті;

- для елементів екосистеми – ймовірність аварії на об’єкті підвищеної небезпеки протягом одного року з еколого–економічними збитками, внаслідок негативного впливу аварії на флору, фауну, довкілля, у розмірах, що перевищують вказані у наступному пункті або встановлені місцевими органами виконавчої влади.

Для кожного визначеного об’єкта «турботи» чи групи об’єктів «турботи», для яких установлюється прийнятний ризик, небажані негативні наслідки, що є предметом угоди для встановлення рівня прийнятного ризику, можуть конкретизуватися.

Розглядаються такі негативні наслідки:

– евакуація або обмеження вільного пересування людей на період понад 2 години, в разі якщо кількість людей, помножена на кількість годин, більше 500;

– припинення постачання питної води, електроенергії, газу, телефонного зв’язку понад 2 години, якщо кількість людей, помножена на кількість годин, більше 1 000;

– постійні чи тимчасові збитки ґрунту площею понад 5 га, включаючи сільськогосподарські угіддя;

– значні чи довгострокові збитки прісноводним або морським середовищам існування, у тому числі понад 10 км річки чи каналу; понад 1 га озера чи ставка, понад 2 га берегової лінії відкритого моря;

– значні чи довгострокові збитки водному об’єкту, підземним водам площею понад 1 га;

– завдання збитків житлу за межами підприємства та приведення його до непридатного стану;

– збитки майну за межами підприємства, інші збитки об’єктам «турботи» на суму понад 2 500 000 гривень, або на суму, що встановлена угодою зацікавлених сторін.

Верхній та нижній рівні прийнятного ризику небажаних наслідків для об’єктів «турботи», що зазначені вище, внаслідок аварії на об’єктах підвищеної небезпеки повинні встановлюватися з урахуванням ризику настання аналогічних подій поблизу об’єкта підвищеної небезпеки з причин, що не пов’язані з аваріями. Їх рівень рекомендується встановлювати в 100 разів нижчим.

Оцінка прийнятності ризику та прийняття рішень щодо зменшення ризику

Прийняття рішень за результатами аналізу небезпеки й оцінки ризику ґрунтується на таких принципах:

– ризик, пов’язаний з наявною на об’єкті підвищеної небезпеки та виявленою потенційною небезпекою для виділених об’єктів «турботи», має бути прийнятним;

– будь–яка діяльність, яка створює ризик, що перевищує прийнятний, є неприпустимою, незалежно від вигоди, яку вона приносить;

– витрати на досягнення та підтримку прийнятного ризику мають бути мінімальними.

На підставі результатів аналізу небезпеки та ризику визначається сумарний рівень ризику кожного об’єкта «турботи», що потрапляє в зону можливого ураження:

– населення у виділених місцях проживання, персоналу, що знаходяться в промисловій зоні підприємств і організацій;

– соціально важливих об’єктів;

– елементів екосистеми;

– майна юридичних і фізичних осіб.

Експлуатація об’єкта підвищеної небезпеки неприпустима, якщо ризик небажаних наслідків для одного з об’єктів «турботи» вищий від встановленого прийнятного ризику.

Будівництво, реконструкція та експлуатація об’єкта підвищеної небезпеки вважається неприпустимою, якщо ризик, визначений відповідно до вимог цієї Методики, перевищує верхній рівень прийнятного ризику.

Якщо ризик, визначений відповідно до вимог цієї Методики, менший від нижнього рівня, то об’єкт підвищеної небезпеки вважається достатньо безпечним, і вимоги щодо зниження ризику зацікавленими особами при прийнятті рішень про його будівництво, реконструкцію чи експлуатацію вважаються необґрунтованими.

У випадках, коли ризик, визначений відповідно до вимог цієї Методики, знаходиться між верхнім і нижнім рівнями, зацікавлені сторони можуть зажадати прийняття додаткових рішень щодо зниження рівня ризику. Рішення про його прийнятність приймається місцевими радами на основі порівняння витрат на зниження ризику порівняно з вигодою, що одержують суб’єкти господарської діяльності та суспільство.

Встановлені згідно з вимогами цієї Методики верхній і нижній рівні прийнятного ризику для об’єктів «турботи» можуть уточнюватися місцевими органами виконавчої влади з урахуванням результатів аналізу небезпеки та ризику, що отримані в процесі розробки та складання декларації безпеки. Розгляд і прийняття рішень, що забезпечують прийнятність ризику, доцільно проводити на всіх етапах аналізу небезпеки та ризику.

Ризик від негативних подій для визначених об’єктів від аварій на об’єкті підвищеної небезпеки, що не перевищує прийнятний, має бути застрахований відповідно до Законів України «Про об’єкти підвищеної небезпеки» та «Про страхування».

Заходи щодо зменшення ризику можуть мати технічний і/або організаційний характер. При виборі конкретних заходів вирішальне значення має загальна оцінка дієвості та надійності заходів, що впливають на ризик, а

також розмір витрат на їх реалізацію.

Вибір запланованих до впровадження заходів безпеки має такі пріоритети:

– заходи щодо зменшення імовірності виникнення аварії;

– заходи щодо зменшення імовірності розвитку аварії;

– заходи щодо зменшення тяжкості наслідків аварії.

Для визначення пріоритетності виконання заходів з метою зменшення ризику в умовах заданих витрат чи обмеженості ресурсів необхідно:

– визначити сукупність заходів, що можуть бути реалізовані при заданих обсягах фінансування;

– ранжирувати ці заходи за показником «ефективність–витрати»;

– обґрунтувати й оцінити ефективність пропонованих заходів.

Вимоги до обґрунтування методів аналізу небезпеки й оцінки ризику

За результатами аналізу небезпеки та ризику для об’єктів підвищеної небезпеки першого класу відповідно до вимог «Порядку декларування безпеки об’єктів підвищеної небезпеки» складається розрахунково–пояснювальна частина Декларації безпеки об’єктів підвищеної небезпеки, в якій має бути обґрунтовано початкові дані, методи аналізу, розрахунки й оцінки, що застосовуються.

Мають бути наведені початкові дані та посилання на джерела, в яких вони містяться.

Вказується технічна документація, в якій міститься інформація про об’єкт аналізу, що використана для оцінки ризику (пояснювальна записка до технічного проекту, технічний проект, план захисту території від надзвичайних ситуацій, технологічний регламент, технічні умови, паспорти устаткування та інша документація).

Вказується довідкова, науково–технічна література, нормативна й інша документація, в якій містяться вихідні дані, використані в аналізі.

У разі застосування відомих методів розрахунку й оцінок, мають бути наведені посилання на літературу та нормативні документи, в яких вони

наведені. Необхідно також надати обґрунтування вибору цих методів із визначенням їх недоліків і переваг.

Якщо застосовують оригінальні (авторські) методи розрахунків і оцінок необхідно надати повний опис і обґрунтування цих методів у розрахунково–пояснювальній частині Декларації безпеки об’єкта підвищеної небезпеки або посилання на апробацію. Обґрунтування має включати зіставлення результатів розрахунку з розрахунками, що виконані згідно з відомими методами, або з результатами відповідних експериментів.

Коли на різних етапах аналізу для визначення масштабу небезпеки та можливих наслідків застосовуються числові рішення складних фізико–математичних моделей із застосуванням комп’ютерних програм, вони мають бути обґрунтовані з використанням тестових перевірок.

Тестування числових розрахунків рекомендується проводити або порівнянням з результатами розрахунків, що виконуються для зіставних умов за допомогою обґрунтованих аналітичних методів, або на підставі експериментальної перевірки.

2.2. Об’єкти підвищеної небезпеки

Загальні положення

У 2001 р. в Україні прийнято Закон « Про об’єкти підвищеної небезпеки», який визначає правові, економічні, соціальні та організаційні основи діяльності, пов’язані з об’єктами підвищеної небезпеки, і спрямований на захист життя і здоров’я людей та довкілля від шкідливого впливу аварій на цих об’єктах шляхом запобігання їх виникненню, обмеження розвитку і ліквідації наслідків.

У Законі наведено ряд термінів, які визначають основні положення документа:

– *об’єкт підвищеної небезпеки (ОПН)* – це об’єкт, на якому використовуються, виготовляються, переробляються, зберігаються або транспортуються одна або кілька небезпечних речовин чи категорій речовин у

кількості, що дорівнює або перевищує нормативно встановлені порогові маси, а також інші об'єкти як такі, що відповідно до закону є реальною загрозою виникнення надзвичайної ситуації техногенного та природного характеру;

- *небезпечна речовина* – хімічна, токсична, вибухова, окиснювальна, горюча речовина, біологічні агенти та речовини біологічного походження, які становлять небезпеку для життя і здоровя людей та довкілля, сукупність властивостей речовин і/або особливостей їх стану, і в наслідок яких за певних обставин може створитися загроза життю та здоров'я людей, довкіллю, матеріальним і культурним цінностям;

- *порогова маса небезпечних речовин* – нормативно встановлена маса окремої небезпечної речовини або категорії небезпечних речовин, чи сумарна маса небезпечних речовин різних категорій;

- *ідентифікація об'єктів підвищеної небезпеки* – порядок визначення об'єктів підвищеної небезпеки серед потенційно небезпечних об'єктів;

- *потенційно небезпечний об'єкт* – об'єкт, на якому можуть використовуватися або виготовлятися, перероблятися, зберігатися чи транспортуватися небезпечні речовини, біологічні препарати, а також інші об'єкти, що за певних обставин можуть створити реальну загрозу виникнення аварії;

- *транскордонний вплив аварії* – шкода, заподіяна населенню та довкіллю однієї держави внаслідок аварії, яка сталася на території іншої держави;

- *ризик* – ступінь імовірності певної негативної події, яка може відбутися в певний час або за певних обставин на території об'єкта підвищеної небезпеки і/або за його межами;

- *прийнятний ризик* – ризик, який не перевищує на території об'єкта підвищеної небезпеки і/або за її межами гранично допустимого рівня;

- *управління ризиком* – процес прийняття рішень і здійснення заходів, спрямованих на забезпечення мінімально можливого ризику;

- *декларація безпеки* – документ, який визначає комплекс заходів, що вживається суб'єктом господарської діяльності з метою запобігання аваріям, а також забезпечення готовності до локалізації, ліквідації аварій та їх наслідків;
- *суб'єкт господарської діяльності* – юридична або фізична особа, у власності або у користуванні якої є хоча б один об'єкт підвищеної небезпеки.

Відповідно до прийнятої Постанови Кабінету Міністрів (КМУ) від 11.07.2002 р., № 956 «Про ідентифікацію та декларування безпеки об'єктів підвищеної небезпеки» затверджено:

– нормативи порогових мас небезпечних речовин для ідентифікації об'єктів підвищеної небезпеки;

– порядок ідентифікації та обліку об'єктів підвищеної небезпеки;

– порядок декларування безпеки об'єктів підвищеної небезпеки.

Виходячи із положень Закону та підзаконних актів, ОПН умовно розділяють на чотири основні сектори:

Сектор 1 – об'єкти з небезпечними речовинами, на які поширюється дія документа «Порядок ідентифікації та обліку об'єктів підвищеної небезпеки», затвердженого постановою КМУ від 11.07.2002 р., № 956 (далі «Порядок ...»).

Ці об'єкти підлягають ідентифікації з присвоєнням «1» чи «2» класу небезпеки відповідно до «Порядку ...» і категорії небезпеки згідно з «Переліком...».

Сектор 2 – гідротехнічні споруди.

Цим об'єктам надають клас гідротехнічної споруди залежно від висоти (чи глибини) і категорії небезпеки відповідно до «Переліку ...».

Сектор 3 – хвостосховища, шламонакопичувачі, накопичуювачі токсичних відходів.

Цим об'єктам надають клас сховища відповідно до його технічних характеристик і ступеня відповідності споруди, а також категорію небезпеки згідно до «Переліку ...».

Сектор 4 – інші об'єкти підвищеної небезпеки, що не входять в перші 3 сектори. Наприклад, об'єкти воєнного призначення, об'єкти, де присутні

радіоактивні речовини, об’єкти розвідки і видобудку корисних копалин, наявність небезпечних речовин, обумовлених природними явищами, кількість яких не може бути контрольована, та інше.

Ідентифікація та облік об’єктів підвищеної небезпеки

Суб’єкт господарської діяльності, у власності або користуванні якого є хоча б один потенційно небезпечний об’єкт чи який має намір розпочати будівництво такого об’єкта, організовує проведення його ідентифікації.

Потенційно небезпечний об’єкт вважається об’єктом підвищеної небезпеки відповідного класу у разі, коли значення сумарної маси небезпечної або декількох небезпечних речовин, що використовуються або виготовляються, переробляються, зберігаються чи транспортуються на об’єкті, перевищує встановлений норматив порогової маси.

Потенційно небезпечним об’єктом вважається апарат або сукупність пов’язаних між собою потоками в технологічний цикл апаратів, об’єднаних за адміністративною та/або територіальною ознакою. Потенційно небезпечним об’єктом за адміністративною ознакою вважається структурний підрозділ (виробництво, цех, відділення, дільниця тощо) суб’єкта господарської діяльності.

Під час проведення ідентифікації для кожного потенційно небезпечного об’єкта розраховується сумарна маса кожної небезпечної речовини із зазначених у нормативах порогових мас індивідуальних небезпечних речовин або кожної небезпечної речовини, яка за своїми властивостями може належати до будь–якої категорії або до декількох категорій небезпечних речовин згідно із зазначеними нормативами.

Нормативи порогових мас небезпечних речовин для ідентифікації об’єктів підвищеної небезпеки наведено в додатку «Порядку ...».

Процедура ідентифікації вважається закінченою, якщо виявиться, що сумарна маса хоча б однієї з усіх видів небезпечних речовин на потенційно небезпечному об’єкті, дорівнює або перевищує норматив порогової маси.

У разі коли сумарна маса жодної небезпечної речовини не перевищує нормативу порогової маси, за її властивостями визначається категорія та група, до яких вона може належати, а також сумарна маса небезпечних речовин однієї групи.

Порогову масу небезпечних речовин однієї групи визначають за формулою:

$$Q(pgr) = \Sigma g(i) / \Sigma(g(i) : Q(i)) \qquad (2.1)$$

де Σ – сумарна величина; $g(i)$ – сумарна маса небезпечної речовини, що знаходиться на об'єкті; $Q(i)$ – норматив порогової маси цієї небезпечної речовини.

Сумарна маса небезпечних речовин однієї групи дорівнює або перевищує її порогове значення, якщо виконується умова:

$$\Sigma(g(i) : Q(i)) \geq 1, \qquad (2.2)$$

Розрахунок найменшого та найбільшого значення порогової маси небезпечної речовини проводиться згідно з нормативами.

У разі коли сумарна маса небезпечних речовин однієї групи, що знаходяться на об'єкті, дорівнює або перевищує порогову масу, визначену відповідно до пунктів 11–13 цього Порядку, процедура ідентифікації вважається закінченою, і об'єкту присвоюється відповідний клас підвищеної небезпеки.

У разі коли сумарна маса небезпечних речовин не перевищує нормативу порогової маси, або коли сумарна маса небезпечних речовин однієї групи не перевищує порогової маси, процедура ідентифікації вважається закінченою і потенційно небезпечний об'єкт не належить до об'єктів підвищеної небезпеки за умови, що відстань від нього до місць великого скупчення людей (житлові масиви, стадіони, кінотеатри, лікарні, школи тощо), транспортних магістралей,

промислових, природоохоронних і життєво важливих цивільних об’єктів перевищує 500 метрів для небезпечних речовин груп 1 і 2 та 1 000 метрів для небезпечних речовин групи 3.

Якщо сумарна маса небезпечних речовин на потенційно небезпечному об’єкті не перевищує найменшого значення порогової маси згідно з нормативами або не перевищує порогової маси, але відстань від цього об’єкта до місць великого скупчення людей, транспортних магістралей, промислових, природоохоронних і життєво важливих цивільних об’єктів менша ніж 500 метрів для небезпечних речовин групи 1 і 2 та 1 000 метрів для небезпечних речовин групи 3, пороговою масою вважається маса небезпечних речовин, визначена за формулою:

$$Q(i.k) = Q(i) \cdot (R(x) : R(n))^2, \qquad (2.3)$$

де $Q(i.k)$ – норматив порогової маси небезпечних речовин для потенційно небезпечних об’єктів, розташованих від місць великого скупчення людей, транспортних магістралей, промислових, природоохоронних і життєво важливих цивільних об’єктів на відстані менше ніж 500 метрів для небезпечних речовин групи 1 і 2 і 1 000 метрів для речовин групи 3; $Q(i)$ – норматив порогової маси індивідуальних небезпечних речовин або категорій небезпечних речовин, або небезпечних речовин однієї категорії чи групи; $R(x)$ – відстань від потенційно небезпечного об’єкта до місць великого скупчення людей, транспортних магістралей, промислових, природоохоронних і життєво важливих цивільних об’єктів; $R(n)$ – гранична відстань, починаючи з якої проводиться перерахунок нормативу порогової маси (для речовин групи 1 і 2 $R(n)$ дорівнює 500 метрів, для речовин групи 3 – 1 000 метрів).

Якщо сумарна маса небезпечних речовин на потенційно небезпечному об’єкті перевищує порогову масу, об’єкту присвоюється відповідний клас підвищеної небезпеки.

Суб’єкт господарської діяльності складає повідомлення про результати ідентифікації об’єктів підвищеної небезпеки за формою ОПН–1 (додаток «Порядку ...») і надсилає його у двотижневий термін відповідним територіальним органам Держгірпромнаглядохоронпраці, Державної інспекції цивільного захисту та техногенної безпеки, Держекоінспекції, державної санітарно–епідеміологічної служби, Держпожбезпеки, Держархбудінспекції, а також відповідній місцевій держадміністрації або виконавчому органу місцевої ради (далі – уповноважені органи).

Місцеві держадміністрації або виконавчі органи місцевих рад публікують відомості про об’єкти підвищеної небезпеки в регіональних друкованих засобах масової інформації протягом 30 – ти днів після отримання повідомлення.

У разі зміни умов виробництва, номенклатури небезпечних речовин або їх кількості суб’єкт господарської діяльності, у власності або користуванні якого є об’єкти підвищеної небезпеки, проводить у 6–місячний термін їх повторну ідентифікацію.

Результати ідентифікації та розрахунки, на підставі яких вона проводилася, зберігаються суб’єктом господарської діяльності протягом 25 – ти років.

У разі припинення юридичної особи (смерті фізичної особи) – суб’єкта господарської діяльності зазначені документи підлягають передачі правонаступникові (спадкоємцеві), а у разі його відсутності – до державного архіву.

У разі відчуження об’єкта підвищеної небезпеки зазначені документи передаються його новому власнику.

Приклад розробки повідомлення про об’єкти підвищеної небезпеки на підприємстві Х за формою ОПН – 1, дані про порогові маси та повідомлення в органи Держгірпромнаглядохоронпраці разом із пояснювальною запискою наведено в додатку «Порядку ...».

Облік об'єктів підвищеної небезпеки

Державний реєстр об'єктів підвищеної небезпеки веде Держгірпромнаглядохоронпраці. Включення об'єкта підвищеної небезпеки до Державного реєстру об'єктів підвищеної небезпеки здійснюється протягом 30–ти робочих днів після подання суб'єктом господарської діяльності до територіального органу Держгірпромнаглядохоронпраці повідомлення про результати ідентифікації.

У разі надання суб'єктом господарської діяльності неповної інформації про результати ідентифікації, що передбачена повідомленням форми ОПН–І, Держгірпромнаглядохоронпраці письмово повідомляє про це суб'єкта господарської діяльності. Реєстрація об'єкта підвищеної небезпеки проводиться протягом 30–ти робочих днів після надання суб'єктом господарської діяльності необхідних матеріалів.

Протягом 10–ти робочих днів після реєстрації Держгірпромнагляд–охоронпраці видає суб'єкту господарської діяльності свідоцтво про державну реєстрацію об'єкта (об'єктів) підвищеної небезпеки.

Держгірпромнаглядохоронпраці публікує до 1 березня поточного року в загальнодержавних друкованих засобах масової інформації перелік об'єктів підвищеної небезпеки, включених до Державного реєстру об'єктів підвищеної небезпеки станом на 31 грудня попереднього року.

Виключення об'єкта підвищеної небезпеки з Державного реєстру об'єктів підвищеної небезпеки здійснюється за рішенням Держгірпромнагляд–охоронпраці на підставі звернення та усіх необхідних документів, які подаються суб'єктом господарської діяльності до територіальних органів Держгірпромнаглядохоронпраці у разі:

- проведення змін, що призвели до зменшення на об'єкті підвищеної небезпеки сумарної маси небезпечних речовин порівняно з найменшим нормативом порогової маси відповідно до нормативів порогових мас;
- ліквідації або виведення з експлуатації (списання з балансу) об'єкта підвищеної небезпеки.

Суб’єкти господарської діяльності несуть відповідальність згідно із законодавством за своєчасне, повне і достовірне проведення ідентифікації об’єктів підвищеної небезпеки.

Декларування безпеки об’єктів підвищеної небезпеки

Суб’єкт господарської діяльності, у власності або користуванні якого є хоча б один об’єкт підвищеної небезпеки, організовує розроблення і складання декларації безпеки об’єкта підвищеної небезпеки (далі – декларація безпеки).

Декларація безпеки складається на основі дослідження суб’єктом господарської діяльності ступеня небезпеки та оцінки рівня ризику виникнення аварій (далі – рівня ризику), що пов’язані з експлуатацією цих об’єктів.

Для об’єктів підвищеної небезпеки, що експлуатуються, декларація безпеки складається як самостійний документ, а для об’єктів підвищеної небезпеки, що будуються (реконструюються, ліквідуються), – як складова частина відповідної проектної документації.

За наявності на одному виробничому майданчику декількох об’єктів підвищеної небезпеки складається одна декларація безпеки.

Декларація безпеки повинна включати:

- результати всебічного дослідження ступеня небезпеки та оцінки рівня ризику;
- оцінку готовності до експлуатації об’єкта підвищеної небезпеки відповідно до вимог безпеки промислових об’єктів;
- перелік прийнятих з метою зниження рівня ризику рішень і здійснених з метою запобігання аваріям заходів;
- відомості про заходи щодо локалізації і ліквідації можливих наслідків аварій.

Для об’єкта підвищеної небезпеки, що експлуатується або ліквідується, подається інформація про заходи, що здійснюються, і про ті, що плануються.

Для об’єкта підвищеної небезпеки, що будується або реконструюється, подається інформація про заходи, які передбачені проектною документацією та плануються до здійснення під час експлуатації.

Для об’єктів підвищеної небезпеки, що ідентифіковані як об’єкти підвищеної небезпеки 1–го класу, результати дослідження ступеня небезпеки та оцінки рівня ризику, а також обґрунтування прийнятих щодо безпечної експлуатації та локалізації і ліквідації наслідків аварій рішень подаються в декларації безпеки у розділі «Розрахунково–пояснювальна частина».

Оцінка рівня ризику проводиться згідно з Методикою визначення ризиків та їх прийнятних рівнів для декларування безпеки об’єктів підвищеної небезпеки.

Суб’єкт господарської діяльності проводить відповідно до вимог Законів України «Про екологічну експертизу» (45/95–ВР), «Про наукову та науково–технічну експертизу» (51/95–ВР) експертизу повноти дослідження ступеня небезпеки та оцінки рівня ризику, а також обґрунтованості та достатності прийнятих щодо зменшення рівня ризику, готовності до дій з локалізації і ліквідації наслідків аварій рішень (далі – експертиза). Фінансування проведення експертизи покладається на суб’єкта господарської діяльності.

Декларація безпеки разом із позитивним висновком експертизи подається відповідним територіальним органам Держгірпромнаглядохоронпраці, Державної інспекції цивільного захисту та техногенної безпеки, Держекоінспекції, державної санітарно–епідеміологічної служби, Держпожбезпеки, Держархбудінспекції, а також відповідній місцевій держадміністрації або виконавчому органу місцевої ради (далі – уповноважені органи):

■ для об’єктів підвищеної небезпеки, що на дату набрання чинності цим Порядком експлуатуються або ліквідуються, – протягом року після державної реєстрації об’єкта підвищеної небезпеки;

■ для об’єктів підвищеної небезпеки, експлуатація яких планується, – разом із заявою на отримання дозволу на експлуатацію відповідно до Закону України «Про об’єкти підвищеної небезпеки» .

Місцеві держадміністрації або виконавчі органи місцевих рад протягом 30–ти днів після отримання декларації безпеки оприлюднюють у регіональних друкованих засобах масової інформації відомості про об’єкт підвищеної небезпеки.

Про можливе здійснення трансграничного впливу аварії на об’єкті підвищеної небезпеки суб’єкт господарської діяльності інформує уповноважені органи, а також в установленому порядку через МЗС відповідні органи держав, території яких можуть зазнавати впливу таких аварій, і пункт зв’язку з метою оповіщення про промислові аварії, який діє в Україні згідно з Конвенцією про трансграничний вплив промислових аварій (995–262) (1992 рік).

Суб’єкт господарської діяльності, у власності або користуванні якого є об’єкти підвищеної небезпеки, надає будь–якій фізичній або юридичній особі на її аргументований запит можливість ознайомитися із змістом декларації безпеки, а також з будь–якою іншою інформацією, яка стосується цих об’єктів.

Декларація безпеки переглядається суб’єктом господарської діяльності один раз на п’ять років. Декларація безпеки переглядається, уточнюється або розробляється в інші терміни у разі:

- зміни умов діяльності об’єкта підвищеної небезпеки, що призводять до підвищення ступеня небезпеки та рівня ризику, незалежно від їх причин;
- зміни та/або набрання чинності нормативно–правовими актами, що впливають на зміст відомостей, поданих у декларації безпеки;
- будівництва в прилеглих районах нових підприємств (об’єктів), якщо це впливає на зміст відомостей, поданих у декларації безпеки;
- обґрунтованої вимоги уповноваженого органу або громадськості.

Оригінал декларації безпеки та висновку експертизи, а також копії документів, що підтверджують передачу зазначених документів

уповноваженим органам, зберігаються у суб'єкта господарської діяльності, у власності або користуванні якого є об'єкт підвищеної небезпеки, протягом 25–ти років.

У разі припинення юридичної особи (смерті фізичної особи) – суб'єкта господарської діяльності – декларація безпеки та висновок експертизи підлягають передачі правонаступникові (спадкоємцеві), а у разі його відсутності – до державного архіву.

У разі відчуження об'єкта підвищеної небезпеки зазначені документи передаються його новому власнику.

Уповноважені органи ведуть облік декларацій безпеки об'єктів підвищеної небезпеки.

Включення декларації безпеки до Державного реєстру об'єктів підвищеної небезпеки здійснюється протягом 30 робочих днів після її подання суб'єктом господарської діяльності до територіального органу Держгірпромнагляд охоронпраці.

Держгірпромнаглядохоронпраці проводить реєстрацію декларацій безпеки з присвоєнням кожній реєстраційного номера (коду), що зазначається на її титульному аркуші.

Протягом 10–ти робочих днів після реєстрації Держгірпромнагляд–охоронпраці письмово повідомляє суб'єкта господарської діяльності про реєстраційний номер (код) декларації безпеки у Державному реєстрі об'єктів підвищеної небезпеки.

Держгірпромнаглядохоронпраці публікує до 1 березня поточного року в загальнодержавних друкованих засобах масової інформації перелік декларацій безпеки, зареєстрованих у Державному реєстрі об'єктів підвищеної небезпеки станом на 31 грудня попереднього року.

Суб'єкти господарської діяльності несуть відповідальність згідно із законодавством за повноту та достовірність відомостей, поданих у декларації безпеки.

Проведення експертизи декларації безпеки

Експертизу декларації безпеки можуть проводити суб'єкти господарської діяльності всіх форм власності, що займаються науковою і науково–технічною діяльністю у сфері безпеки промислових об'єктів, у тому числі спеціалізовані експертні організації, акредитовані відповідно до вимог Закону України «Про наукову та науково–технічну експертизу» (51/95–ВР) (далі – експертні організації).

Експертну організацію для проведення експертизи суб'єкт господарської діяльності обирає самостійно. Експертизу не може проводити експертна організація, яка розробляла декларацію безпеки.

Умови проведення експертизи визначаються договором між суб'єктом господарської діяльності та експертною організацією.

У висновку експертизи дається оцінка повноти дослідження ступеня небезпеки та оцінки рівня ризику, а також обґрунтованості та достатності прийнятих щодо зменшення рівня ризику готовності до дій з локалізації і ліквідації наслідків аварій рішень.

Висновок експертизи повинен містити:

– найменування виду експертизи із зазначенням її об'єктів;

– виклад підстав для проведення експертизи;

– відомості про експертну організацію та експертів;

– дані про замовника та перелік об'єктів експертизи;

– відомості про розглянуті в процесі експертизи документи та об'єкти;

– результати проведення експертизи.

Висновок експертизи, підписаний експертами, які її проводили, затверджує керівник експертної організації. Підпис керівника засвідчується печаткою експертної організації.

Результати проведення експертизи повинні містити оцінку:

– повноти і достовірності інформації, що міститься в декларації безпеки;

– обґрунтованості результатів дослідження ступеня небезпеки та оцінки рівня ризику;

– обґрунтованості та достатності рішень, прийнятих на основі аналізу рівня ризику, для зниження його до прийнятної величини, готовності до дій з локалізації і ліквідації наслідків аварій.

У разі негативного висновку експертизи суб'єкт господарської діяльності має право подати декларацію безпеки на повторну експертизу після врахування зауважень.

Суб'єкт господарської діяльності може оскаржити висновок експертизи декларації безпеки в установленому порядку.

Організація, що проводить експертизу декларації безпеки, несе відповідальність згідно із законодавством за її повноту, достовірність та об'єктивність.

Функціонування системи аналізу й управління ризиками

Для вирішення питання регулювання безпеки населення, територій і суспільства в цілому в Україні створюється система аналізу управління ймовірності спричинення шкоди за так званим «об'єктам турботи», головним з яких є людина.

Основними етапами такої системи є:

1) збирання повної і достовірної інформації про об'єкти підвищеної небезпеки, проведення їх ідентифікації та реєстрації;

2) інформування суспільства через засоби масової інформації;

3) кількісна та якісна оцінка небезпеки кожного об'єкта, ідентифікація для населення і території, яка включає: визначення ризику виникнення аварії на об'єкті, оцінення можливості її локалізації в процесі розвитку, визначення можливих негативних наслідків та ймовірності їх настання, визначення можливості ліквідації негативних наслідків аварії;

4) зіставлення розрахунковим шляхом отриманих ризиків з установленими прийнятними рівнями;

5) за необхідності розроблення і реалізація заходів зі зниження розрахункових рівнів ризиків до встановлених прийнятних рівнів;

6) інформування суспільства через засоби масової інформації про ступінь небезпеки об’єкта;

7) проведення обов’язкового страхування громадської відповідальності суб’єкта господарської діяльності за шкоду, яку може бути завдано пожежами та аваріями на об’єктах підвищеної небезпеки;

8) контроль за рівнем небезпеки об’єктів з урахуванням часу.

Законодавством передбачено основні напрями механізму реалізації системи управління ризиками.

Зокрема суб’єкт господарської діяльності зобов’язаний:

- провести ідентифікацію об’єкта підвищеної небезпеки і зареєструвати його в органах держнагляду;
- забезпечити розробку й експертизу декларації безпеки, плану локалізації і ліквідації аварійних ситуацій та аварій на об’єкті, узгодити і зареєструвати їх в установленому порядку;
- одержати дозвіл на експлуатацію об’єкта в місцевих органах виконавчої влади;
- забезпечити експлуатацію об’єкта з мінімальними можливими ризиком і з виконанням вимог інших нормативно-правових актів, які регулюють діяльність, пов’язану з об’єктами підвищеної небезпеки;
- застрахувати свою громадянську відповідальність за шкоду, яку може бути завдано пожежами та аваріями на об’єктах підвищеної небезпеки.

Державний нагляд за виконанням вимог нормативно–правових актів відносно об’єктів підвищеної небезпеки виконують органи:

- Держгірпромнаглядохоронпраці;
- Державна інспекція із забезпечення захисту населення і території від надзвичайних ситуацій техногенного та природного характеру (ДСНС);
- Державна інспекція із забезпечення екологічної безпеки та охорони навколишнього середовища;
- Державна інспекція санітарно-епідемічної безпеки;

- Державна інспекція містобудування.

Запитання для самоконтролю

1. Яке призначення методики визначення ризиків та їх допустимих рівнів? Назвіть галузь застосування.

2. Основні терміни та визначення, щодо об’єктів підвищенної небезпеки.

3. Із яких етапів складається аналіз небезпеки та ризику аварій на об’єктах підвищенної небезпеки? Основні етапи аналізу.

4. У чому полягає завдання дослідження ризику на об’єкті підвищенної небезпеки? Заходи щодо розробки декларації.

5. Соціально важливі об’єкти «турботи». Що належить до категорії «інші» важливі об’єкти турботи?

6. Які методи аналізу небезпек застосовуються при аналізі експлуатаційних небезпек?

7. Як визначається територіальний ризик? Що враховується при оціненні масштабів аварії? Наслідки аварій.

8. Як визначається прийнятний (допустимий) ризик для об’єкта турботи?

9. Які рівні ризику є не допустимими для територіального та соціального ризиків?

10. Які рівні ризику є не допустимими для індивідуального ризику?

11. Які види небажаних негативних наслідків розглядаються для об’єктів «турботи»?

12. На яких принципах ґрунтується прийняття рішень за результатами аналізу небезпеки й оцінки ризику?

13. Чи може університет належити до об’єктів підвищеної небезпеки (ОПН)?

14. На скільки секторів умовно поділяють ОПН?

15. Коли можна вважати закінченою процедуру ідентифікації ОПН? Порогова маса небезпечних речовин.

16. За якою формою складається повідомлення про результати ідентифікації ОПН?

17. Який документ повинен бути у суб'єкта господарської діяльності, що свідчить про його турботу за забезпечення безпеки ОПН?

18. Що включають основні напрями механізму реалізації системи управління ризиками на законодавчому рівні?

Тема 3. УПРАВЛІННЯ РИЗИКАМИ. МІЖНАРОДНИЙ СТАНДАРТ ISO 31000:2009

3.1. «П'яти крокова система» оцінки професійних ризиків.

3.2. Міжнародний стандарт ISO 31000:2009.

3.1. **«П'яти крокова система» оцінки професійних ризиків**

У міжнародній практиці поширеним підходом до оцінки професійних ризиків є так звана « П'яти крокова система».

Крок 1. Ідентифікація небезпек, що призводять до ризику. На цьому етапі потрібно розглянути на робочому місці все, що потенційно може спричинити заподіяння шкоди, і визначити працівників, які можуть зазнавати небезпеки.

Крок 2. Оцінювання та «ранжирування» ризиків (їх серйозність, їх імовірність та ін.), розподіл за важливістю.

Крок 3. Визначення превентивних заходів. На цьому етапі необхідно ідентифікувати підходящі заходи для виключення ризиків та управління ними.

Крок 4. Вживання заходів. Реалізація цього кроку полягає у складанні плану реалізації захисних та превентивних заходів (можливо, не всі проблеми можуть бути вирішені негайно), визначенні, хто, що і коли конкретно робить і якими засобами забезпечується виконання запланованих заходів.

Крок 5. Моніторинг та перевірка. Оцінку слід проводити на регулярній основі. Результати оцінки повинні переглядатися при значущих змінах в організації виробництва, а також при нещасних випадках.

Елементи цього підходу містяться в європейських рекомендаціях з оцінки ризику, а також у Методичних вказівках щодо проведення аналізу ризику небезпечних виробничих об'єктів, затверджених постановою Держгіртехнагляду від 10.07.2001 р. № 30.

3.2. Міжнародний стандарт ISO 31000:2009

ISO 31000 призначений для сімейства стандартів, пов'язаних із управлінням ризиками та запропанованих Міжнародною організацією зі стандартизації. Метою ISO 31000:2009 є забезпечення загальних керівних принципів з управління ризиками. ISO 31000 спрямований на забезпечення загальновизнаної парадигми для практиків і компаній, що використовують процеси управління ризиками, щоб замінити безліч існуючих стандартів, методологій та парадигм, які відрізнялися між галузями, з урахуванням питань і регіонів.

У цей час стандарт ISO 31000 включає:

• ISO 31000:2009 – Принципи та Керівництво з впровадження;

• ISO / IEC 31010:2009 – Управління ризиками – методи оцінки ризику[18];

• ISO Guide 73:2009 – Управління ризиками – Словник [19].

ISO 31000 був опублікований як стандарт 13 листопада 2009 р. та надає стандартний підхід щодо здійснення управління ризиками. Переглянуті і узгоджені ISO / IEC Guide 73 було опубліковано в той самий час. Мета ISO 31000:2009 – застосування і адаптація для «будь–яких державних, приватних або громадських підприємств, об'єднань, груп або індивіду».

18. ISO / IEC 31010, Ризик–менеджмент – Техніки оцінки ризику

19. Керівництво ISO 73: 2009, Risk Ризик–менеджмент: Словник

Таким чином, загальна сфера ISO 31000 – в сімействі стандартів управління ризиками – не розроблення для певної групи промисловості системи управління, мається на увазі, швидке забезпечення оптимальної структури практики і керівництва усіх операцій, пов'язаних з управлінням ризиками.

ISO 31000:2009 надає загальні керівні принципи для розробки, впровадження та супроводу процесів управління ризиками у межах всієї організації. Такий підхід до оформлення практики управління ризиками сприятиме найбільш широкому впровадженню компаніями, які вимагають для управління ризиками стандарт, що вміщує декілька систем управління.

У рамках цього підходу до управління ризиками передбачається забезпечення всіх стратегічних, управлінських і оперативних завдань організації на проектах, функцій і процесів, які будуть узгоджені із загальним набором цілей управління ризиками.

Відповідно ISO 31000:2009 призначений для широкої групи зацікавлених осіб, включаючи:

• зацікавлених сторін виконавчого рівня;

• призначенних кураторів групи управління ризиками на підприємстві;

• ризик–аналітиків та співробітників управління;

• лінійних керівників і менеджерів проектів;

• внутрішніх аудиторів;

• незалежних практиків.

Ризик концептуалізації. Однією з ключових змін парадигми є запропонований у ISO 31000 ризик концептуалізації. Відповідно до ISO 31000:2009 і перегляду термінології, поняття «ризик» більше не є «випадковістю або ймовірністю втрати», або «ефектом невизначеності мети». Слово «ризик» тепер може бути використано для позначення як позитивних, так і негативних можливостей.

ISO 31000 – рамковий підхід. Стандарт ISO 31000:2009 був отриманий як заміна існуючому стандарту з управління ризиками – AS/NZS 4360:2004. Стандарт ISO 31000:2009 призначений для системи управління, яка підтримує

розроблення, впровадження, підтримання та покращення процесів управління ризиками.

Здійснення. Мета стандарту ISO 31000 – застосування у рамках існуючих систем управління, формалізація і поліпшення процесів управління ризиками.

Впровадження стандарту ISO 31000 передбачало:

• закриття прогалин при передачі звітності в управлінні ризиками на підприємстві;

• вирівнювання цілей як основ управління з ISO 31000;

• удосконалення механізмів управління системою звітності;

• створення єдиних критеріїв оцінки ризику та методик.

Наслідки. Більшість наслідків прийняття нового стандарту стосуються реорганізації існуючої практики управління згідно з документацією, комунікацією та соціалізацією нової парадигми управління операційних ризиків; на відміну від загальної переорієнтації практики управління в рамках всієї організації. Відповідно, найвищі службові особи управління ризиками організацій, мають бути інформовані про наслідки прийняття стандарту і бути спроможними розробити ефективні стратегії для впровадження стандарту по всьому ланцюжку поставок і комерційних операцій.

Деякі аспекти верхньої підзвітності управління, стратегічного здійснення політики й ефективних структур управління потребують більшої уваги щодо організації, яку раніше використовували як зайве, а тепер – як методологію управління ризиками.

У деяких сферах, що стосуються менеджменту ризиків, зокрема, безпеки та корпоративної соціальної відповідальності, яка може працювати з використанням відносно простих процесів управління ризиками, більше матеріалу необхідно буде змінити, особливо щодо чіткого формулювання політики управління ризиками, формалізації процесів власності ризиків, структурування у рамках процесів і прийняття програми безперервного поліпшення.

Управління ризиками. ISO 31000:2009 передбачає порядок, за яким необхідно працювати із ризиками з урахуванням пріоритетів:

а) уникнення ризиків, вирішивши не починати або не продовжувати діяльність, що призводить до ризику;

б) вилучення або зменшення ризику для того, щоб контролювати можливі наслідки;

в) усунення джерел ризику;

г) зміни ймовірності;

д) зміни наслідків;

е) розподілу ризиків з іншою стороною або сторонами (у тому числі договорів та фінансування ризику);

ж) збереження ризик–обґрунтованого рішення.

Акредитація. ISO 31000 було розроблено з метою сертифікації (2009). Починаючи з березня 2013 року, затверджено тренінги з акредитації та сертифікації щодо ISO 31000. Професійні сертифікати організовані та видаються Академією професійної сертифікації (APC, http://www.apc.org.hk).

Менеджмент ризиків. Впровадження серії стандартів ISO 31000, підготовленої 262 Проектним комітетом «Управління ризиками» Міжнародної організації зі стандартизації (ISO), допоможе виявити і, в умовах повної невизначеності, ефективно управляти ризиками, які впливають на досягнення цілей і діяльність організацій, наприклад, на їх економічну ефективність, ділову репутацію, навколишнє природне середовище, безпеку персоналу і соціальні наслідки. На сьогоднішній день серія ISO 31000 представлена групою стандартів, настановами та технічними звітами, що наведені далі.

ISO 31000:2009 «Менеджмент ризиків. Принципи і керівні вказівки» містить одинадцять принципів і загальні керівні вказівки з ефективного виявлення та управління ризиками, тобто, зовнішніми і внутрішніми факторами і впливами, які додають невизначеності у досягнення цілей організації. Цей стандарт також включає в себе рекомендації з розробки, впровадження та постійного вдосконалення структури, мета якої полягає в інтеграції процесу

управління ризиками в загальну схему управління, формування стратегії, а також планування, управління, процеси, політику, цінності і культуру організації. Положення стандарту ISO 31000: 2009 можуть бути застосовані до будь–якого типу ризику, незалежно від його походження, що має позитивні або негативні наслідки. ISO 31000:2009 може бути використаний в організації в цілому або її окремих частинах і різних видах діяльності, включаючи стратегії і рішення, операції, процеси, функції, проекти, товари, послуги та активи. Сфера застосування стандарту поширюється на будь–які державні та комерційні підприємства, асоціації, групи і фізичні особи. Метою створення ISO 31000: 2009 є гармонізація процесів управління ризиками в існуючих і майбутніх стандартах, а також забезпечення єдиного підходу для підтримки та реалізації вимог стандартів, що стосуються конкретних ризиків і/або галузей промисловості.

ISO Guide 73:2009 «Менеджмент ризиків. Словник» доповнює ICO 31000, забезпечує послідовне розуміння й узгоджений підхід до концепції управління ризиками, містить визначення загальних термінів, пов'язаних з ідентифікацією, аналізом, моніторингом, оцінкою, управлінням ризиком, а також процесами і, власне, менеджментом ризиків. Цей посібник призначено для використання особами, відповідальними за управління ризиками в організаціях, експертів і фахівців, що беруть участь в діяльності ISO і IEC, і розробників національних і галузевих нормативних документів, що стосуються менеджменту ризиків.

ISO/TR31004:2013 «Менеджмент ризиків. Керівництво з впровадження ISO 31000» сприяє ефективному впровадженню ISO 31000 та забезпечує:

- структурований підхід до переходу від існуючої практики управління ризиками до ISO 31000 з гнучкою перспективою адаптації до майбутніх змін;
- роз'яснення базових концепцій ISO 31000 з рекомендаціями та прикладами, адаптованими до індивідуальних потреб користувачів;
- додаткове керівництво за принципами ISO 31000 та основи управління ризиками.

ISO/IEC 31010:2009 «Менеджмент ризиків. Методи оцінки ризиків» був підготовлений 56 Технічним комітетом «Надійність» Міжнародної електротехнічної комісії (IEC) спільно з 262 TC ISO. Цей стандарт доповнює положення ISO 31000.

ISO/IEC 31010 зосереджено на поняттях, процесах і виборі методу оцінки ризиків та забезпечує основу для прийняття рішення про застосування найбільш доцільного підходу для оцінки конкретних ризиків.

У стандарті наведено приклади різних методів оцінки ризику (у тому числі «мозковий штурм», метод Делфі, «попередній аналіз небезпеки», методи HAZOP, HACCP, FMEA, FTA, «дерево прийняття рішень», техніка SWIFT, метод Монте–Карло та ін. – всього 31 метод) і дані посилання на інші міжнародні стандарти, в яких більш докладно описано їх застосування.

Міжнародний стандарт ISO 31000 – Перше видання 2009-11-15.

ISO (International Organization for Standardization – Міжнародна організація зі Стандартизації) є всесвітньою федерацією національних органів по стандартизації (органів-членів ISO). Робота над підготовкою Міжнародних Стандартів виконується, як правило, технічним комітетом ISO. Кожен орган–член ISO, зацікавлений у меті, для якої був створений технічний комітет, має право бути представленим у цьому комітеті. Міжнародні організації, урядові та неурядові, що підтримують зв’язок з ISO, також беруть участь у роботі. ISO також тісно співпрацює з Міжнародною електротехнічною комісією (IEC), ведеться спільна робота з усіх питань електротехнічної стандартизації.

Міжнародні Стандарти складаються відповідно до правил, викладених у Директивах ISO / IEC, Частина 2.

Основною метою технічного комітету є підготовка Міжнародних Стандартів. Проекти Міжнародних Стандартів направляються технічним комітетом органам-членам ISO для голосування. Публікація документа як Міжнародного Стандарту відбувається тільки після схвалення щонайменше 75% голосуючих органів-членів ISO.

Особливу увагу приділено тому, що деякі елементи цього документа можуть бути предметом патентних прав. ISO не повинна бути відповідальною за їх ідентифікацію або всі подібні патентні права.

Стандарт ISO 31000 був підготовлений ISO Technical Management Board Working Group (робочею групою із технічного менеджменту) з управління ризиками.

Організації всіх типів і розмірів стикаються з внутрішніми і зовнішніми чинниками і впливами, через які стає неможливо визначити, як і коли вони досягнуть своїх цілей. Вплив невизначеності на цілі організації визначається як «ризик».

Будь–яка діяльність організації пов’язана з ризиком. Організації управляють ризиком за допомогою його ідентифікації, аналізу та подальшого вирішення щодо обробки з метою задоволення критеріїв ризику. Протягом усього процесу організації здійснючи комунікації та консалтинг із зацікавленими сторонами, управляють та аналізують ризик і засоби управління, які модифікують ризик з метою забезпечення того, що наступна обробка ризику не буде потрібна. Даний Міжнародний Стандарт описує цей систематичний і логічний процес у деталях.

У той час як всі організації управляють ризиком до певної міри, цей Міжнародний Стандарт встановлює деякі принципи, при виконанні яких управління ризиками стає більш ефективним. Міжнародний Стандарт рекомендує організаціям розвивати, впроваджувати та постійно покращувати систему, метою якої є інтеграція процесу з управління ризиками з керівництвом, стратегією і плануванням, управлінням, процесами звітності, політикою, цінностями і культурою.

Ризик-менеджмент можна застосувати до цілої організації, до її майданчиків і рівнів, у будь-який час, а також і до певних функцій, проектів та видів діяльності.

Незважаючи на те що практика ризик-менеджменту розвинулася після тривалого часу і в багатьох галузях для задоволення різних потреб,

впровадження послідовних процесів у рамках всебічної системи може допомогти гарантувати, що ризик управляється ефективно, раціонально і послідовно у всій організації. Загальний підхід, описаний в цьому Стандарті, відбиває принципи та керівництва для управління будь-якою формою ризиків систематичним і прозорим способом для будь-якої галузі і будь-якого контексту.

Кожна певна сфера ризик-менеджменту застосовна до індивідуальних потреб, аудиторії, сприйняття і критеріїв. Тому основною особливістю цього Міжнародного Стандарту є «встановлення контексту» як заходів на початку загального процесу управління ризиками. Встановлення контексту зафіксує цілі організації, умови, за яких вона намагається досягти своїх цілей, зацікавлені сторони і різноманітність критеріїв ризику, кожен з яких допоможе виявити й оцінити природу та складність ризику організації.

Відношення між принципами управління ризиком, системою, в якій воно з'являється і процесом управління ризиками описано в цьому Міжнародному Стандарті, та наведено на рис. 3.1.

Коли система впроваджена і підтримується відповідно до Міжнародного Стандарту, управління ризиками дозволяє організації:

– збільшити ймовірність досягнення цілей;

– підтримувати випереджаюче управління;

– поліпшити фінансову звітність;

– поліпшити обізнаність про необхідність ідентифікувати й обробляти ризик у всій організації;

– поліпшити ідентифікацію можливостей і обробки ризиків;

– відповідати релевантним законодавчим вимогам та регламентам, а також міжнародним нормам;

– поліпшити діяльність управління;

– посилити довіру зацікавлених сторін;

– встановити надійну основу для прийняття рішень і планування;

– поліпшити контроль;

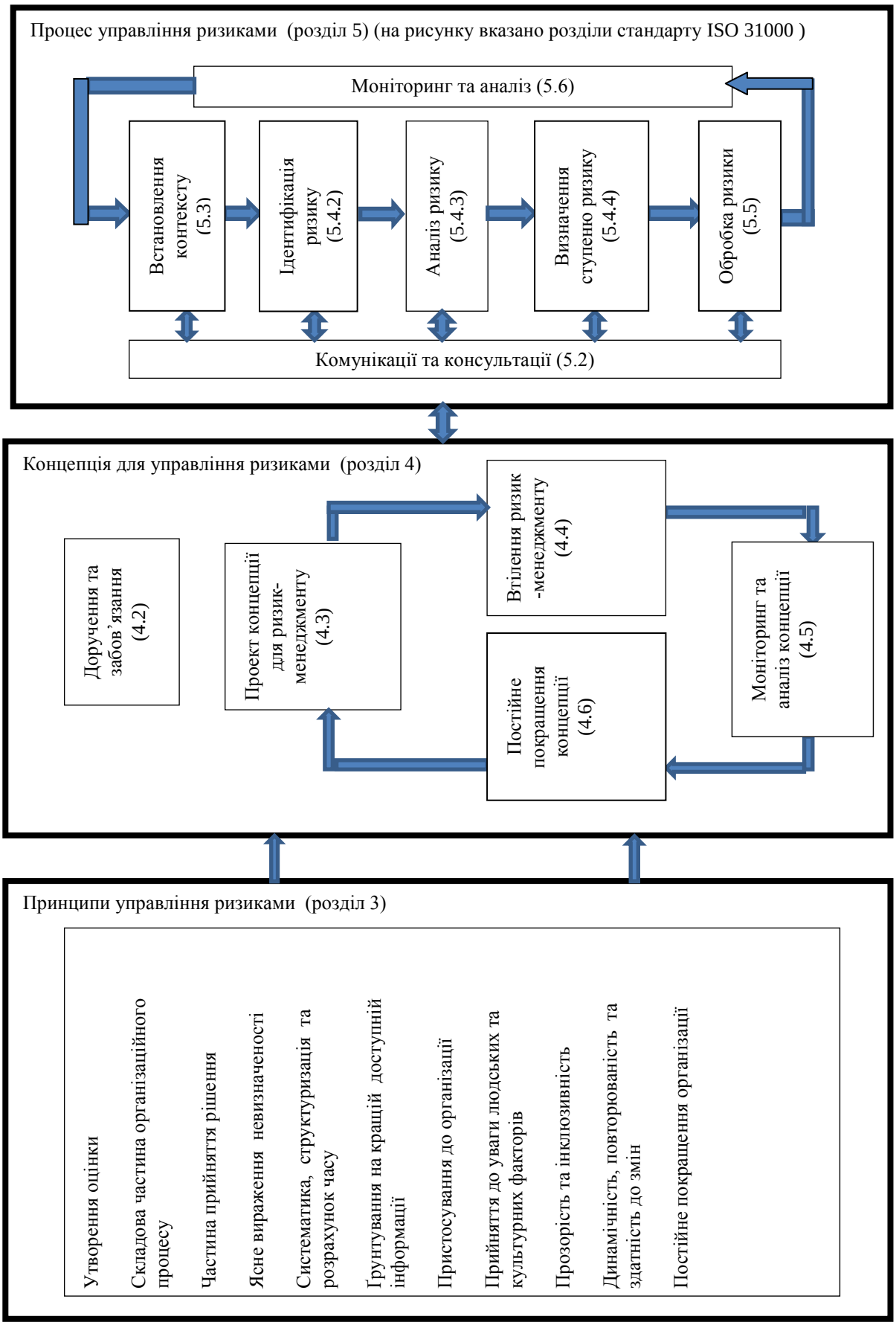

Рисунок 3.1. – Відношення між принципами управління ризиком, системою, в якій воно з'являється і процесом управління ризиками

– ефективно розподілити і використати ресурси для обробки ризику;

– поліпшити оперативну ефективність і результативність;

– поліпшити показники професійної безпеки та здоров'я, а також екологічні показники;

– поліпшити попередження втрат і дії з ліквідації наслідків пригод;

– мінімізувати втрати;

– поліпшити навчання на робочому місці;

– поліпшити працездатність колективу.

Ций Міжнародний Стандарт призначений для задоволення потреб широкого кола зацікавлених сторін, включаючи:

– відповідальних осіб за розвиток політики ризик менеджменту у своїй організації

– відповідальних осіб за забезпечення того, що ризиком ефективно управляють у всій організації або в якійсь певній області, проект або діяльності

– осіб, яким необхідна оцінка продуктивності організації в області управління ризиками

– розробників стандартів, інструкцій, процедур і кодексів правил, які повністю або частково встановлюють, яким чином слід управляти ризиками в контексті даного документа.

Поточні процеси управління багатьох організацій включають компоненти управління ризиками, також багато організацій вже офіційно прийняли формальні процеси управління ризиками для особливих типів ризиків або обставин. У подібних випадках організація може виконувати аналіз існуючих практик і процесів відповідно до цього Міжнародного Стандарту.

У Міжнародному Стандарті використовуються вирази «ризик менеджмент» і «Управління ризиком». Сформульований в загальному сенсі вираз «ризик-менеджмент» належить до «архітектури» (тобто принципів, умов і процесів) ефективного управління ризиками, при цьому вираз «управління ризиком» належить до застосування цієї архітектури до певного ризику. У

стандарті використовуються такі терміни, як прозорість та інклюзивність. Інклюзивність (від лат. Include, що означає включаю, укладаю) – це властивість, пов’язана з включенням живого чи неживого об’єкта в будь-яке явище або їх безліч. Інклюзія означає процес залучення в що–небудь. Синонімом «інклюзивний» є слово «включений», а протилежним за значенням – «ексклюзивний» (або виключений).

Сфера застосування.

Даний Міжнародний Стандарт надає принципи та концептуальні керівництва з управління ризиками, може бути використаний будь–яким державним, приватним чи громадським підприємством, асоціацією, групою компаній або окремою компанією, тому його може офіційно прийняти будь–яка індустрія або сфера діяльності.

Цей Міжнародний Стандарт може бути застосовний протягом всього життєвого циклу організації, а також до широкого спектра діяльності, включаючи стратегії і рішення, операції, процеси, функції, проекти, продукцію, послуги та активи; до будь-якого типу ризиків, незалежно від того, яку природу вони мають, а також позитивні чи негативні наслідки.

Незважуючи на те що цей Міжнародний Стандарт пропонує концептуальні керівні принципи, його метою не є проголошення однаковості ризик-менеджменту у всіх організаціях. При розробці та впровадженні проектів і концепцій ризик-менеджменту потрібно враховувати різні потреби кожної організації, конкретні цілі, контекст, структуру, операції, процеси, функції, проекти, продукцію, послуги та активи, а також практичну роботу.

Передбачається, що цей стандарт буде використовуватися для узгодження процесів з управління ризиками в існуючих і майбутніх стандартах. Він надає загальний підхід сприяння стандартів, в яких йдеться про особливі ризики та/або сфери ризиків, не замінюючи ці стандарти.

Терміни та визначення

Ризик – в*плив невизначеності на цілі*. Вплив розглядається як відхилення від очікуваного – з позитивними або негативними наслідками. Цілі можуть

мати різні аспекти (фінансові; аспекти, що стосуються професійної безпеки та здоров'я; екологічні задачі) і можуть належити до різних рівнів (стратегічний рівень, організаційний, рівень проекту, продукції та процесу).

Невизначеність – це стан, частково відсутність інформації щодо розуміння або знання події, її наслідків або ймовірності.

Ризик-менеджмент – скоординовані дії для того, щоб направляти і контролювати організацію відносно ризиків

Концепція ризик-менеджменту – набір компонентів, що надають основи й організаційні заходи для проектування, впровадження, моніторингу, аналізу і постійного поліпшення ризик-менеджменту у всій організації. Основи включають політику, цілі, доручення і зобов'язання управляти ризиками . Організаційні заходи передбачають планування, відносини, звітність, ресурси, процеси і діяльність. Концепція ризик-менеджменту включена в загальну стратегію організації, оперативну політику і діяльність.

Політика ризик-менеджменту – становище загальних намірів і напрямів організації щодо ризик-менеджменту.

План ризик-менеджменту – схема в складі концепції ризик-менеджменту, що визначає підхід, компоненти менеджменту та ресурси, застосовні до управління ризиками. Компоненти менеджменту зазвичай включають процедури, практики, призначення відповідальних осіб, послідовність і час дій. План ризик-менеджменту може бути застосований до певного продукту, процесу і проекту, а також до частини і цілої організації.

Власник ризику – особа або об'єкт, який несе відповідальні за управління ризиками.

Процес управління ризиками – систематичне застосування політики менеджменту, процедур і практик щодо відношенню щодо комунікації, консалтингу, встановлення контексту, а також ідентифікації, аналізу, оцінки, дослідження, моніторингу та аналізу ризику .

Встановлення контексту – визначення зовнішніх і внутрішніх параметрів, які необхідно взяти до уваги під час управління ризиками, а також встановлення сфери та критеріїв ризику для політики ризик-менеджменту.

Зовнішній контекст – зовнішнє середовище, в якому організація прагне досягти своїх цілей. Зовнішній контекст може включати:

- середовище – культурне, соціальне, політичне, правове, регулятивне, фінансове, технологічне, економічне, природне, конкурентне або міжнародне, національне, регіональне, або локальне;
- ключові рушійні сили і тренди, що впливають на цілі організації;
- відносини із зовнішніми зацікавленими сторонами, їх сприйняття та оцінка.

Внутрішній контекст – внутрішнє середовище, в якому організація прагне досягти своїх цілей. Внутрішній контекст може включати:

- управління, організаційну структуру, ролі та відповідальність;
- політику, цілі, стратегії, що використовуються для досягнення цілей;
- можливості, розуміння у рамках ресурсів та знань (наприклад, фінанси, час, процеси, системи і технології);
- сприйняття та оцінку внутрішніх зацікавлених сторін;
- інформаційні системи, інформаційні потоки, а також процес прийняття рішень (формальних і неформальних);
- відносини з внутрішніми зацікавленими сторонами, їх сприйняття та оцінка;
- культуру організації;
- стандарти, керівництва і моделі, офіційно прийняті організацією;
- форму та обсяг договірних відносин.

Комунікації і консультації – постійний і повторюваний процес, яким управляє організація для того, щоб надати, поділитися або придбати інформацію, а також для того, щоб розпочати діалог із зацікавленими сторонами та іншими щодо управління ризиками. Інформація може стосуватися суті, природи, ймовірності, строгості, оцінки, прийнятності, обробки або інших

аспектів управління ризиками. Консультація – це двосторонній процес інформаційної комунікації між організацією та її зацікавленими сторонами або іншими сторонами з певного питання, прийняття рішення або визначення напряму за конкретною темою. Консультація – це процес, що впливає на рішення краще, ніж повноваження, а також це вхідні дані для прийняття рішення, а не спільне прийняття рішення.

Зацікавлена сторона – особа або організація, яка може вплинути (або на неї можна вплинути, а також відчувати себе під впливом) на рішення або діяльність. Особа, що приймає рішення, може бути зацікавленою стороною.

Оцінка ризику – загальний процес ідентифікації ризику, аналіз ризику і визначення ступеня ризику.

Ідентифікація ризику – процес знаходження, розпізнавання й опису ризику. Ідентифікація ризику включає ідентифікацію джерел ризику, подій, їх причин і потенційних наслідків. Ідентифікація ризику може включати історичні дані, теоретичний аналіз, інформаційні та експертні опції і потреби зацікавлених сторін.

Джерело ризику – елемент, який сам по собі або в комбінації з іншими має внутрішній потенціал для виникнення ризику. Джерело ризику може бути матеріальним або нематеріальним.

Подія – поява або зміна певних обставин. Подія може являти собою одну або багато обставин і може мати декілька причин. Подія може складатися з того, що не відбувається. Іноді подія може належати до термінів «Інцидент» або «Випадковість». Подія без наслідків також може належати до термінів «часткова удача», «випадок», «загроза події», «небезпечне становище».

Наслідок – результат події, що впливає на цілі. Подія може привести до ряду наслідків. Наслідок може бути визначеним або невизначеним і мати позитивний або негативний вплив на цілі. Наслідки можуть бути виражені якісно і кількісно. Початкові наслідки можуть спричинити за собою більш серйозні.

Ймовірність – можливість того, що щось станеться. В термінології ризик-менеджменту слово «ймовірність» використовується для посилання на можливість, що щось станеться, вимірюється і визначається об'єктивно і суб'єктивно, кількісно та якісно, й описується за допомогою загальних термінів або математично (наприклад, ймовірність або частота в цей період часу). Англійський термін «ймовірність» у багатьох мовах не має прямого еквівалента, в той час як термін «можливість» часто використовується. Незважаючи на це в англійській мові «ймовірність» часто інтерпретується як математичний термін. Отже, у термінології ризик-менеджменту використовується «ймовірність», тому цей термін має більш широку інтерпретацію, ніж «можливість».

Структура ризику – **о**пис будь-якої групи ризиків. Група ризиків може містити такі ризики, які належать до цілої організації, частини організації або інших компонентів.

Аналіз ризику – процес розуміння природи ризику і визначення рівня ризику. Аналіз ризику надає основу для визначення ступеня ризику і для вирішення обробки ризику. Аналіз ризику включає оцінку ризику.

Критерії ризику – дані, за якими оцінюється значущість ризику. Критерії ризику засновані на цілях організації, її зовнішньому і внутрішньому контексті. Критерії ризику можуть бути похідними від стандартів, законів, політики та інших вимог.

Рівень ризику – величина ризику, виражена в рамках комбінації наслідків та їх ймовірностей.

Визначення ступеня ризику – процес порівняння результатів аналізу ризику з критеріями ризику для визначення того, чи можна прийняти величину ризику. Визначення ступеня ризику сприяє обробці ризику.

Обробка ризику – процес модифікації ризику. Обробка ризику може включати: обхідний шлях ризику за допомогою рішення не починати або не продовжувати діяльність, яка провокує появу ризику; збереження або збільшення ризику з метою дослідити обставини; видалення джерела ризику;

зміну ймовірності; зміну наслідків; поділ ризику з іншою стороною або сторонами (включаючи контракти і фінансування ризику); збереження ризику при наявності повної інформації. Обробки ризиків, які мають справу з негативними наслідками, іноді приводять до «зменшення ризиків», «усунення ризиків», «уникнення ризиків» і «редукції ризиків». Обробка ризику може створити нові ризики або модифікувати вже існуючі.

Контроль – вимірювання, здатне змінити ризик. Контроль включає будь–який процес, політику, приладу, практика або інші дії, що модифікують ризик. Контроль не завжди впливає на очікуваний або передбачуваний модифікуючий ефект.

Залишковий ризик – ризик, який залишається після обробки ризику. Залишковий ризик може містити в собі не ідентифікований ризик. Залишковий ризик може також називатися «збережений ризик».

Моніторинг – постійна перевірка, нагляд, критичне спостереження або визначення статусу ідентифікації зміни показників та очікуваних результатів. Моніторинг може бути застосований до концепції ризик-менеджменту, процесу ризик-менеджменту, ризику або контролю.

Аналіз – процес для визначення придатності, адекватності та ефективності виконаних дій для досягнення встановлених цілей. Аналіз може бути застосований до концепції ризик-менеджменту, процесу ризик-менеджменту, ризику або контролю.

Принципи ризик-менеджменту.

Для того щоб управління ризиками було ефективним, організація повинна на всіх рівнях відповідати принципам, перерахованим нижче.

а) *Ризик-менеджмент створює і захищає оцінки.*

Ризик-менеджмент сприяє очевидному досягненню цілей і поліпшенню показників, наприклад, здоров’я та безпеки людини, захисту, відповідності законодавству та регламенту, публічного визнання, захисту навколишнього середовища, якості продуктів, проектного управління, ефективності діяльності, керівництва та репутації.

б) *Ризик-менеджмент – це складова частина всіх організаційних процесів.*

Ризик-менеджмент – є не автономною діяльністю, вона не відокремлена від основної діяльності та процесів організації. Ризик-менеджмент – це частина відповідальності управління і складова частина всіх організаційних процесів, включаючи стратегічне планування та управління процесами проектів і змін.

в) *Ризик-менеджмент є частиною прийняття рішення.*

Ризик-менеджмент допомагає особам, які приймають рішення, зробити правильний вибір, розставити пріоритети і визначити альтернативні курси дій.

г) *Ризик-менеджмент ясно відображає невизначеність*

Ризик-менеджмент враховує невизначеність, природу цієї невизначеності та спосіб їх вираження.

д) *Ризик-менеджмент систематизований, структурований і погоджений за часом.*

Систематичний, структурований і погоджений за часом підхід до ризик-менеджменту сприяє ефективності, а також послідовним, порівняльним достовірним результатам.

е) *Ризик-менеджмент заснований на кращій доступній інформації.*

Вхідні дані для процесу управління ризиками засновані на інформаційних ресурсах, таких, як історичні дані, досвід, зворотний зв’язок зацікавлених сторін, спостереження, прогнози і вислови експертів. Однак особи, які приймають рішення, повинні бути інформовані і брати до уваги будь–які обмеження в даних або використанні моделювання, а також можливість розбіжності думок експертів.

ж) *Ризик-менеджмент особливий для кожної організації.*

Ризик-менеджмент сконцентрований на зовнішньому і внутрішньому контексті організації та структурі ризику.

и) *Ризик-менеджмент враховує людські та культурні фактори.*

Ризик менеджмент розпізнає потенціал, сприйняття та наміри зовнішніх і внутрішніх зацікавлених сторін, які можуть сприяти або заважати досягненню цілей організації.

к) *Ризик-менеджмент володіє транспарентністю та інклюзивністю.*

Відповідне і правильне за часом залучення зацікавлених сторін, зокрема, осіб, які повинні приймати рішення на всіх рівнях організації, гарантує, що ризик-менеджмент залишається релевантним і оновленим. Залучення також дозволяє зацікавленим сторонам бути відповідно представлено й усвідомлювати, що їхні погляди прийняті до уваги при визначенні критеріїв ризику.

л) *Ризик-менеджмент – це динамічний, повторюваний і здатний до змін процес процес де* трапляються внутрішні і зовнішні події, змінюється контекст і знання, мають місце моніторинг та аналіз, виникають нові ризики, отже щось змінюється, а інше зникає. Тому ризик-менеджмент реагує на зміни.

м) *Ризик-менеджмент сприяє постійному поліпшенню організації.*

Організації повинні розвивати і впроваджувати стратегії для поліпшення розвитку їх ризик-менеджменту на ряду з іншими аспектами організації.
Додаток А стандарту ISO 31000 пропонує подальші поради організації з метою зробити управління ризиками більш ефективним.

Концепція

Загальні положення. Успіх менеджменту ризиків залежатиме від ефективності управлінської концепції, що надає основи й угоди, які впроваджуються в організацію на всіх її рівнях. Концепція робить внесок в ефективний ризик–менеджмент шляхом застосування його процесів на різних рівнях і в певних контекстах всередині організації. Така система дає гарантію того, що про інформацію, зібрану під час реалізації процесів ризик-менеджменту, був зроблений доцільний звіт, її покладено в основу прийняття рішень, і це на неї спираються на всіх відповідних організаційних рівнях. Цей

пункт описує невід'ємні компоненти ризик-менеджменту, і те, як вони взаємодіють у повторюваному середовищі, як це показано в рис. 3.2.

Рисунок 3.2. – Взаємозв'язки між компонентами концепції ризик-менеджменту

Мета цієї концепції – не припис до системи менеджменту, а скоріше допомога організації у процесі інтеграції ризик-менеджменту в загальну систему менеджменту.

Таким чином, організації повинні освоїти компоненти концепції для власних потреб. Якщо існуючі практики і процеси управління всередині організації включають компоненти ризик-менеджменту, або якщо організація вже застосовує формальні процеси ризик-менеджменту для певних типів

ризику, все це має бути проаналізовано з критичної точки зору й оцінено щодо цього Міжнародного Стандарту, включаючи інформацію яка міститься у його Додатку А, щоб переконатися в їх доцільності та ефективності.

Доручення та зобов'язання

Введення в ризик-менеджмент і безперервна гарантія його ефективності потребують сильної і виправданої прихильності з боку керівництва організації, а також: доручень та зобов'язань; розробки системи для ризик-менеджменту; розуміння організації та контексту, в якому вона функціонує; встановлення політики ризик-менеджменту; звітності; інтеграції в процеси організації; ресурсів; встановлення внутрішньої комунікації та механізму звітності; встановлення зовнішньої комунікації та механізму звітності; постійного поліпшення концепції; застосування ризик-менеджменту на практиці; застосування системи ризик-менеджменту на практиці; застосування на практиці процесів ризик-менеджменту; моніторингу та оцінки концепції ризик-менеджменту; стратегічного і ретельного планування для досягнення прихильності на всіх рівнях. Керівництву необхідно:

- визначити та затвердити політику ризик-менеджменту;
- бути впевненим у тому, що рівень культури всередині організації та політики ризик-менеджменту відповідають один одному;
- визначити показники ефективності ризик-менеджменту, що відповідають показниками ефективності організації;
- порівняти цілі ризик-менеджменту з цілями і стратегіями організації;
- бути впевненим у своєму відповідно до юридичних та нормативних питань;
- розподілити відповідальності й обов'язок на всіх рівнях організації;
- дати гарантію того, що ресурси, необхідні для ризик-менеджменту, були розподілені;
- донести до всіх зацікавлених сторін переваги ризик-менеджменту;

- бути впевненим у тому, що концепція ризик-менеджменту і раніше залишається доцільною.

Проект концепції ризик-менеджменту

Розуміння організації та її контексту. Перед початком розробки і впровадження концепції ризик-менеджменту важливо оцінити й зрозуміти як зовнішній, так і внутрішній контекст організації, оскільки вони можуть значною мірою вплинути на розробку концепції. Оцінка зовнішнього контексту організації може включати (але не обмежуватися):

а) соціальне і культурне, політичне, законодавче, нормативне, фінансове, технологічне, економічне, природне і конкурентне середовище, як міжнародне, так і національне, регіональне та місцеве;

б) ключові рушійні сили і напрями, що впливають на цілі організації;

в) відносини із зовнішніми зацікавленими сторонами, їх перспективи та цінності.

Оцінка внутрішнього контексту організації передбачає (але не обмежується):

- правління, організаційну структуру, посади та обов'язки;
- політику, цілі та стратегії, яких необхідно досягти;
- можливості – ресурси та знання (наприклад капітал, час, людські ресурси, процеси, системи і технології);
- інформаційні системи, інформаційні потоки і процеси прийняття рішень (формальні і неформальні);
- відносини з внутрішніми зацікавленими сторонами, їх перспективи та цінності;
- культуру всередині організації;
- стандарти, керівництва та моделі, прийняті всередині організації;
- форму й об'єм контрактних відносин.

Встановлення політики ризик-менеджменту. Політика ризик-менеджменту повинна ясно відображати цілі та прихильність організації щодо ризик-менеджменту і відповідати таким критеріям:

- прагненню організації до обробки ризиків;
- зв’язків між цілями організації і політиками, в тому числі політиці ризик-менеджменту;
- відповідальності і обов’язків з обробки ризиків;
- способу, до якого вдаються у вирішенні конфлікту інтересів;
- зобов’язань щодо забезпечення необхідними ресурсами того, хто відповідає за управління ризиками;
- тому, як буде вимірюватися і підтверджуватися ефективність ризик-менеджменту;
- зобов’язань щодо постійної оцінки та поліпшення політики ризик-менеджменту і концепції, або внаслідок якої-небудь події, а також під час зміни якихось обставин, тому що політика ризик-менеджменту повинна управлятися належно.

Відповідальність. Організація повинна дати гарантію того, що існує відповідальність, уповноважені та належний рівень компетенції для управління ризиками, включаючи впровадження та підтримку процесів ризик-менеджменту, а також гарантію доцільності, ефективності та достатності будь-яких методів управління. Цьому може сприяти:

- ідентифікація власників ризику, які відповідальні та уповноважені управляти ризиками;
- ідентифікація осіб, відповідальних за розвиток, застосування і підтримання концепції управління ризиками;
- ідентифікація інших відповідальностей щодо процесів ризик-менеджменту, покладених на персонал усіх рівнів всередині організації ризик-менеджменту;
- встановлення заходів ефективності, а також зовнішніх та/або внутрішніх процесів підтвердження та розгляду керівництвом;
- гарантія визнання на всіх відповідних рівнях.

Інтеграція в процеси організації. Ризик-менеджмент має бути впроваджений у всі практики організації доти, доки він має доречний, ефективний і достатній характер. Процеси ризик-менеджменту повинні стати частиною процесів організації, а ніяк не стояти осторонь від них. Зокрема, ризик-менеджмент має бути впроваджений у політику розвитку, оцінку бізнес- і стратегічного планування, а також у процеси управління змінами.

У всій організації повинен існувати план ризик-менеджменту з метою гарантії того, що політика ризик-менеджменту застосовується до всіх процесів і практик цієї організації. План ризик-менеджменту може бути інтегрований в інші плани організації, наприклад, у стратегічний план.

Ресурси. Організація повинна розподілити необхідні для ризик-менеджменту ресурси. Мають бути розглянуті такі аспекти:

- людські ресурси, навички, досвід і конкурентоспроможність;
- ресурси, необхідні для кожного кроку процесу ризик-менеджменту;
- процеси організації, методи і засоби обробки ризиків;
- документовані процеси та процедури;
- системи менеджменту інформації та знань;
- навчальні програми.

Встановлення внутрішньої комунікації і звітного механізму. Організація повинна встановити внутрішню комунікацію і механізми звітності, для того щоб підтримати процеси контролю і володіння ризиками. Ці механізми повинні давати такі гарантії:

- ключові компоненти концепції ризик-менеджменту і будь-яких подальших модифікацій управляються належно;
- існує зрозуміла система внутрішньої звітності щодо концепції, її ефективності та результатів;
- необхідна інформація, отримана під час застосування ризик-менеджменту, доступна в будь-який час і на відповідних рівнях;
- існують процеси консультації з внутрішніми зацікавленими сторонами.

Механізми повинні, там де необхідно, включати процеси щодо об’єднання інформації за ризиками з безлічі ресурсів, а також враховувати секретність такої інформації.

Встановлення зовнішньої комунікації і звітного механізму. Організація повинна розробити та впровадити план того, як буде відбуватися комунікація із зовнішніми зацікавленими сторонами. Він повинен включати:

- залучення відповідних зовнішніх зацікавлених сторін і гарантію ефективного обміну інформацією;
- систему зовнішньої звітності, щоб відповідати юридичним, нормативним і урядовим вимогам;
- надання відгуків з комунікацій та консалтингу;
- використання комунікації як методу створення атмосфери довіри всередині організації;
- комунікацію із зацікавленими сторонами в разі виникнення кризи або нештатної ситуації.

Механізми повинні, включати процеси щодо об’єднання інформації за ризиками з безлічі ресурсів, як і внутрішніх комунікаціях, а також брати до уваги секретність такої інформації.

Впровадження ризик-менеджменту

Впровадження концепції для управління ризиками. В процесі впровадження концепції організації з управління ризиками ця організація повинна:

- визначити відповідні часові рамки і стратегії для впровадження концепції;
- застосовувати політику ризик-менеджменту і його процеси до процесів всередині організації;
- відповідати юридичним і нормативним вимогам;
- дати гарантію того, що процес прийняття рішень, включаючи розробку та постановку цілей, відповідає результатам процесів ризик-менеджменту;
- проводити ознайомлювальні та навчальні семінари;

- повідомляти зацікавленим сторонам, що концепція ризик-менеджменту залишається доцільною.

Впровадження процесів з управління ризиками. Ризик-менеджмент має бути впроваджений при повній гарантії того, що його процеси, застосовуються відповідно до плану ризик-менеджменту на всіх відповідних рівнях і позиціях організації як частина його практик і процесів.

Моніторинг та аналіз концепції

Для того щоб дати гарантію, що ризик-менеджмент ефективний і продовжує підтримувати продуктивність організації, така організація повинна:

- Вимірювати ефективність ризик-менеджменту щодо показників, які періодично аналізуються на відповідність вимогам;
- Час від часу вимірювати зріст відносно і окремо від плану ризик-менеджменту;
- Періодично з'ясовувати, чи відповідають по колишньому концепція, політика і план ризик-менеджменту вимогам, враховуючи внутрішній і зовнішній контекст організації;
- Вести звіт про ризики і зростанні відповідно до плану ризик-менеджменту, а також про тому, як дотримується політика ризик-менеджменту;
- Аналізувати ефективність концепції ризик-менеджменту.

Постійне поліпшення концепції. Засновані на результатах моніторингу та оцінки повинні прийматися рішення щодо поліпшення концепції ризик-менеджменту, його політики та плану. Такі рішення повинні привести до поліпшення управління ризиками всередині організації та загальної культури управління ризиками.

Процес

Загальні положення. Процеси ризик-менеджменту мають бути:

– невід'ємною частиною менеджменту;
– впроваджено в культуру і практику;
– пристосовані до бізнес–процесів організації.

Процес ризик-менеджменту показаний на рис. 3.3.

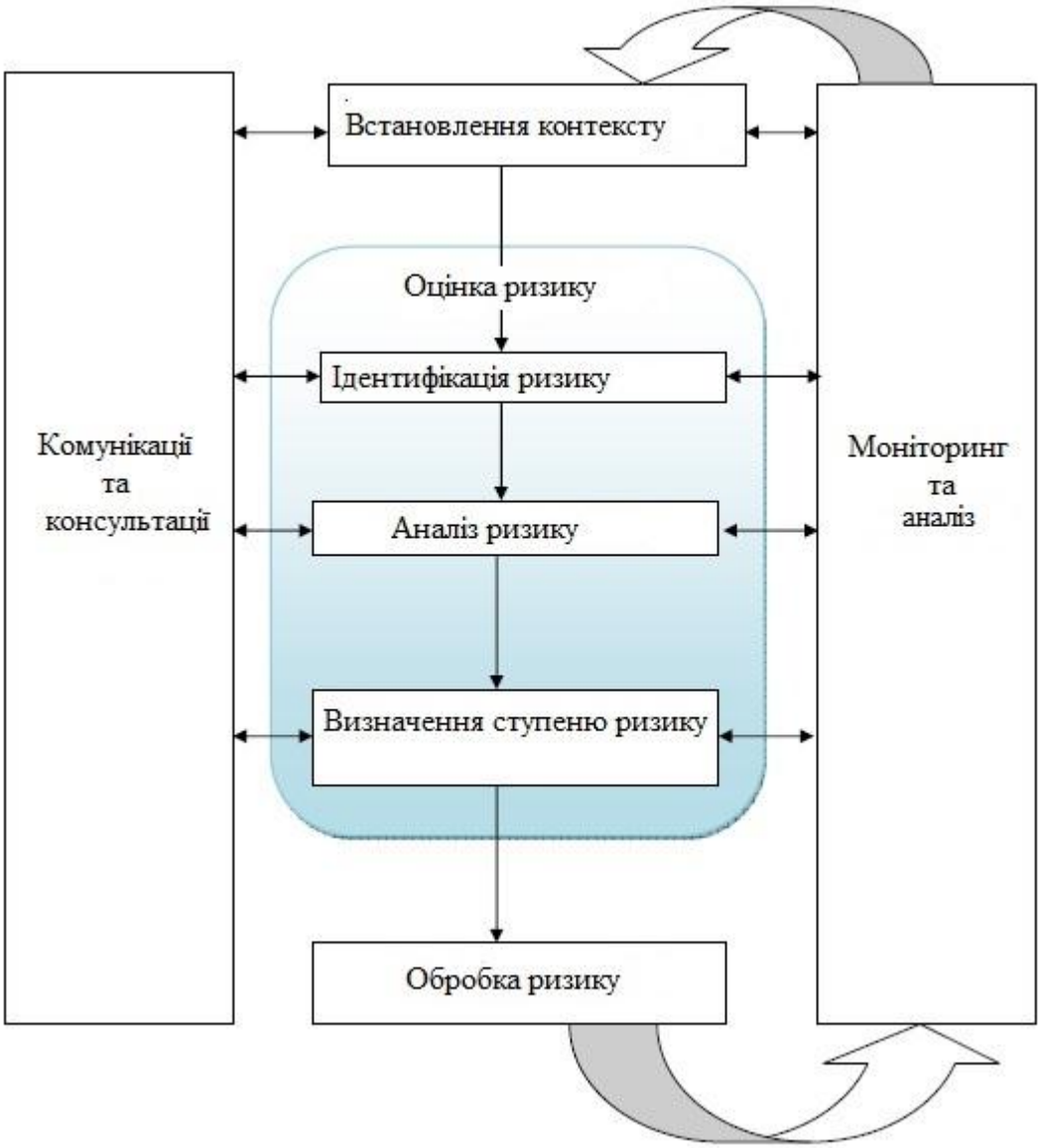

Рисунок 3.3 – Процес ризик-менеджменту

Комунікації та консультації. Комунікації і консультації із зовнішніми і внутрішніми зацікавленими сторонами повинні відбуватися на всіх стадіях процесу управління ризиками. Тому плани щодо комунікації та консультації мають бути розроблені ще в початковій стадії. Вони повинні висвітлювати питання, що стосуються ризиків безпосередньо, їх причин, наслідків (якщо такі відомі), і заходів, яких було вжито з метою обробки такого ризику. Ефективні зовнішні та внутрішні комунікації і консультації повинні давати гарантію що ті, хто відповідальні за процес управління ризиком, і зацікавлені сторони

усвідомлюють підстави для прийняття рішень і причини, того, чому потрібні певні дії.

Консультаційний підхід всередині команди передбачає:

- комунікації і консультації; моніторинг та аналіз;
- оцінку ризику;
- встановлення контексту;
- визначення ступеня ризику;
- аналіз ризику;
- ідентифікацію ризику;
- обробку ризику;
- допомогти в належному встановленні контексту;
- гарантувати, що інтереси зацікавлених сторін зрозумілі і що з ними рахуються;
- гарантувати, що ризики належним чином ідентифіковані;
- зводити різні сфери експертних знань воєдино для аналізу ризиків;
- гарантувати те, що при визначенні критеріїв ризику та їх оціненні, розглядаються різні точки зору;
- забезпечити підтвердження і підтримку плану обробки;
- підвищити доцільність управління змінами під час процесу ризик-менеджменту;
- розробити доцільний план внутрішньої і зовнішньої комунікації.

Комунікації і консультації із зацікавленими сторонами важливі, оскільки вони дають судження про ризик, засновані на їх власному сприйнятті ризику. Ці сприйняття можуть змінитися через різницю в цінностях, потребах, припущеннях, поняттях і очікуваннях зацікавлених сторін. Оскільки їхні погляди можуть істотно вплинути на прийняті рішення, сприйняття зацікавлених сторін, повинно бути ідентифіковано, документовано, і повинно прийматися до уваги при прийнятті рішень.

Комунікації і консультації повинні сприяти обміну достовірною, важливою, точною і зрозумілою інформацією, враховуючи конфіденційні та особисті аспекти її цілісності.

Встановлення контексту

Загальні положення. Встановлюючи контекст, організація ясно формулює свої цілі, визначає зовнішні і внутрішні параметри, які будуть прийняті до уваги при управлінні ризиками, а також встановлює сферу розповсюдження і критерії ризиків для решти процесів. У той час як багато з цих параметрів подібні до тих, які були розглянуті при розробці концепції ризик-менеджменту при встановленні контексту для процесу управління ризиками вони повинні бути розглянуті детально, оскільки належать до процесу управління в сфері конкретного ризику.

Встановлення зовнішнього контексту. Зовнішній контекст – це зовнішнє середовище, в якому організація прагне досягти своїх цілей.

Розуміння зовнішнього контексту важливо для гарантії того, що цілі та очікування зовнішніх зацікавлених сторін будуть розглянуті при розробці критеріїв ризику. Він заснований на контексті всієї організації, але з певними тонкощами у вигляді юридичних і нормативних вимог, сприйняттях зацікавлених сторін та інших аспектах ризику, природних для сфери застосування процесів ризик-менеджменту.

Зовнішній контекст може включати але не бути обмеженим (див. стор.131).

Встановлення внутрішнього контексту. Внутрішній контекст – це внутрішнє середовище, в якому організація прагне досягти своїх цілей.

Процес ризик-менеджменту повинен відповідати культурі, процесам, структурі та стратегіям організації. Внутрішній контекст це щось, що може вплинути зсередини на те, як організація буде управляти ризиками. Він повинен бути встановлений, оскільки:

а) ризик-менеджмент поданий у контексті цілей організації;

б) цілі та критерії певного проекту, процесу або діяльності повинні

розглядатися у світлі цілей організації загалом;

в) деякі організації не можуть визначити можливості для досягнення їх стратегічних, проектних або бізнес-цілей, і це не якнайкраще відбивається на активності, довірі, надійності та цінності організації.

Необхідно розуміти, що таке внутрішній контекст (див. стор. 131).

Встановлення контексту процесу управління ризиками. Повинні бути встановлені цілі, стратегії, сфера застосування і параметри діяльності організації, або тих частин організації, в яких застосовується процес ризик-менеджменту. Менеджмент ризиків повинен проводитися з розглядом необхідності узгодження ресурсної бази, що використовується при обробці ризику.

Необхідні ресурси, обов'язки та уповноважені, записи, які повинні вестися, також необхідно визначити. Контекст процесу ризик-менеджменту буде різнитися зважаючи на потреби організації. Він може включати (але не бути обмеженим):

- визначення цілей і завдань заходів з ризик-менеджменту;
- визначення відповідальностей щодо процесу в ході заходів ризик-менеджменту;
- визначення області застосування, так само як і глибини і ширини заходів щодо ризик-менеджменту, в тому числі необхідні включення і виключення;
- визначення заходів, процесів, функцій, проектів, продукції, послуг або активів щодо часу і розташування;
- визначення взаємовідносин між певним проектом, процесом або діяльністю та іншими проектами, процесу або діями організації;
- визначення методологій оцінки ризиків;
- визначення методу, яким буде оцінюватися ефективність управління ризиком;
- ідентифікацію та встановлення рішень, які необхідно прийняти;

- ідентифікацію, визначення сфери застосування, або складання необхідних досліджень і ресурсів, необхідних для таких досліджень.

Увага до тих чи інших факторів може гарантувати, що застосовуваний процес ризик-менеджменту відповідає обставинам, що склалися, організації і ризикам, що гальмують здійснення організацією її цілей.

Визначення критеріїв ризику. Організація повинна визначити критерії для використання в процесі оцінки значущості ризику. Критерії повинні відображати цінності, цілі і ресурси організації. Деякі критерії можуть бути введені або витягнуті з юридичних і нормативних або ж інших вимог, яких дотримується організація.

Критерії ризиків повинні відповідати політиці ризик-менеджменту організації, мають бути визначені на початку процесу ризик-менеджменту і постійно оновлюватися.

При визначенні критеріїв ризику необхідно розглянути такі фактори:

- природу і тип причин та наслідків, які можуть виникнути, і те, як вони вимірюватимуться;
- як буде визначена ймовірність;
- часові рамки ймовірності та / або наслідків;
- як буде визначено рівень ризику;
- погляди зацікавлених сторін;
- рівень, на якому ризик стає допустимим або прийнятним;
- чи повинні розглядатися комбінації множинних ризиків, і якщо так, то як і які комбінації мають бути розглянуті.

Оцінка ризику

Загальні положення. Оцінка ризику – це загальний процес ідентифікації, аналізу та оцінки ступеня ризику. ISO/IEC 31010 надає керівництво з техніки оцінення ризику.

Ідентифікація ризику. Організація повинна визначити джерело ризику, сфери його впливу, ризикові випадки (включаючи зміну обставин), їх причини, а також їх потенційні наслідки.

Мета цього кроку – скласти вичерпний список ризиків, заснований на тих ризикових випадках, які можуть створити підґрунтя для збільшення можливостей, запобігання, погіршення, скорочення досягнення цілей.

Важливо ідентифікувати ризики, пов'язані з втраченою можливістю. Вичерпна ідентифікація критично важлива, оскільки ризик, який не був ідентифікований на цій стадії, не буде включений у подальший аналіз.

Ідентифікація повинна охоплювати всі ризики (незалежно від того, чи знаходиться їх джерело під контролем організації, чи ні), навіть якщо джерело ризику або його причина неочевидні.

Ідентифікація ризику повинна включати перевірку ланцюгової реакції деяких визначених наслідків, включаючи каскадний ефект і сумарні дії. Вона також має розглядати широкий спектр наслідків, навіть якщо джерело ризику або його причина неясні. Поряд з ідентифікацією можливих наслідків необхідно розглядати можливі причини і сценарії, які можуть вказати на приблизні наслідки. Усі значущі причини мають бути прийняті до уваги.

Організація повинна застосовувати інструменти і техніки ідентифікації ризиків, які відповідають її цілям і можливостям, а також ризикам, з якими вона зіткнулася.

Відповідна та актуальна інформація дуже важлива при ідентифікації ризиків. Вона по можливості повинна включати в себе і загальну інформацію. Працівники, які володіють відповідними знаннями, повинні бути залучені до процесу ідентифікації ризиків.

Аналіз ризику. Щоб проаналізувати ризик, необхідно прийти до його розуміння. Аналіз ризику надає входи для оцінки ступеня ризику й обговорень з питань необхідності проведення обробки ризику, а також стратегій і методів його обробки. Аналіз ризику може також надавати входи для прийняття рішень щодо ризиків різних типів і рівнів, особливо тих, де стоїть вибір.

Аналіз ризиків включає в себе розгляд причин і джерел ризику, його позитивних і негативних наслідків та ймовірності виникнення цих наслідків. Фактори, що впливають на наслідки та ймовірність, й повинні бути визначені. Ризик аналізується шляхом визначення наслідків та їх ймовірності, а також інших супутніх ризику характеристик. Ризиковий випадок може спричинити множинні наслідки і відбитися на безлічі цілей.

Існуючі методи управління, їх ефективність і достатність також необхідно врахувати.

Те, як відбиваються наслідки і ймовірність і те, як вони комбінуються при визначенні рівня ризику, – має відображати тип ризику, доступну інформацію і мету, для якої використовується вихід процесу обробки ризику. Все це повинно відповідати критеріям ризику. Також важливо враховувати незалежність різних ризиків і їх джерел.

Достовірність при визначенні рівня ризику та його чутливості за попередніми умовами і припущеннями повинна бути невід'ємною частиною аналізу і доводитися до відомості тих, хто приймає рішення і, відповідно, зацікавлених осіб. Такі фактори, як розбіжності в думках експертів, невпевненості, доступність, якість, кількість і постійна актуальність інформації, чи обмеження при моделюванні повинні бути чітко сформульовані і виведені на перший план.

Аналіз ризику може бути зроблений з різними видами деталей, залежно від ризику, мети аналізу, та інформації, даних і доступних ресурсів. Аналіз може бути якісним, наполовину кількісним або кількісним, або їх поєднанням, залежно від обставин.

Наслідки і ймовірність їх виникнення можуть бути визначені шляхом моделювання результатів події або набором подій, або екстраполяцією від експериментальних досліджень або на основі наявних даних.

Наслідки можуть бути виражені у вигляді матеріальних і нематеріальних наслідків. У деяких випадках, більш ніж однієї числової величини або дескриптора, обов'язково зазначати наслідки і ймовірність їх для різних часів,

місць, груп або ситуацій. Наслідки і їх вірогідність можуть бути визначені моделюванням результатів ризикового випадку або випадків, або екстраполяцією експериментальних досліджень або доступних даних.

Визначення ступеня ризику. Мета визначення ступеня ризику полягає у прийнятті рішень з його аналізу, заснованого на тому, які ризики необхідно обробити, і пріоритетності у застосуванні обробки.

Визначення ступеня ризику передбачає порівняння рівня, виявленого в процесі аналізу ризику, з критеріями ризику, визначеними при встановленні контексту.

Необхідність обробки розглядається на підставі такого порівняння. Рішення повинні враховувати більш широкий контекст ризику і включати в себе розгляд поміркованості ризику, що має відношення до сторін, за винятком тих організацій, які від ризику тільки виграють. Рішення повинні прийматися відповідно до законодавчих, нормативних та інших вимог.

У деяких обставинах оцінка ступеня ризику може призвести до того, що буде необхідний додатковий аналіз. Також оцінка ступеня ризику може привести до рішення не обробляти ризик, а підтримувати його в існуючому стані.

На таке рішення може вплинути ставлення організації до ризиків та встановленя для нього критеріїв.

Обробка ризику

Загальні положення. Обробка ризику включає в себе одну або більше позицій модифікації ризиків і застосування таких модифікацій.

Як тільки вони були застосовані, методи обробки надають або модифікують способи управління.

Обробка ризику включає циклічний процес:

- оцінки обробки ризику;
- прийняття рішення про допустимість існуючого ризику;
- генерації нового способу обробки, якщо ризик недопустимий;

- оцінки ефективності обробки.

Способи обробки ризику необов’язково виключають один одного і необов’язково доречні за всіх обставин.

Способи можуть включати:

а) уникнення ризику шляхом рішення не починати або не продовжувати діяльність, що призвела до ризику;

б) взяття на себе ризику або підвищення його рівня, щоб використати можливість;

в) знищення джерела ризику;

г) зміну ймовірності;

д) зміну наслідків;

е) розподіл ризику з іншою стороною або сторонами (включаючи контракти і фінансування ризику);

ж) обґрунтоване рішення прийняття на себе страхового ризику.

Вибір опцій обробки ризику. Вибір найбільш доцільної опції обробки ризику передбачає балансування цін і спроб впровадження щодо вигод, згідно з юридичними, нормативними та іншими вимогами, такими як соціальна відповідальність і захист навколишнього середовища. Рішення повинні також врахувати ризики, пов’язані з такою оборобкою, яка не буде виправдана з економічної точки зору, наприклад важкі ризики (що спричиняють вкрай негативні наслідки), але рідкісні (з низькою ймовірністю).

Деякі опції обробки можуть бути прийняті до уваги і здійсненні спільно або окремо. Організація, як правило, може отримати вигоду при застосуванні сукупності опцій обробки ризиків.

При виборі опції обробки ризику організація має враховувати цінності та сприйняття зацікавлених сторін, і найбільш відповідні способи комунікації з ними. Там, де опції обробки ризику можуть вплинути на ризики поза організацією або у відносинах із зацікавленими сторонами, це також потрібно враховувати. І хоча опції обробки ризику однаково ефективні, деякі з них можуть бути більш допустимими для деяких зацікавлених сторін, ніж інші.

План з обробки ризиків повинен ясно ідентифікувати пріоритетний порядок, в якому застосовуватимуться окремі опції обробки ризику.

Обробка ризику сама по собі може спричиняти ризик. Значним ризиком може бути помилка або неефективність заходів обробки ризиків. Моніторинг має бути невід'ємною частиною плану з обробки ризику як гарантія того, що вживаються ефективні заходи.

Обробка ризику може спричинити вторинні ризики, які також необхідно розглядати, обробляти, за якими необхідно стежити й аналізувати. Такі вторинні ризики повинні бути включені в той самий план з обробки ризиків, як і початкові ризики, таким чином немає ніякої необхідності в обробці такого ризику як нового. Зв'язок між двома ризиками необхідно ідентифікувати і підтримувати.

Підготовка і впровадження планів обробки ризику. Мета планів з обробки ризику – документувати те, як вибрана опція обробки ризику буде застосована.

Інформація, яка надається в планах з обробки має включати:

- причини вибору опцій обробки, включаючи очікувані вигоди;
- тих, хто несе відповідальність за ствердження плану, і тих, хто відповідальний за впровадження такого плану;
- пропоновані дії;
- ресурсні вимоги, включаючи нештатні ситуації;
- заходи ефективності та обмеження;
- вимоги щодо звітності та моніторингу;
- часові рамки і плани–графіки.

Плани обробки повинні бути інтегровані з процесами управління всередині організації і мають обговорюватися з зацікавленими сторонами.

Ті, хто приймають рішення, і зацікавлені сторони повинні усвідомлювати природу і ступінь залишкового ризику після його обробки. Залишковий ризик повинен бути документований. До такого ризику має бути застосований моніторинг, оцінка, і, якщо необхідно, додаткова обробка.

Моніторинг та аналіз

Моніторинг, а також оцінка повинні бути сплановані під час процесу ризик-менеджменту і мають підлягати регулярній перевірці та нагляду. Вони можуть мати як періодичний, так і ситуативний характер.

Відповідальності з моніторингу та аналізу мають бути чітко визначені. Процеси організації з моніторингу та аналізу повинні включати всі аспекти процесу ризик-менеджменту з метою:

- гарантії того, що методи управління ефективні і достатні як при розробці, так і при функціонуванні;
- придбання додаткової інформації з метою поліпшення оцінки ризику;
- аналізу та засвоєння уроків із ризикових випадків (включаючи інциденти, зміни, успіхи і провали);
- виявлення змін у зовнішньому і внутрішньому контексті, включаючи зміни в умовах ризику і сам ризик, який може спричинити перевірку обробки ризику і пріоритетів;
- ідентифікації появи ризиків.

Прогрес у застосуванні планів з обробки ризиків є мірою ефективності. Результат може бути включений у загальний менеджмент ефективності всередині організації, вимірювання, зовнішні і внутрішні звітні заходи.

Результати моніторингу та аналізу повинні бути записано і належно доведені до відома зовнішніх і внутрішніх зацікавлених сторін, а також мають бути використані як вхідні для аналізу концепції ризик-менеджменту.

Запис процесів ризик-менеджменту

Заходи з ризик-менеджменту повинні бути доступні для аналізу. У процесі ризик-менеджменту записи є основою поліпшення методів та інструментів, а також процесу в цілому.

Рішення, що стосуються створення записів мають враховувати:

- потреби організації в безперервному навчанні;
- переваги від повторного використання інформації в управлінських цілях;
- витрати і спроби створення та підтримки записів;
- юридичні, нормативні та операційні потреби записів;
- метод оцінки, доступність вилучення та способи зберігання;
- період зберігання;
- конфіденційність інформації.

Властивості поліпшеного ризик-менеджменту [20]

Загальні положення. Всі організації повинні прагнути до високого рівня ефективності концепції ризик-менеджменту, це узгоджується з прийнятими рішеннями. Нижче наведено список ознак високого рівня ефективності в управлінні ризиками. Щоб допомогти організаціям у вимірі їх ефективності щодо цих критеріїв нижче наведені принципові індикатори кожної ознаки.

Ключові виходи. Організація володіє актуальним, правильним і вичерпним розумінням ризиків. Ризики організації відповідають її критеріям ризиків.

Ознаки. Постійне поліпшення. Наголос робиться на постійне поліпшення ризик-менеджменту, шляхом постановки цілей організації, вимірювань, аналізу та подальшої модернізації процесів, систем, ресурсів, можливостей і навичок.

Все це може бути підкреслено існуванням відкритих цілей у сфері продуктивності, що вимірюється в індивідуальній продуктивності організації та окремих її менеджерів. Продуктивність організації може бути виміряна і доведена до відома зацікавлених осіб. Зазвичай аналіз продуктивності має проводитись принаймні раз на рік, а потім відбувається перевірка процесів, постановка перевірених цілей у сфері продуктивності на наступний період.

20. Додаток А стандарту ISO 31000. Свойства улучшенного риск менеджмента. ISO 31000:2009 Международный Стандарт ISO 31000 Первое издание 2009-11-15. Риск Менеджмент – Принципы и руководства.

Така оцінка ефективності ризик-менеджменту – невід'ємна частина всієї оцінки продуктивності організації та системи вимірювань відділів та окремих співробітників.

Повна відповідальність за ризики. Покращений ризик–менеджмент включає всеосяжну, повністю визначену допустиму відповідальність за ризики, методи управління і завдання з обробки ризиків. Уповноважені працівники повною мірою беруть відповідальність, вони володіють достатніми навичками і мають доречні ресурси для перевірки систем управління, моніторингу ризиків, поліпшення управління, а також здатні ефективно доводити ризики до відома внутрішніх і зовнішніх сторін.

Все це може бути відзначено всіма членами організації за умови, що вони повністю обізнані про ризики, методи управління і завдання, за якими вони несуть відповідальність. Зазвичай це записується в посадових інструкціях, базах даних або інформаційних системах. Визначення ролей ризик-менеджменту, обов'язків і відповідальностей має бути частиною програм із уведення посад в організації.

Організація дає гарантію того, що ті, хто несуть відповідальність, повністю забезпечені повноваженнями, часом, навчанням, ресурсами та навичками, достатніми для виконання їх зобов'язань.

Впровадження ризик-менеджменту в процес прийняття рішень. Всі рішення, прийняті всередині організації, незалежно від рівня значущості та важливості, потребують відкритого розгляду ризиків і застосування ризик-менеджменту до певного необхідного ступеня.

Це може бути зазначено записами нарад і рішень з метою показу того, що відкриті обговорення за ризиками були. Більш того, має бути присутня можливість побачити, що всі компоненти ризик-менеджменту подано відповідно до ключових процесів прийняття рішень в організації, наприклад обговорення з приводу розподілу капіталу за головним проектом, за реструктуризацією і змінами всередині організації.

З цих причин науково-методологічний ризик-менеджмент постає в межах організації як основа ефективного управління.

Постійні комунікації. Покращений ризик-менеджмент включає постійні комунікації із зовнішніми і внутрішніми зацікавленими сторонами, включаючи всеосяжне і часте надання звітів з ефективності ризик-менеджменту як частини належного управління.

Це може бути зазначено комунікацією із зацікавленими сторонами як невід'ємна і природна частина ризик-менеджменту. Комунікація постає як двосторонній процес, так, щоб належно поінформовані рішення могли бути прийняті відповідно до рівня ризику та необхідності його обробки щодо встановлених сучасних критеріїв ризику.

Вичерпна і регулярна внутрішня та зовнішня звітність і за значними ризиками, і за ефективністю ризик-менеджменту робить внесок в ефективне управління всередині організації.

Повна інтеграція у структуру управління організації. Ризик–менеджмент розглядається як центральний процес управління в організації, такий, при якому ризики розглядаються у світлі впливу невідповідностей на цілі.

Структура управління та процес засновані на управлінні ризиками. Ефективний ризик-менеджмент вважається керівниками природним засобом досягнення цілей організації. Це підтверджується мовою керівників і важливими письмовими матеріалами організації, що використовує термін «неясності» стосовно до ризиків. Ця ознака також відбивається в політиці організації, особливо тієї, що належить до ризик-менеджменту. Як правило, ця ознака верифікується шляхом проведення інтерв'ю з керівниками та шляхом огляду з дій і тверджень.

Запитання для самоконтролю

1. Які етапи включено до міжнародної системи «Пяти крокова система» оцінки професійних ризиків?

2. Які стандарти входять до групи ISO 31000?

3. Які напрями передбачаються щодо втілення стандарту ISO 31000 ?

4. Чи є обмеження у застосуванні положення стандарту ISO 31000:2009 до певного типу ризиків (за їх походженням, позитивними або негативними наслідками)?

5. Що означає «встановлення контексту» як заходу на початку загального процесу управління ризиками за стандартом ISO 31000:2009?

6. Для чого організації необхідно впровадження Міжнародного стандарту управління ризиками?

7. Які необхідно розглянути фактори при визначенні критеріїв ризику?

8. Що таке ідентифікаціся ризику? Для чого це виконується?

9. Які аналізуються ризики? За якими показниками?

10. Що включає в себе процес обробки ризиків?

11. З якою метою процеси організації з моніторингу та аналізу повинні включати всі аспекти процесу ризик-менеджменту?

12. Для чого необхідно виконувати записи процесів ризик-менеджменту?

13. Що таке повна відповідальність за ризики?

Тема 4. МЕНЕДЖМЕНТ РИЗИКУ. МЕТОДИ ОЦІНКИ РИЗИКУ

4.1. Сфера застосування Міжнародного стандарту ISO / IEC 31010.

4.2. Процес оцінки ризику

4.1. Сфера застосування Міжнародного стандарту ISO / IEC 31010[21]

Практично всі організації стикаються з необхідністю оцінки ризику для зниження кількості небезпечних подій і досягнення поставлених цілей. Цілі організації можуть зачіпати різні аспекти її діяльності: від стратегії до випуску конкретної продукції, розробки процесів і проектів.

Цілі можуть бути визначені у соціальній, екологічній, технологічній, комерційній, фінансовій та економічній галузях, а також у сфері репутації організації, її безпеки і соціального, культурного, політичного впливу на населення.

Всій діяльності організації супутній ризик. Менеджмент ризику допомагає у прийнятті рішень в умовах невизначеності і можливості виникнення подій чи обставин (планових і непередбачених), що впливають на досягнення цілей організації.

Менеджмент ризику включає застосування логічних і системних методів для:

- обміну інформацією та консультацій в сфері ризику;
- встановлення сфери застосування при ідентифікації, аналізі, оцінці та обробці ризику, що відповідає будь-якій діяльності, процесу, функції або продукції;

21. Методи оцінки ризику ISO / IEC 31010: 2009 – Міжнародний стандарт ISO / IEC 31010: 2009 «Менеджмент ризику» («Risk management – Risk assessment techniques»).

- моніторингу та аналізу ризику;
- реєстрації отриманих результатів та складання звітності.

Оцінка ризику є частиною процесу менеджменту ризику і являє собою структурований процес, в рамках якого ідентифікують способи досягнення поставлених цілей, проводять аналіз наслідків та ймовірності виникнення небезпечних подій для прийняття рішення про необхідність обробки ризику.

Оцінка ризику дозволяє відповісти на такі основні запитання:

- які події можуть статися і їх причина (ідентифікація небезпечних подій)?;
- які наслідки цих подій?;
- яка ймовірність їх виникнення?;
- які фактори можуть скоротити несприятливі наслідки або зменшити ймовірність виникнення небезпечних ситуацій.

Крім того, оцінка ризику допомагає відповісти на запитання: рівень ризику є прийнятним, або потрібна його подальша обробка? Цей стандарт заснований на успішному застосовувані методу оцінки ризику і не містить нових, ще не апробованих понять і методів. Цей стандарт є основоположним у сфері менеджменту ризику і призначений для підприємств різних галузей промисловості.

Нормативні документи, що містять методи і критерії оцінки ризику для конкретних галузей, повинні відповідати вимогам цього стандарту. Цей стандарт розроблений на додаток до ІСО 31000 і містить рекомендації щодо вибору і застосування методів оцінки ризику. Оцінка ризику, виконана відповідно до цього стандарту, застосовна при виконанні інших елементів процесу менеджменту ризику.

У цьому стандарті подано методи оцінки ризику і дані посилання на інші міжнародні стандарти, в яких більш докладно описано застосування конкретних методів оцінки ризику. Цей стандарт не призначений для цілей оцінки відповідності та використання обов’язкових або договірних вимог.

Стандарт не містить конкретних критеріїв для прийняття рішення з аналізу ризику та вказівок щодо застосування методів аналізу ризику в конкретній ситуації. Цей стандарт допускає використання інших методів оцінки ризику з урахуванням їх застосовності в конкретній ситуації*.

У цьому стандарті використані нормативні посилання на такі стандарти: Керівництво ІСО 73: 2009 Менеджмент ризику. Словник. Керівні принципи для використання в стандартах (ISO Guide 73: 2009, Risk management – Vocabulary – Guidelines for use in standards) ISO / IEC 31000: 2009 Менеджмент ризику. Загальні принципи і керівництво (ISO 31000: 2009, Risk management – Principles and guidelines).

У цьому стандарті використано терміни та визначення з Керівництва ISO / IEC 73.

Цілі і переваги

Основною метою оцінки ризику є подання на основі об'єктивних свідчень інформації, необхідної для прийняття обґрунтованого рішення щодо способів обробки ризику.

Оцінка ризику забезпечує:

✓ розуміння потенційних небезпек і впливу їх наслідків на досягнення встановлених цілей організації;

✓ отримання інформації, необхідної для прийняття рішень;

✓ розуміння небезпеки і її джерел;

✓ ідентифікацію ключових чинників, що формують ризик, вразливих місць організації та її систем;

✓ можливість порівняння ризику з ризиком альтернативних організацій, технологій, методів і процесів;

✓ обмін інформацією про ризик і невизначеності;

✓ інформацію, необхідну для ранжирування ризику;

* *П р и м і т к а* . Цей стандарт не пов'язаний з аспектами безпеки. Стандарт є основоположним у сфері менеджменту ризику, будь-які посилання на безпеку мають довідковий характер. При настанні чинності вимог безпеки слід керуватися положеннями Керівництва ISO / IEC 51

✓ запобігання нових інцидентів на основі дослідження наслідків інцидентів;

✓ вибір способів обробки ризику;

✓ відповідність правовим і обов'язковим вимогам;

✓ отримання інформації, необхідної для обґрунтованого рішення про прийняття ризику відповідно до встановлених критеріїв;

✓ оцінку ризику на всіх стадіях життєвого циклу продукції.

Оцінка ризику і структура менеджменту ризику

Оцінка ризику, встановлена в цьому стандарті, відповідає структурі і процесу менеджменту ризику, встановленим ІСО 31000.

Структура менеджменту ризику передбачає встановлення політики, процедури та організаційних заходів, спрямованих на впровадження менеджменту ризику в усіх підрозділах організації. Організація повинна офіційно сформулювати політику і стратегію в області менеджменту ризику, а також застосовувати відповідні методи оцінки ризику.

Відповідальні за оцінку ризику повинні знати:

- сферу діяльності і цілі організації;
- рівень прийнятного ризику та способи обробки неприйнятного ризику;
- способи інтеграції процесів оцінки ризику в процеси менеджменту організації;
- методи оцінки ризику та способи їх застосування у процесі менеджменту ризику;
- систему підзвітності, розподілу відповідальності і повноважень в галузі оцінки ризику;
- необхідні і доступні ресурси для виконання оцінки ризику;
- способи реєстрації та аналізу оцінки ризику.

Оцінка ризику і процес менеджменту ризику

Загальні положення

Оцінка ризику є основним елементом процесу менеджменту ризику, що включає відповідно до ІСО 31000 такі елементи:

- обмін інформацією та консультації;
- встановлення сфери застосування менеджменту ризику;
- оцінку ризику (включаючи ідентифікацію ризику, аналіз ризику і порівняльну оцінку ризику);
- обробку ризику;
- моніторинг та аналіз ризику.

Будучи основним елементом процесу менеджменту ризику, діяльність з оцінки ризику має бути інтегрована в інші елементи цього процесу.

Обмін інформацією та консультації

Результативність оцінки ризику залежить від ефективності обміну інформацією та консультацій з причетними сторонами.

Залучення причетних сторін до процесу менеджменту ризику є корисним при:

- розробці плану обміну інформацією;
- визначенні сфери застосування менеджменту ризику;
- вивченні та аналізі інтересів причетних сторін;
- суміщенні та гармонізації різних сфер знань для ідентифікації та аналізу ризику;
- аналізі різних думок в оцінці ризику;
- забезпеченні відповідної ідентифікації ризику;
- забезпеченні схвалення і підтримки плану обробки ризику.

Причетні сторони повинні сприяти обміну інформацією про процес менеджменту ризику з іншими елементами менеджменту, такими, як управління змінами, розробка програм і проектів та управління ними, а також фінансовий менеджмент.

Встановлення сфери застосування менеджменту ризику

При встановленні сфери застосування менеджменту ризику визначають основні параметри управління і критерії процесу менеджменту ризику. При цьому повинен бути проведений аналіз внутрішніх і зовнішніх параметрів сфери застосування, що належать до організації в цілому, а також визначено специфіку оцінюваного ризику. При встановленні сфери застосування менеджменту ризику повинні бути також визначені й узгоджені цілі оцінки ризику, критерії ризику і програма оцінки ризику.

При встановленні сфери застосування менеджменту ризику в рамках процесу оцінки ризику визначають зовнішнє і внутрішнє середовище організації, мету діяльності організації в галузі менеджменту ризику, а також проводять класифікацію небезпечних подій.

Встановлення зовнішньої сфери застосування включає визначення зовнішніх умов, в яких функціонує організація, у тому числі:

✓ зовнішнє середовище, пов'язане з веденням бізнесу, соціальної та екологічної сферами діяльності, правовими та обов'язковими вимогами, культурними факторами, конкуренцією, фінансовим становищем і політикою держави на міжнародному, національному, регіональному або місцевому рівні;

✓ ключові тенденції і мотиви, що впливають на досягнення цілей організації;

✓ значущість зовнішніх причетних сторін та їх сприйняття ризику.

Встановлення внутрішньої сфери застосування включає визначення:

✓ можливостей організації з точки зору ресурсів та інформації в сфері ризику;

✓ інформаційних потоків і процесів прийняття рішень;

✓ внутрішніх причетних сторін;

✓ цілей і завдань організації, а також стратегій, необхідних для їх досягнення;

✓ сприйняття організацією ризику та його значущості для організації;

✓ політики і процесів організації;

✓ стандартів і застосовуваних порівняльних моделей, прийнятих організацією,

✓ структури організації (наприклад, системи управління, розподілу функцій і відповідальності).

Встановлення цілей в сфері менеджменту ризику передбачає:

✓ визначення розподілу обов'язків, відповідальності і підзвітності;

✓ визначення необхідних дій в сфері менеджменту ризику з урахуванням встановлених обмежень і винятків;

✓ визначення розміру й об'єму розглянутих проекту, процесу, функції або діяльності з урахуванням умов обмеження за часом і місцем розташування;

✓ визначення взаємозв'язку розглянутого проекту з діяльністю та іншими проектами організації;

✓ визначення методів оцінки ризику;

✓ визначення критеріїв ризику;

✓ визначення критеріїв оцінки дій в сфері менеджменту ризику;

✓ ідентифікацію та визначення вимог до прийнятих рішень і вживання дій;

✓ визначення, за необхідності досліджень, мети і глибини досліджень, а також необхідних для цього ресурсів.

Визначення критеріїв ризику включає в себе встановлення:

✓ характеру і типу наслідків реалізації небезпечних подій і способів їх оцінки;

✓ методів оцінки ймовірності небезпечної події;

✓ методів встановлення рівнів ризику;

✓ критеріїв прийняття рішень за необхідності обробки ризику;

✓ критеріїв прийнятності ризику;

✓ можливості одночасного виникнення різних видів небезпечних подій і особливості відповідного ризику.

При розробці критеріїв можуть бути використані такі джерела інформації:

✓ цілі процесу менеджменту ризику;

✓ критерії, встановлені у вимогах;

✓ загальні джерела даних;

✓ загальноприйняті в промисловості критерії, такі як рівень загальної безпеки;

✓ рівень ризику організації;

✓ правові, обов'язкові та інші вимоги для обладнання або видів діяльності.

Оцінка ризику

Оцінка ризику – процес, що поєднує ***ідентифікацію***, ***аналіз*** *і* ***порівняльну оцінку ризику.***

Ризик може бути оцінений для всієї організації, її підрозділів, окремих проектів, діяльності або конкретної небезпечної події. Тому в різних ситуаціях можуть бути застосовані різні методи оцінки ризику.

Оцінка ризику забезпечує розуміння можливих небезпечних подій, їх причин та наслідків, ймовірності їх виникнення та прийняття таких рішень:

✓ про необхідність робити відповідні дії;

✓ про способи максимальної реалізації всіх можливостей зниження ризику;

✓ про необхідність обробки ризику;

✓ про вибір між різними видами ризику;

✓ про пріоритетність дій з обробки ризику;

✓ про вибір стратегії обробки ризику, що дозволяє знизити ризик до прийнятного рівня.

Обробка ризику

Після завершення оцінки ризику приймають і виконують одне або декілька рішень про обробку ризику, що дозволяють змінити ймовірність виникнення небезпечної події та / або її вплив. Обробка ризику зазвичай є адаптивним процесом перевірки ризику на його прийнятність і відповідність

раніше встановленим критеріям для визначення необхідності подальшої обробки ризику.

Моніторинг та аналіз

Моніторинг та аналіз ризику є складовою частиною процесу менеджменту ризику. Регулярне проведення моніторингу, аналізу та управління ризиком спрямовані на перевірку:

– достовірності припущень про ризик;

– достовірності припущень, на яких заснована оцінка ризику, включаючи зовнішні та внутрішні сфери застосування;

– досяжності очікуваних результатів;

– відповідності результатів оцінки ризику фактичній інформації про ризик;

– правильності застосування методів оцінки ризику;

– ефективності обробки ризику.

Процеси моніторингу та аналізу ризику повинні бути задокументовані, а результати моніторингу та аналізу ризику – зафіксовані у звіті.

4.2.Процес оцінки ризику

Стислий огляд

Завдяки глибокому дослідженню ризику його оцінка допомагає особам, які приймають рішення, та відповідальним сторонам впливати на досягнення поставлених цілей, а також вибирати адекватні та ефективні засоби управління ризиком. Оцінка ризику є основою для прийняття рішень з обробки ризику. Вихідні дані процесу оцінки ризику є вхідними даними процесів прийняття рішень в організації. Оцінка ризику є процесом, що об’єднує ідентифікацію, аналіз ризику і порівняльну оцінку ризику (рис. 4.1). Спосіб реалізації цього процесу залежить не тільки від сфери застосування процесу менеджменту ризику, але також і від методів оцінки ризику.

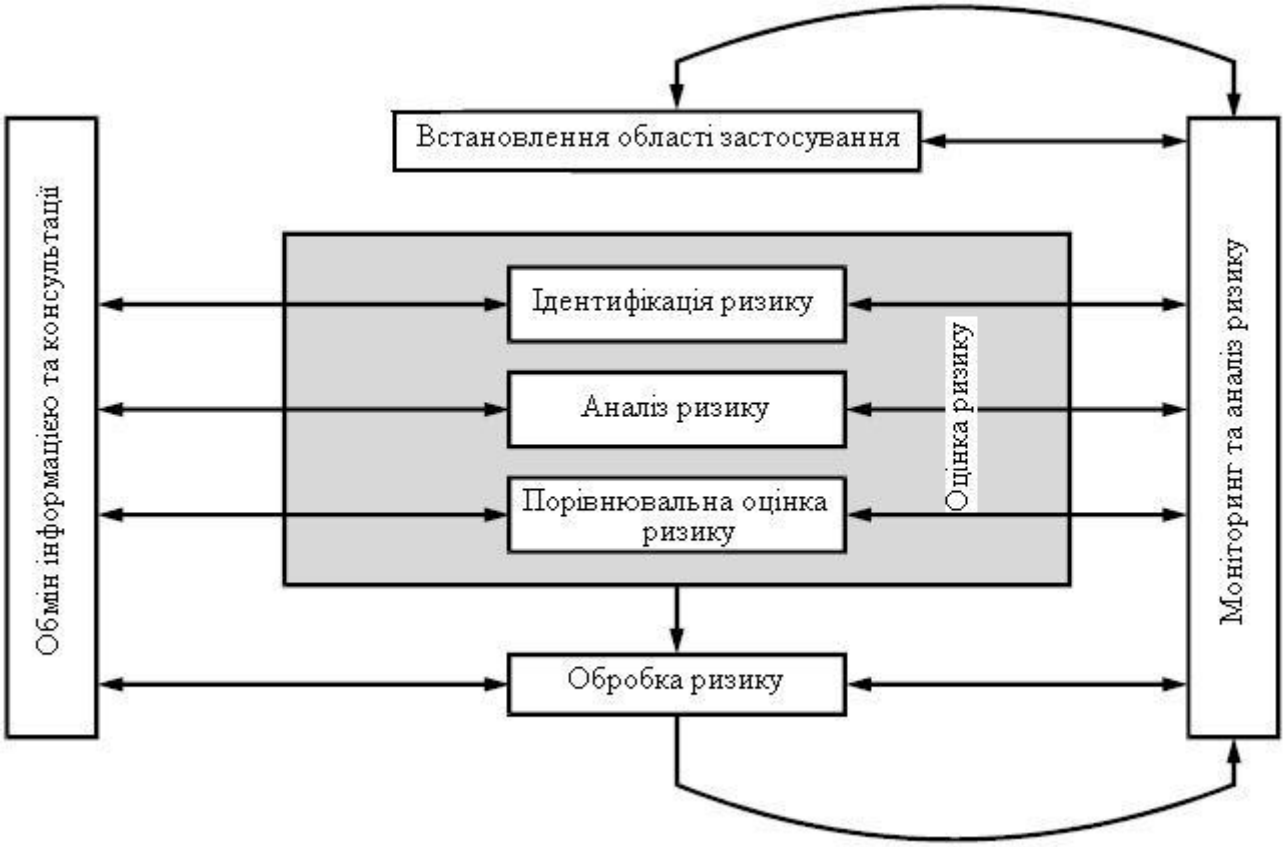

Рисунок 4.1 – Вхідні дані процесу загальної оцінки ризику

При проведенні оцінки ризику може знадобитися застосування мульті дисциплінарного підходу, оскільки ризики можуть потрапляти в широкий діапазон причин і наслідків.

Ідентифікація ризику

Ідентифікація ризику – це процес визначення елементів ризику, складання їх переліку та опису кожного з елементів ризику.

Метою ідентифікації ризику є складання переліку джерел ризику і подій, які можуть вплинути на досягнення кожної з встановлених цілей організації або зробити виконання цих цілей неможливим. Після ідентифікації ризику організація повинна ідентифікувати суттєві особливості проекту, персонал, процеси, системи і засоби управління.

Процес ідентифікації ризику включає ідентифікацію причин і джерел небезпечних подій, ситуацій, обставин чи ризику, які можуть істотно вплинути на досягнення цілей організації і характер цих впливів.

Методи ідентифікації ризику можуть включати:

- методи оцінки ризику на основі документальних свідчень, прикладами яких є аналіз контрольних листів, аналіз експериментальних даних, а також даних і подій, що відбулися в минулому;
- підхід, згідно з яким група експертів слідує встановленому процесу ідентифікації ризику за допомогою структурованої безлічі підказок чи запитань;
- індуктивні методи, такі, як HAZOP.

Для підвищення точності і повноти ідентифікації ризику можуть бути використані різні допоміжні методи, наприклад, метод мозкового штурму і метод **Дельфі**.

Незалежно від фактично використовуваних методів при ідентифікації ризику важливо враховувати людські й організаційні чинники. Відхилення, викликані впливом людських і організаційних чинників, а також небезпечні події, пов’язані з інформаційними технологіями, мають бути враховані в процесі ідентифікації ризику.

Аналіз ризику

Загальні положення. Аналіз ризику включає в себе аналіз і дослідження інформації про ризик. Аналіз ризику забезпечує вхідні дані процесу загальної оцінки ризику, допомагає у прийнятті рішень щодо необхідності обробки ризику, а також допомагає вибрати відповідні стратегії і методи обробки ризику. Аналіз ризику включає аналіз ймовірності та наслідків ідентифікованих небезпечних подій з урахуванням наявності та ефективності застосовуваних методів управління. Дані про ймовірність подій та їх наслідки використовують для визначення рівня ризику.

Також аналіз ризику передбачає дослідження джерел небезпечних подій, їх позитивних і негативних наслідків і ймовірностей появи цих подій. При цьому повинні бути ідентифіковані фактори, що впливають на ймовірність події і її наслідки. Подія може мати множинні наслідки і може впливати на різні цілі. Також мають бути враховані результати застосування та ефективність існуючих методів управління. Різні методи аналізу ризику описані в додатку В Міжнародного стандарту. У складних ситуаціях може бути застосовано кілька методів.

Аналіз ризику зазвичай включає оцінку діапазону можливих наслідків події, ситуації або обставин і відповідних їм ймовірностей для визначення рівня ризику. Проте в деяких випадках, наприклад, коли наслідки незначні, або ймовірність події надзвичайно низька, для прийняття рішень може бути достатньо досліджень тільки одного параметра.

У деяких випадках наслідок може бути результатом реалізації кількох подій або неідентифікованої події. У цьому випадку оцінку ризику необхідно зосередити на аналізі значущості та вразливості компонентів досліджуваної системи. При цьому слід визначити методи обробки ризику, відповідні рівні захисту і стратегії відновлення.

Методи, що використовуються при аналізі ризику, можуть бути *якісними, кількісними* або *змішаними*. Ступінь глибини і деталізації аналізу залежить від конкретної ситуації, доступності достовірних даних і потреб організації, пов’язаних із прийняттям рішень. Деякі методи і ступінь деталізації аналізу можуть бути встановлені відповідно до правових та обов’язкових вимог.

При якісній оцінці ризику визначають наслідки, ймовірність і рівень ризику за шкалою «високий», «середній» і «низький»; оцінка наслідків та ймовірності може бути об’єднана; порівняльну оцінку рівня ризику в цьому випадку проводять згідно з якісними критеріями.

У змішаних методах використовують числову шкалу оцінки наслідків, ймовірності та їх поєднання для визначення рівня ризику за відповідною формулою. Шкали можуть бути лінійними, логарифмічними або побудовані за

іншими принципами. Формули, що використовуються, відповідно можуть бути різними.

При кількісному аналізі оцінюють практичну значущість і вартість наслідків, їх ймовірності і отримують значення рівня ризику в певних одиницях, встановлених при розробці сфери застосування менеджменту ризику. Повний кількісний аналіз не завжди може бути можливий або бажаний через недостатність інформації про аналізовані системи, види діяльності організації, нестачу даних, вплив людського фактора та ін. Або тому що такий аналіз не потрібний, або трудовитрати на кількісний аналіз занадто великі. У такому випадку ранжування ризиків високо кваліфікованими фахівцями може бути більш ефективним.

Якщо застосований якісний аналіз ризику, чіткі пояснення всіх використовуваних термінів і принципів, що лежать в основі критеріїв, повинні бути зареєстровані у вигляді записів.

У разі застосування кількісного аналізу необхідно пам’ятати, що рівні обчисленого ризику є тільки оцінками. Необхідно забезпечити узгодженість невизначеностей отриманих оцінок з рівнем точності і прецизійності методів і даних, що використовуються.

Рівні ризику повинні бути виражені у відповідних термінах для конкретного виду ризику в найбільш зручній формі. У деяких випадках значення ризику може бути виражене у вигляді розподілу ймовірностей діапазону наслідків.

Оцінка методів управління

Рівень ризику залежить від адекватності та ефективності застосовуваних методів управління. Для оцінки методів управління ризиком необхідно відповісти на такі запитання:

- які методи застосовують для зниження конкретного ризику?
- чи справді застосування цих методів приводить до обробки ризику, що забезпечує досягнення прийнятного рівня ризику?

- чи справді ці методи управління ризиком працюють як заплановано, і їх ефективність за необхідності може бути продемонстрована?

Відповіді на ці запитання можна отримати тільки за наявності встановлених в організації документації і процесів.

Рівень ефективності конкретного методу управління або комбінації взаємопов'язаних методів може бути виражений у вигляді якісної, змішаної або кількісної оцінки. У більшості випадків високу точність такої оцінки забезпечити дуже важко. Проте доцільним є застосування заходів підвищення рівня ефективності методу управління ризиком, на основі яких можна зробити висновок про те, які дії необхідні і найкращі для поліпшення управління ризиком або забезпечення різних видів обробки ризику.

Аналіз наслідків

При аналізі наслідків визначають характер і тип впливу, який може відбутися при виникненні конкретної події, ситуації або обставин. Подія може надати декілька впливів різної значущості, вплинути на досягнення декількох цілей і зачепити інтереси причастних сторін організації. Залучені причетні сторони і типи наслідків, які необхідно проаналізувати, визначають при встановленні сфери застосування менеджменту ризику.

Аналіз наслідків може змінюватися від простого опису результатів до деталізованого кількісного моделювання ситуації, процесів та аналізу подразників.

Впливи можуть мати невеликі наслідки, але високу ймовірність появи або значущі наслідки і низьку ймовірність появи, а також будь–який проміжний варіант. У деяких випадках доречно зосередитися на небезпечних подіях із дуже небезпечними наслідками, оскільки саме ці події спричиняють найбільше занепокоєння. В інших випадках важливо проаналізувати окремо наслідки з високою і низькою значущістю для організації. Наприклад, часто повторювані, незначні за впливом події можуть мати великі сукупні або довгострокові

наслідки. Крім того, дії з обробки цих ситуацій ризику найчастіше різні, тому їх корисно проаналізувати окремо.

Аналіз наслідків може включати таке:

- облік існуючих методів управління ризиком, спрямованих на зниження наслідків і всіх супутніх факторів, що впливають на наслідки;
- дослідження взаємозв'язку наслідків небезпечної події та встановлених цілей;
- роздільне вивчення віддалених наслідків події, які відбуваються у теперішній час, якщо вони включені до сфери застосування оцінки ризику;
- розгляд вторинних наслідків, таких, що впливають на взаємопов'язані системи, види діяльності, обладнання або організацію.

Аналіз та оцінка ймовірності

Для оцінки ймовірності зазвичай застосовують такі три загальні підходи, які можуть бути використані як самостійно, так і спільно.

1. Використання відповідних хронологічних даних для ідентифікації події або ситуації, що відбулися в минулому, допускає можливість екстраполяції ймовірності їх появи в майбутньому. Дані, що використовуються, мають належати до досліджуваних систем, обладнання, організації або видів діяльності, а також до вимог діяльності організації. Якщо згідно з наявними даними частота появи події дуже низька, то всі оцінки ймовірності будуть мати високу невизначеність. Це характерно для ситуацій, імовірність появи яких близька до нуля, коли поява події, ситуації або обставин у майбутньому малоймовірна.

2. Використання для оцінки ймовірності методів прогнозування, таких, як аналіз дерева помилок і аналіз дерева подій (додаток В). Якщо хронологічні дані недоступні або недостовірні, то для оцінки ймовірності необхідно провести аналіз системи, діяльності, обладнання або організації та відповідних відмов або працездатних станів. Для оцінки ймовірності основної події числові дані для обладнання, персоналу, організації та систем, отримані на основі

експлуатації та з опублікованих джерел даних, слід використовувати спільно. При застосуванні методів прогнозування важливо забезпечити повноту аналізу загальної причини можливості появи відмов, що включають відмови різних частин або компонентів системи, викликані однією причиною. Для оцінки ймовірності відмов обладнання та систем, а також їх елементів, що спричинені процесами зносу, застосовують методи моделювання, які дозволяють врахувати вплив невизначеності.

3. Використання експертних оцінок у систематизованому і структурованому процесі оцінки ймовірності. Для отримання експертних оцінок слід використовувати всю доступну інформацію, включаючи хронологічні дані, відомості про особливості системи, специфіку організації, експериментальні дані та ін. Існують формалізовані методи отримання експертних оцінок, які допомагають формулювати відповідні запитання. Доступні методи – це методи Дельфі, попарного порівняння, ранжирування за категоріями оцінки й абсолютних оцінок.

Попередній аналіз

Необхідно провести аналіз небезпечних подій, щоб ідентифікувати найбільш істотні види небезпеки, виключити менш істотні або незначні види небезпеки з подальшого аналізу. Основною метою попереднього аналізу є зосередження ресурсів на найважливіших видах небезпечних подій і ризику. Важливо не пропустити події з високою частотою появи й істотним сукупним ризиком.

Аналіз повинен бути заснований на критеріях, встановлених у сфері застосування менеджменту ризику. На етапі попереднього аналізу приймають такі рішення:

- ✓ проводити обробку ризику без подальшої оцінки;
- ✓ виключити з обробки незначні види ризику, обробка яких невиправдана і недоцільна;
- ✓ продовжити більш детальну оцінку ризику.

Вихідні припущення і отримані результати мають бути зареєстровані.

Невизначеність і чутливість. Часто аналізу ризику властива значна невизначеність. Розуміння невизначеності необхідно для ефективної інтерпретації результатів аналізу ризику та відповідного обміну інформацією. Аналіз невизначеності, що відповідає цим методам і моделям, які використовуються для ідентифікації та аналізу ризику, виконує важливу функію. Аналіз невизначеності передбачає з'ясування похибок результатів, спричинених змінами параметрів і припущень. З аналізом невизначеності тісно пов'язаний аналіз чутливості.

Аналіз чутливості передбачає визначення амплітуди змін ризику залежно від змін окремих індивідуальних вхідних параметрів. Такий аналіз застосовують для ідентифікації даних, для яких необхідна висока точність, і даних, до точності яких ризик менш чутливий.

Повнота і точність аналізу ризику мають бути забезпечені настільки, наскільки можливо. Джерела невизначеності повинні бути ідентифіковані для всіх досліджуваних показників, тому слід використовувати всю відому інформацію про невизначеність застосовуваних моделей, методів і даних. Результати аналізу параметрів чутливості мають бути встановлені.

Порівняльна оцінка ризику. Порівняльна оцінка ризику – це зіставлення рівня ризику з критеріями ризику, встановленими при визначенні сфери застосування менеджменту ризику, для визначення типу ризику і його значущості. Порівняльна оцінка ризику використовує інформацію про ризик, отриману при аналізі ризику. Результати порівняльної оцінки ризику застосовують для прийняття рішень про майбутні дії. Етичні, юридичні, фінансові та інші питання, а також сприйняття ризику організацією можуть вплинути на прийняття рішення.

Прийняті рішення можуть стосуватися таких питань:

– необхідності обробки ризику;

– пріоритетів обробки ризику;

– необхідності виконання дій;

– вибору способу обробки ризику.

Характер прийнятих рішень і критерії, що використовуються при прийнятті рішень, встановлено раніше при визначенні сфери застосування, однак на цьому етапі вони мають бути повторно і більш детально розглянуті з позиції вже отриманих даних про ідентифіковані небезпеки і ризики.

Найбільш проста структура для визначення критеріїв ризику – це встановлення одного рівня, який розділяє небезпеки і ризик, що потребують обробки, від тих, які подібних дій не потребують. Застосування такої структури призводить до простих і зрозумілих результатів, проте не відображає невизначеність, властиву оцінці ризику і встановленому примежовому з рівнем ризику.

Рішення про необхідність і способи обробки ризику залежить від витрат і переваг прийняття ризику та поліпшення управління ризиком.

Відповідно до загального підходу слід **розділити ризик на три групи**.

1. *Вища група*, в якій рівень ризику є неприпустимим, безвідносно до переваг прийняття ризику і доходів, одержуваних від діяльності організації, обробка ризику є необхідною незалежно від витрат.

2. *Середня група* («сіра» зона), для якої витрати та переваги прийняття ризику слід враховувати, а можливості – співвідносити з наслідками.

3. *Нижча група*, в якій рівень ризику незначний або настільки малий, що необхідність в обробці ризику відсутня.

Для віднесення ризику до нижчої групи («Низький, наскільки реально можливо» в системі критеріїв ALARP – As Low As Reasonably Practicable (принцип розумної достатності)), що використовується в сфері безпеки, застосовують такий підхід: для низького ризику в середній групі встановлюють змінну шкалу, в якій витрати і переваги можуть бути безпосередньо зіставлені, а можливу шкоду від подій з високим ризиком слід знижувати доти, доки вартість подальшого зниження ризику не перевищить отримані переваги.

Документація

Процес оцінки ризику має бути зареєстрований разом із результатами оцінки. Ризик повинен бути виражений у зрозумілих і точних термінах та одиницях. Необхідний ступінь звітності залежить від цілей і сфери визначення оцінки, за винятком дуже простих випадків документація має містити:

- цілі та сферу застосування;
- опис відповідних систем, її частин і функцій;
- стислий опис зовнішніх і внутрішніх цілей иа сфери діяльності організації у взаємозв'язку з оцінюваними ситуацією системою або обставинами;
- критерії ризику, що застосовуються, і відповідні висновки;
- недоліки, припущення й обґрунтування прийнятих гіпотез;
- методи оцінки;
- результати ідентифікації ризику;
- дані, припущення, їх джерела та валідацію їх використання;
- результати аналізу ризику та кількісну оцінку ризику;
- дані аналізу чутливості та невизначеності;
- критичні припущення та інші фактори, для яких необхідний моніторинг;
- протоколи обговорення результатів;
- висновки та рекомендації;
- посилання.

Якщо оцінка ризику проводиться в рамках безперервного процесу менеджменту ризику, то вона повинна бути виконана і зареєстрована способом, що дозволяє використовувати її результати на всіх етапах життєвого циклу системи, організації, обладнання або діяльності. Оцінка повинна актуалізуватись у міру отримання нової інформації, зміни сфери застосування аналізу ризику та потреб процесу менеджменту.

Моніторинг та повторна оцінка ризику. Процес оцінки ризику висуває на перший план сферу застосування оцінки ризику, а також інші фактори, які

можуть зазнати змін протягом тривалого часу. Передбачення переваги оцінки ризику також можуть змінитися або коригуватися. Такі фактори повинні бути чітко ідентифіковані для процесів безперервного моніторингу і повторної оцінки, щоб оцінка ризику могла оновлюватися в міру необхідності.

Дані моніторингу оцінки ризику повинні бути ідентифіковані і зібрані. Слід проводити моніторинг і реєстрацію ефективності методів управління, що використовуються при аналізі ризику. Повинна бути визначена відповідальність за оформлення та перегляд відповідних свідоцтв та документації.

Застосування оцінки ризику на різних стадіях життєвого циклу. Кожному виду діяльності, проектування і розробки продукції відповідає свій життєвий цикл: від концепції і розробки до стадії повного завершення експлуатації (використання), яка, наприклад, може передбачати демонтаж та утилізацію обладнання.

Оцінка ризику може бути застосована на всіх стадіях життєвого циклу. Зазвичай її багаторазово використовують із різними рівнями деталізації на кожній стадії життєвого циклу для прийняття рішень. Для різних стадій життєвого циклу встановлені різні вимоги і застосовні різні методи оцінки ризику. Наприклад, на стадії концепції і техніко–економічного обґрунтування, коли ідентифікують можливі перспективи застосування продукції, оцінка ризику може бути використана для прийняття рішення про продовження робіт. У ситуації, коли існує кілька варіантів, оцінка ризику може бути використана для оцінки альтернативних способів при прийнятті рішення, що забезпечує найкращий баланс позитивного і негативного ризику.

На стадії проектування та розробки оцінка ризику сприяє:

- забезпеченню допустимого ризику системи;
- вдосконаленню проекту;
- дослідженню економічної ефективності;
- ідентифікації подій, що впливають на подальші стадії життєвого циклу.

Оцінка ризику може бути використана для отримання інформації, необхідної при розробці процедур у нормальних і надзвичайних умовах.

Запитання для самоконтролю

1. Як можуть поділятися цілі організації залежно від діяльності?
2. Які логічні і системні методи із менеджменту ризику застосовуються?
3. На які основні запитання дозволяє відповісти оцінка ризику?
4. Чи розглядає цей стандарт аспекти безпеки?
5. Яка є основна мета оцінки ризику та що вона забезпечує?
6. Які обов'язкові процедури за структурою менеджменту ризику керівництво організації повинно застосувати та довести до усіх своїх підрозділів?
7. Встановлення зовнішньої сфери застосування включає визначення зовнішніх умов. Що до них належить?
8. Що застосовується для визначення та встановлення внутрішньої сфери застосування?
9. Що передбачає встановлення цілей у сфері менеджменту ризику?
10. Що входить до визначення критеріїв ризику?
11. Які складові має процес оцінки ризику?
12. З чого складається процес ідентифікації ризику?
13. Із чого складаються якісні методи оцінки ризиків?
14. Що передбачає та як проводиться кількісний аналіз?
15. Чи залежить рівень ризику від управління підприємством?
16. Що входить до аналізу наслідків ризиків?
17. Із чого складається аналіз та оцінка ймовірності?
18. Для чого проводиться попередній аналіз?
19. Від чого залежить рішення про необхідність і способи обробки ризику? На які групи слід розділити ризик за загальним підходом?
20. Що повинна включати звітність?

Тема 5. ВИБІР МЕТОДІВ ОЦІНКИ РИЗИКУ

5.1. Стислий опис методів оцінки ризику.

5.2. Методи оцінки ризику:

- Мозковий штурм
- Структуровані або частково структуровані інтерв'ю
- Метод Дельфі
- Контрольні листи
- Попередній аналіз небезпек (PHA)
- Дослідження HAZOP
- Аналіз небезпеки і критичних контрольних точок
- Оцінка токсикологічного ризику
- Структурований аналіз сценаріїв методом «що, якщо?». Метод Swift
- Аналіз сценаріїв
- Аналіз впливу на бізнес (BIA)
- Аналіз першопричини
- Аналіз видів і наслідків відмов; аналіз видів, наслідків та критичності відмов (FMEA)
- Аналіз дерева несправностей (FTA)
- Аналіз дерева подій (ETA)
- Аналіз причин та наслідків
- Причинно–наслідковий аналіз (діаграма Ісікави)
- Аналіз рівнів захисту (LOPA)
- Аналіз дерева рішень
- Аналіз впливу людського фактора (HRA)
- Аналіз «краватка–метелик»

- Технічне обслуговування, спрямоване на забезпечення надійності (RCM)
- Аналіз прихованих дефектів і аналіз паразитних кіл (SA)
- Марківський аналіз
- Моделювання методом Монте–Карло
- Байєсівський аналіз і мережа Байєса
- Криві FN
- Індекси ризику
- Матриця наслідків і ймовірностей
- Аналіз ефективності витрат (аналіз «витрат і вигод»)
- Мультикритеріальний аналіз рішень (MCDA)
- Метод Файн–Кінні

5.1. Стислий опис методів оцінки ризику

Загальні положення

У цьому підрозділі наведено опис способів вибору методів оцінки ризику, а також основні методи і прийоми оцінки ризику. У деяких випадках використовують кілька методів оцінки ризику.

Вибір методу. Оцінка ризику може бути виконана з різним ступенем глибини і деталізації з використанням одного або декількох методів різного рівня складності. Форма оцінки та її вихідні дані повинні бути сумісні з критеріями ризику, встановленими при визначенні сфери застосування. У підрозділі подано концептуальні співвідношення між різними категоріями методів оцінки ризику та суттєвими факторами ризику в конкретній ситуації і наведено приклади вибору методу оцінки ризику для конкретної ситуації.

При виборі методу оцінки ризику необхідно враховувати, що метод повинен:

✓ відповідати ситуації, що розглядається, та організації;

✓ надавати результати у формі, що сприяє підвищенню обізнаності про вид ризику і способи його обробки;

✓ забезпечувати простежуваність, відтворюваність і верифікацію процесу та результатів.

Має бути наведено обґрунтування вибору методів оцінки ризику із зазначенням їх прийнятності та придатності. Необхідно забезпечити відповідність використовуваних методів і вихідних даних для об'єднання отриманих результатів різних досліджень.

Після прийняття рішення про виконання оцінки ризику та визначення сфери її застосування слід вибрати методи оцінки ризику на основі:

➢ *мети дослідження*. Цілі оцінки ризику безпосередньо пов'язані з методами, що використовуються. Наприклад, якщо проводиться порівняльне дослідження різних варіантів, то можуть бути застосовані менш деталізовані моделі опису наслідків для аналогічних частин системи;

➢ *відповідальності за прийняті рішення*. У деяких випадках необхідний високий рівень деталізації, щоб прийняти рішення, в інших – достатньо більш загального розуміння;

➢ *типу і діапазону аналізованого ризику*;

➢ *можливих наслідків небезпечної події*. Рішення щодо глибини оцінки ризику повинно відображати початкове сприйняття наслідків (яке, швидше за все, зміниться після завершення попередньої оцінки ризику);

➢ *ступеня необхідних експертиз, людських та інших ресурсів*. Простий правильно застосований метод може забезпечити кращі результати, якщо він відповідає сфері застосування оцінки, ніж складна процедура, виконана з помилками. Зазвичай зусилля з оцінки ризику мають відповідати рівню аналізованого ризику;

➢ *доступності інформації і даних*. Для деяких методів необхідно більше інформації та даних, ніж для інших;

- *потреби в модифікації / оновленні оцінки ризику*. Можливо, в майбутньому оцінка повинна бути змінена / оновлена, і для цього можуть бути застосовані різні методи;
- *обов'язкових і договірних вимог*.

На вибір методу оцінки ризику впливають різні фактори, такі, як доступність ресурсів, характер і ступінь невизначеності даних та інформації, складність методу.

Доступність ресурсів

На вибір методу оцінки ризику впливають такі чинники доступності ресурсів:

- практичний досвід, навички та можливості групи оцінки ризику;
- обмеження за часом та інші ресурси організації;
- доступний бюджет, якщо необхідні зовнішні ресурси.

Характер і ступінь невизначеності інформації. Характер і ступінь невизначеності інформації включають в себе розуміння якості, кількості та повноти інформації про ризик, що аналізується. Розуміння передбачає усвідомлення достатності отриманої інформації про ризик, його джерела і причини, його наслідки для досягнення встановлених цілей. Невизначеність може бути пов'язана з невизначеністю даних і недоліком достовірних даних. Наприклад, для зниження невизначеності можуть бути змінені методи збору даних або способи застосування цих методів в організації. Причиною невизначеності може бути незастосування на місцях ефективних методів збору даних про ризик, що ідентифікується. Невизначеність може бути невід'ємною властивістю зовнішніх і внутрішніх цілей та сфери застосування менеджменту ризику в організації. Доступні дані не завжди забезпечують достовірну основу для прогнозування. Для унікальних видів ризику можуть бути відсутні хронологічні дані, а причетні сторони можуть по–різному інтерпретувати доступні дані про ризик. Особи, які виконують оцінку ризику, повинні розуміти тип і характер невизначеності та оцінити її значення для достовірності оцінки

ризику. Необхідно підтримувати постійний обмін інформацією про ризик з особами, що приймають рішення.

Складність. Завдання оцінки ризику може бути складним, наприклад, оцінка ризику для складної системи не зводиться до оцінки ризику її компонентів без урахування їх взаємодії. У деяких випадках обробка одиничного ризику може мати велике значення через вплив ризику на іншу діяльність. Необхідно розуміти зв'язок послідовних дій і ризику, щоб запобігти ситуації, при якій дії щодо управління одним ризиком призводять до катастрофічної ситуації в іншій сфері. Розуміння складності одиничного ризику або набору ризиків організації вкрай важливо при виборі методу(-ів) оцінки ризику.

Типи методів оцінки ризику. Методи оцінки ризику можуть бути класифіковані різними способами, що забезпечує розуміння їх переваг і недоліків, що наведено у таблиці 5.1. У підрозділі 5.2 дано опис кожного методу оцінки ризику щодо отриманої оцінки та рекомендації відповідно до його застосування в конкретних ситуаціях.

Види методів

Класифікація методів пов'язана з такими етапами процесу оцінки ризику:

- ідентифікація ризику;
- аналіз ризику – аналіз наслідків;
- аналіз ризику – якісна, змішана або кількісна оцінка імовірнісних характеристик ризику;
- аналіз ризику – оцінка ефективності існуючих засобів управління;
- аналіз ризику – кількісна оцінка рівня ризику;
- порівняльна оцінка ризику.

Для кожного етапу процесу оцінки ризику застосовність методу оцінки ризику визначається за шкалою: *точно застосовується*, *застосовується* і *не застосовується* (табл. 5.1).

Факторами, що впливають на вибір методу оцінки ризику, є:

- складність проблеми і методів, необхідних для аналізу ризику;

➢ характер і ступінь невизначеності оцінки ризику, заснованої на доступній інформації, та відповідність цілям;

➢ необхідні ресурси: тимчасові, інформаційні та ін.;

➢ можливість отримання кількісних оцінок вихідних даних.

Для кожного методу рівень відповідності визначається за шкалою: **високий**, **середній** або **низький**.

Таблиця 5.1 – Характеристика застосування методів оцінки ризику

Найменування методу	Процес оцінки ризику					Номер додатка
	Іденти-фікація ризику	Аналіз ризику			Порів-няльна оцінка ризику	
		Наслідки	Ймовірні харак-теристики	Рівень ризику		
Мозковий штурм	SA[1)]	NA[2)]	NA	NA	NA	В 01
Структуровані або частково структуровані інтерв'ю	SA	NA	NA	NA	NA	В 02
Метод Дельфі	SA	NA	NA	NA	NA	В 03
Контрольні листи	SA	NA	NA	NA	NA	В 04
Попередній аналіз небезпеки (PHA)	SA	NA	NA	NA	NA	В 05
Дослідження небезпеки та працездатності (HAZOP)	SA	SA	NA	NA	NA	В 06
Аналіз небезпеки та критичних контрольних точок (HACCP)	SA	SA	NA	NA	SA	В 07
Оцінка токсикологічного ризику	SA	SA	SA	SA	SA	В 08
Структурований аналіз сценаріїв методом «що, як що?» (SWIFT)	SA	SA	SA	SA	SA	В 09
Аналіз сценаріїв	SA	SA	A	A	A	В 10
Аналіз впливу на бізнес (BIA)	A	SA	A	A	A	В 11
Аналіз першопричини (RCA)	NA	SA	SA	SA	SA	В 12
Аналіз видів та наслідків відмов (FMEA)	SA	SA	SA	SA	SA	В 13

Продовження табл. 5.1

Аналіз дерева несправностей (FTA)	A	NA	SA	A	A	B 14
Аналіз дерева подій (ETA)	A	SA	A	A	NA	B 15
Аналіз причин та наслідків	A	SA	SA	A	A	B 16
Причино–наслідковий аналіз	SA	SA	NA	NA	NA	B 17
Аналіз рівнів захисту (LOPA)	A	SA	A	A	NA	B 18
Аналіз дерева рішень	NA	SA	SA	A	A	B 19
Аналіз впливу людського фактора (HRA)	SA	SA	SA	SA	A	B 20
Аналіз «краватка-метелик»	NA	A	SA	SA	A	B 21
Технічне обслуговування, спрямоване на забезпечення надійності	SA	SA	SA	SA	SA	B 22
Аналіз скритих дефектів (SA)	A	NA	NA	NA	NA	B 23
Марківський аналіз	A	SA	NA	NA	NA	B 24
Моделювання методом Монте–Карло	NA	NA	NA	NA	SA	B 25
Байєсівський аналіз і мережа Байєса	NA	SA	NA	NA	SA	B 26
Криві FN	A	SA	SA	A	SA	B 27
Індекси ризику	A	SA	SA	A	SA	B 28
Матриця наслідків та ймовірностей	SA	SA	SA	SA	A	B 29
Аналіз ефективності витрат (CBA)	A	SA	A	A	A	B 30
Мультикритеріальний аналіз рішень (MCDA)	A	SA	A	SA	A	B 31
[1)] SA – точно застосовується. [2)] NA – не застосовується. [3)] A – застосовується.						

5.2. Методи оцінки ризику

Мозковий штурм

Стислий огляд

Метод мозкового штурму – це обговорення проблеми групою фахівців у доброзичливій манері, метою якого є ідентифікація можливих видів відмов і відповідних небезпек, ризику, критеріїв прийняття рішень та/або способів обробки ризику. Термін «мозковий штурм» часто використовують більш широко для позначення будь–якого обговорення в групі. Однак у процесі класичного мозкового штурму застосовують спеціальні методи, коли твердження одних учасників обговорення сприяють виникненню у решти учасників мозкового штурму нових оригінальних ідей.

Метод передбачає стимулювання обговорення, періодичний напрям обговорення групи в суміжні сфери та забезпечення охоплення проблем, виявлених у результаті обговорення.

Область застосування

Метод мозкового штурму може бути використаний самостійно або застосований у поєднанні з іншими методами оцінки ризику. Метод спрямований на заохочення образного мислення учасників і застосовується на всіх етапах процесу менеджменту ризику і всіх стадіях життєвого циклу системи. Цей метод може бути використаний для загального обговорення, коли проблеми тільки ідентифіковані, для більш детального аналізу і для конкретних проблем.

При застосуванні методу мозкового штурму важливе значення надається можливості учасників прогнозувати ситуацію. Тому цей метод особливо корисний при ідентифікації ризику застосування нових технологій, коли відсутні дані або необхідні нові нестандартні способи вирішення проблеми.

Вхідні дані

Команда фахівців, що володіють знанням організації, системи, процесу або методів, які необхідно оцінити.

Процес виконання методу

Процес мозкового штурму може бути формальним або неформальним. Формальний процес мозкового штурму зазвичай більш структурований: учасники заздалегідь підготовлені, точно встановлені мета обговорення і способи оцінки висунутих ідей та отриманих результатів. Неформальний процес мозкового штурму менш структурований і часто має вузькоспеціалізований характер.

У формальному процесі *ведучий* виконує такі дії:

– формулює до обговорення навідні і провокуючі запитання відповідно до обговорюваної проблеми;

– визначає цілі обговорення і пояснює його порядок;

– першим починає обговорення (задає напрям обговорення), а члени команди розглядають висунуті ідеї, намагаючись ідентифікувати якомога більше проблем і рішень. При цьому ніхто не обговорює правильні вони чи ні і необхідність внесення їх до списку. Всі ідеї мають право на внесення до списку, що забезпечує вільне обговорення без заборон і зупинок. Всі вхідні дані беруть і не критикують, тому група швидко просувається в дослідженні і всебічному обговоренні проблеми;

– *ведучий* може направити обговорення в інше русло шляхом залучення нових членів команди, визначати ідеї, що висловлені в одному напрямі, вичерпані або обговорення яких занадто відхилилося від поставлених цілей. Основна мета полягає в необхідності зібрати якомога більше різноманітних ідей для подальшого аналізу.

Вихідні дані

Вихідні дані залежать від стадії процесу менеджменту ризику, на якій застосований метод мозкового штурму, наприклад, на стадії ідентифікації вихідними даними можуть бути переліки небезпечних подій і необхідних засобів управління.

Переваги та недоліки

Перевагами методу мозкового штурму є:

– розвиток в учасників нестандартного мислення, яке допомагає в ідентифікації нових видів ризику знаходити нові рішення;

– залучення до обговорення ключових причетних сторін і, отже, поліпшення процесу обновлення інформації;

– швидкість і легкість застосування методу.

Недоліки методу:

– можливий недолік навичок і знань учасників обговорення для ефективного генерування ідей;

– оскільки метод простий і неструктурований, то важко перевірити всебічність обговорення та підтвердити, що всі небезпеки і види ризику ідентифіковані;

– динаміка обговорення в групі може бути такою, при якій деякі учасники, що володіють цінними ідеями, не проявляють себе, в той час як інші домінують при обговоренні. Цей недолік може бути подоланий шляхом залучення комп'ютерної техніки та використання методу закритих груп або дискусійного форуму. Метод комп'ютерного мозкового штурму допускає анонімну участь, що дозволяє уникнути особистих і політичних розбіжностей учасників. При використанні методу закритих груп ідеї направляються координатору і потім обговорюються членами групи.

Структуровані або частково структуровані інтерв'ю

Стислий огляд

У структурованому інтерв'ю опитуваному ставлять запитання із заздалегідь підготовленого переліку, що заохочують всебічний аналіз ситуації і, таким чином, більш повну ідентифікацію небезпек і ризику. Частково структуроване інтерв'ю аналогічно структурованому, однак воно забезпечує більшу свободу при обговоренні досліджуваної проблеми.

Сфера застосування

Структуровані і частково структуровані інтерв'ю корисні в ситуаціях, коли важко зібрати людей для обговорення або коли вільне обговорення в групі

неможливо. Ці види інтерв'ю найчастіше використовують як частину процесу аналізу ризику для ідентифікації небезпек або оцінки ефективності засобів управління. Вони можуть бути застосовані на всіх стадіях проекту або процесу. Структуровані і частково структуровані інтерв'ю можуть бути використані при зборі вхідних даних для оцінки ризику причетними сторонами.

Вхідні дані

Вхідні дані включають:

– точне визначення цілей інтерв'ю;

– список опитуваних, який повинен бути складений з урахуванням інтересів залучених причетних сторін;

– перелік запитань.

Процес виконання методу

Спочатку необхідно скласти перелік запитань, що направляють роздуми опитуваного. Запитання мають бути, наскільки можливо, простими, викладені зрозумілою для опитуваного мовою і охоплювати тільки одну проблему. Відповіді на запитання не повинні бути обмежені за часом. Запитання, спрямовані на роз'яснення відповідей, повинні бути підготовлені заздалегідь.

Потім запитання мають бути запропоновані опитуваноїй особі. При уточненні відповіді повинні бути обмеження за часом. Необхідно стежити за тим, щоб постановка запитання не підказувала опитуваному певну відповідь.

При аналізі відповідей необхідно проявляти гнучкість і забезпечити можливість дослідження сфер, пропонованих опитуваними у своїх відповідях.

Вихідні дані

Вихідними даними є інформація про сприйняття причетними сторонами проблем, які є предметом інтерв'ю.

Переваги та недоліки

Переваги структурованого інтерв'ю:

– аналізування проблеми опитуваними;

– обмін інформацією «один на один» дозволяє розглянути проблему з усіх сторін;

– можливість залучити до обговорення проблеми більшу кількість причетних сторін, ніж при методі мозкового штурму, в якому задіяна відносно невелика група осіб.

Недоліки включають таке:

– структуроване інтерв'ю потребує великих витрат часу інтерв'юера для отримання й обробки різноманітних і численних думок про проблему;

– метод допускає упередженість і небажання обговорювати проблему в групі;

– при використанні методу важко застосувати способи стимулювання і фантазії людини, які є особливістю мозкового штурму.

Метод Дельфі

Стислий огляд

Метод Дельфі призначений для отримання узагальненої думки групи експертів. Хоча цей термін сьогодні часто використовують більш широко у всіх формах мозкового штурму, істотною особливістю методу Дельфі є те, що експерти висловлюють свою думку індивідуально й анонімно, при цьому маючи можливість дізнатися думки інших експертів.

Сфера застосування

Метод Дельфі може бути застосований на всіх стадіях процесу менеджменту ризику або всіх етапах життєвого циклу системи, скрізь, де необхідні узгоджені оцінки експертів.

Вхідні дані

Варіанти рішень проблеми, для відбору яких необхідна узгоджена єдина думка.

Процес виконання методу

Процес включає в себе проведення частково структурованого анкетного опитування групи експертів.

При цьому експерти не повинні зустрічатися один з одним, що дозволяє забезпечити незалежність їхніх думок.

Має бути виконана така процедура:

– формування групи виконання та моніторингу процесу Дельфі;

– вибір групи експертів (можуть бути сформовані одна або декілька груп фахівців);

– розробка початкового переліку запитань;

– тестування переліку запитань;

– відправлення переліку запитань індивідуально кожному учаснику дискусії;

– аналіз та узагальнення відповідей експертів і поширення результатів серед учасників дискусії;

– повторне опитування учасників дискусії та повторення процесу доти, доки не буде досягнута згода з обговорюваної проблеми.

Вихідні дані

Єдина думка з проблеми.

Переваги та недоліки

Переваги методу включають таке:

– оскільки процедура є анонімною, більш імовірно, що будуть виражені непопулярні думки;

– всі погляди на проблему рівнозначні, що дозволяє уникнути домінування думки окремих осіб;

– отримання прав власності на вихідні дані;

– учасники обговорення не повинні знаходитися в одному конкретному місці у конкретний час.

Недоліки методу:

– метод Дельфі є трудомістким і витратним за часом;

– учасники повинні точно і ясно висловити свої думки в письмовій формі.

Контрольні листи

Стислий огляд

Контрольні листи являють собою переліки небезпек, ризику або відмов засобів управління, які зазвичай розробляють на основі отриманого раніше досвіду, результатів попередньої оцінки ризику або результатів відмов, що сталися в минулому.

Сфера застосування

Контрольний лист може бути використаний для ідентифікації небезпек і ризику або оцінки ефективності засобів управління. Контрольні листи можуть бути використані на всіх стадіях життєвого циклу продукції, процесу або системи. Контрольні листи можуть бути використані як частина інших методів оцінки ризику, проте вони найбільш корисні для перевірки повноти розгляду досліджуваної проблеми після застосування більш образних і творчих методів при ідентифікації нових проблем.

Вхідні дані

Попередня інформація та експертні оцінки з проблеми, що забезпечують вибір запитань та розробку значущого контрольного листа (бажано затвердженого).

Процес виконання методу

Повинна бути виконана така процедура:

- визначення сфери застосування;
- складання контрольного листа так, щоб він охоплював всю сферу застосування. Контрольні листи мають бути ретельно складені для досягнення поставленої мети. Наприклад, складений раніше контрольний лист не може бути використаний при ідентифікації нових небезпек або ризику;
- особа або група осіб повинні застосовувати контрольний лист послідовно до кожного елементу процесу або системи для визначення того, чи подано цей елемент у контрольному листі.

Вихідні дані

Вихідні дані залежать від стадії процесу менеджменту ризику, на якій застосовані контрольні листи. Наприклад, вихідними даними можуть бути переліки неадекватних засобів управління або переліки небезпек.

Переваги та недоліки

Переваги методу контрольних листів:

– контрольні листи можуть використовувати особи, які не є експертами;

– якщо контрольні листи добре розроблені, то вони об'єднують різноманітні види експертних оцінок у просту для використання форму оцінки;

– контрольні листи забезпечують те, що основні проблеми не упущені.

Недоліки методу контрольних листів:

– робота з контрольними листами часто стримує свободу думок при ідентифікації небезпек;

– контрольні листи використовують для дослідження «відомих знань», але не «відомого незнання» або «невідомого незнання»;

– застосування контрольних листів заохочує формальну поведінку персоналу за принципом «поставити галочку»;

– метод контрольних листів заснований на спостереженнях, тому існує стійка тенденція не бачити або не помічати проблеми.

Попередній аналіз небезпек (PHA)

Стислий огляд

PHA (Preliminary Hazard Analysis) є простим індуктивним методом аналізу, мета якого полягає в ідентифікації небезпек, небезпечних ситуацій і подій, які можуть порушити роботу або завдати шкоди цьому виду діяльності, обладнанню або системі.

Сфера застосування

PHA зазвичай виконують на ранніх стадіях розробки проекту в умовах нестачі інформації про деталі проекту або робочих процесів. PHA часто передує подальшим дослідженням або спрямований на отримання інформації

для розробки вимог до проектованої системи. PHA також може бути корисний при аналізі існуючих систем, спрямованому на ранжирування небезпек і ризику для подальшого аналізу ризику.

Вхідні дані

Вхідні дані включають в себе:

- інформацію щодо оцінюваної системі;
- деталі проекту системи, які доступні і стосуються справи.

Процес виконання методу

Перелік небезпек, загальних небезпечних ситуацій та ризику формують на основі такої інформації:

- дані про матеріали що використовуються чи виготовляються, їх хімічної або іншої активності;
- перелік обладнання, що використовується;
- відомості про робоче середовище;
- схема розташування обладнання;
- відомості про взаємодію компонентів системи та ін.

Для ідентифікації ризику і подальшої оцінки може бути виконано якісний аналіз наслідків небажаної події та їх ймовірностей.

PHA слід повторювати в міру проходження стадій проектування, розробки і випробувань для виявлення нових небезпек і внесення необхідних змін. Отримані результати можуть бути подані у вигляді таблиці або у вигляді «дерева».

Вихідні дані

Вихідні дані включають в себе:

- ✓ перелік небезпек і відповідного ризику;
- ✓ рекомендації щодо прийняття ризику, рекомендовані засоби управління, вимоги до конструкції або запит на виконання більш детальної оцінки.

Переваги та недоліки

Переваги методу:

- метод PHA можна використовувати в ситуації обмеженої інформації;
- метод PHA дозволяє досліджувати ризик на ранніх стадіях життєвого циклу системи.

Недоліки методу:

- метод PHA надає тільки попередню інформацію;
- метод PHA не є всебічним методом і не може забезпечити детальну інформацію про небезпечні події та способи їх запобігання.

Дослідження HAZOP

Стислий огляд

Абревіатура HAZOP означає дослідження небезпеки і працездатності (Hazard and Operability Study). Дослідження HAZOP є структурованим і систематизованим аналізом продукції, запланованим для існуючого процесу, процедури або системи. Дослідження HAZOP є методом ідентифікації небезпек і ризику для людей, устаткування, навколишнього середовища та/або досягнення цілей організації. Від групи дослідження HAZOP зазвичай очікують по можливості конкретних рішень з обробки ризику.

HAZOP є якісним методом, заснованим на використанні керуючих слів, які допомагають зрозуміти, чому мета проектування або умови функціонування не можуть бути досягнуті на кожному етапі проекту, процесу, процедури або системи. Дослідження HAZOP зазвичай виконує міждисциплінарна група протягом кількох засідань.

Дослідження HAZOP, подібно методу FMEA, спрямоване на ідентифікацію видів відмов процесу, системи або процедури, їх причин та наслідків. Відмінність дослідження HAZOP від методу FMEA полягає в тому, що при застосуванні дослідження HAZOP розглядають небажані результати та відхилення від намічених результатів і умов для пошуку можливих причин і видів відмови, тоді як у методі FMEA аналіз починають з ідентифікації видів відмови.

Сфера застосування

Дослідження HAZOP спочатку було розроблено для аналізу системи хімічних процесів, але згодом сфера його застосування була розширена для застосування в технічних системах і складних виробництвах. Сфера застосування методу включає в себе механічні та електронні системи, процедури, системи програмного забезпечення, організаційні зміни, розробку та аналіз юридичних документів (наприклад, контрактів) та ін. Процес дослідження HAZOP може бути застосований при будь–яких змінах конструкції, компонента(-ів), розроблених процедур і дій людини.

Дослідження HAZOP широко використовують для аналізу програмного забезпечення. Якщо його застосовують до управління безпекою критичних видів обладнання та комп'ютерних систем, то метод позначають CHAZOP (Дослідження управління небезпекою і працездатністю або дослідження комп'ютерної небезпеки і працездатності – Control Hazards and Operability Analysis).

Дослідження HAZOP зазвичай роблять на стадії деталізації конструкції, коли повна схема наміченого процесу вже розроблена, проте ще можна внести необхідні зміни. З іншого боку, дослідження HAZOP може бути застосоване послідовно з різними керуючими словами на кожній стадії проектування і розробки. Воно також може бути виконано на стадії виробництва, однак на цій стадії внесення змін за результатами досліджень може бути більш витратним.

Вхідні дані

Основними вхідними даними дослідження HAZOP є: поточна інформація про системи, що досліджуються, процеси або процедури, а також цілі та функціональні вимоги до проекту. Вхідні дані можуть містити: креслення, перелік вимог, технологічні карти, схеми управління процесом і відповідних логічних зв'язків схеми розміщення обладнання, процедури функціонування та технічного обслуговування, плани дій в аварійних ситуаціях. Якщо HAZOP не пов'язаний з програмним забезпеченням, то вхідними даними можуть бути будь–які документи, що описують функції та елементи досліджуваних систем

або процедур. Наприклад, вхідними даними можуть бути: діаграма організаційної структури і опис відповідальності та обов'язків персоналу, проект договору або процедури.

Процес виконання методу

У процесі дослідження HAZOP розглядають проект і вимоги до процесу, що досліджується, процедури або системи, які підрозділяють їх на частини і проводять аналіз кожної з цих частин, щоб виявити, які відхилення від наміченого виконання можуть статися, що може бути причиною можливих відхилень і яка ймовірність їх наслідків. Цих цілей досягають шляхом систематичного дослідження того, як кожна частина системи, процесу або процедури реагує на зміни основних параметрів при використанні відповідного керуючого слова. Керуючі слова можуть бути підібрані для конкретної системи, процесу або процедури, або можуть бути використані загальні керуючі слова, що охоплюють всі типи відхилень.

У табл. 5.2 наведено приклади часто використовуваних керуючих слів для технічних систем. Подібні керуючі слова, такі, як «занадто рано», «занадто пізно», «більше», «менше», «занадто довго», «занадто швидко», «неправильний напрямок», «неправильна мета», «неправильна дія» можуть бути використані для ідентифікації помилок оператора.

Таблиця 5.2 – Приклад керуючих слів дослідження HAZOP

Терміни	Визначення
Не або ні	Повне заперечення цілей проекту
Більше (вище)	Кількісне збільшення значень параметрів вихідних даних або робочих умов
Менше (нижче)	Кількісне зменшення значень параметрів
Так само, як	Кількісне збільшення (наприклад, додатковий матеріал)
Частина (в суміші)	Кількісне зменшення (наприклад, тільки один або два компоненти
Заміна/Навпроти	Логічна протилежність (наприклад, протитечія)

Продовження табл. 5.2

Інший	Повне заперечення цілей проекту, результати прямо протилежні (наприклад, оплавлення або недоречний матеріал)
Сумісний	З матеріалом або навколишнім середовищем Фізичні властивості матеріалу або процесу Фізичні умови, такі як температура, швидкість

Керуючі слова застосовуються до таких параметрів: зазначене призначення компонента системи або проекту (наприклад, передача інформації), експлуатаційні аспекти.

Етапи дослідження HAZOP передбачають:

- призначення особи, наділеної необхідною відповідальністю та повноваженнями для проведення дослідження HAZOP і забезпечення будь–яких дій, спрямованих на повне завершення цього процесу;
- визначення цілей і сфери застосування дослідження;
- встановлення набору ключових і керуючих слів для дослідження;
- формування групи HAZOP. В цю групу зазвичай включають експертів з основних та суміжних дисциплін, проектувальників і виробничий персонал, здатних провести відповідну технічну експертизу й оцінити вплив відхилень від наміченого або існуючого проекту. Рекомендується включати в групу персонал, який безпосередньо не залучений до роботи щодо розглянутих проекту, системи, процесу чи процедури;
- визначення необхідної документації.

На нараді група HAZOP проводить такі дії:

- поділяє систему, процес або процедуру на менші елементи, підсистеми, підпроцеси, компоненти для проведення їх аналізу;

- погоджує завдання проекту для кожної підсистеми, підпроцесу або компонента, і потім для кожного елемента підсистеми або компонента застосовує керуючі слова, одне за одним, що дозволяє виявити можливі відхилення, які можуть призвести до небажаних результатів;
- у разі ідентифікації небажаних результатів погоджує причину і наслідки для кожної події і пропонує способи їх обробки, що спрямовані на запобігання їх повторної появи або пом'якшення можливих наслідків, якщо вони неминучі;
- реєструє та ідентифікує протоколи обговорень і запропонованих способів обробки ризику.

Вихідні дані

У процесі HAZOP час обговорення по кожному пункту дослідження має бути зареєстрований.

Записи повинні включати в себе: керуюче слово, що використовується, відхилення, його (їх) можливі причини, запропоновані дії з ідентифікованих проблем і відповідального за ці дії. Для будь–якого відхилення, яке не можна виправити, необхідно оцінити його ризик.

Переваги та недоліки

Дослідження HAZOP має такі переваги:

- метод забезпечує систематичне і повне дослідження системи, процесу або процедури;
- до роботи залучаються експерти з суміжних напрямів діяльності, включаючи фахівців, що мають практичний виробничий досвід роботи, яким, ймовірно, доведеться впроваджувати рекомендації з обробки ризику;
- метод допомагає у виборі рішення і способів обробки ризику;
- метод застосовують до широкого діапазону систем, процесів і процедур;
- метод дозволяє точно розглянути причини і наслідки помилок виконавців.

У рамках процесу HAZOP проходить реєстрація всіх записів, що дозволяє забезпечити об’єктивні свідчення для подальшого аналізу.

Недоліки дослідження HAZOP:

- детальний аналіз може бути тривалим за часом і тому бути дорогим;
- детальний аналіз потребує наявності докладної документації та вимог до систем, процесів або процедур;
- дослідження HAZOP може бути зосереджено на знаходженні детальних рішень, а не на перегляді використаних основних припущень (цей недолік можна пом’якшити поетапним застосуванням методу);
- обговорення може бути зосереджено на окремих проблемах проекту і не торкатися широких або зовнішніх проблем;
- метод обмежений завданнями проекту, сферою та цілями дослідження, визначеними для групи;
- метод заснований на експертних оцінках проектувальників, яким може бути складно встановити недоліки своїх проектів.

Посилання на стандарт

МЕК 61882. Дослідження небезпеки і працездатності (HAZOP). Керівництво з застосування.

Аналіз небезпеки і критичних контрольних точок

Стислий огляд

Метод аналізу небезпеки і критичних контрольних точок (HACCP – *Hazard Analysis and Critical Control Points* іноді називають «Аналіз ризиків і критичних контрольних точок»). Він дозволяє побудувати структуру ідентифікації небезпек і перевірки засобів управління у всіх частинах процесу. Цей метод спрямований на захист від небезпек і забезпечення високої надійності і безпеки продукції. Основною метою HACCP є мінімізація ризику шляхом застосування засобів управління в процесі виробництва продукції, а не тільки при контролі кінцевої продукції.

Сфера застосування

Спочатку метод HACCP був розроблений для забезпечення якості продуктів харчування в космічній галузі. Сьогодні цей метод зазвичай використовують організації харчової промисловості для управління ризиком фізичного, хімічного або біологічного забруднення харчових продуктів. Метод HACCP також використовують при виготовленні фармацевтичних препаратів і медичних пристроїв. Принцип ідентифікації факторів, які можуть вплинути на якість продукції, і використання контрольних точок виробничого процесу, де є необхідний моніторинг критичних параметрів і можливих небезпек, може бути також застосовано в інших технічних системах.

Вхідні дані

Застосування методу HACCP починають зі складання технологічної карти або блок–схеми процесу та збору інформації про небезпеки, які можуть вплинути на якість, безпеку або надійність процесу і кінцевої продукції. Інформація про небезпеки, відповідний ризик і способи їх контролю являє собою вхідні дані HACCP.

Процес виконання методу

Метод HACCP заснований на таких принципах:

– ідентифікації небезпек і відповідних запобіжних дій;

– визначення контрольних точок процесу, в яких можна усунути небезпеку або контролювати їх виникнення (критичні контрольні точки, або HACCP);

– встановлення критичних меж при контролі виникнення небезпек, тобто для кожної критичної контрольної точки необхідно встановити діапазон зміни параметрів;

– моніторингу критичних меж для кожної критичної контрольної точки;

– визначення коригувальних дій, якщо параметри процесу вийшли за встановлені межі;

– встановлення процедур верифікації;

– впровадження процедур управління записами і документацією на кожному етапі процесу.

Вихідні дані

Зареєстровані записи, включаючи карти аналізу небезпек і план НАССР, являють собою вихідні дані НАССР.

До карти аналізу небезпек для кожного етапу процесу мають бути включені:

– небезпеки, які можуть бути новими, контрольованими або зростаючими на певному етапі процесу;

– оцінка значущості ризику даних небезпек (така оцінка ризику заснована на розгляді наслідків та ймовірності небезпечної події і є результатом поєднання отриманого раніше досвіду, отриманих експериментальних даних і даних опублікованих джерел);

– висновок про значущість сукупного ризику;

– можливі запобіжні дії для кожної небезпеки;

– можливість застосування моніторингу або контролю виникнення небезпеки на певному етапі (підтвердження того, що точка є критичною контрольною точкою).

План НАССР містить супровідні процедури, застосування яких забезпечує управління ризиком конкретного проекту, продукції, процесу або процедури. План НАССР передбачає перелік всіх критичних контрольних точок із зазначенням для кожної контрольної точки:

– критичних меж, що допускають проведення запобіжних дій;

– дій щодо виконання моніторингу та безперервного контролю (в тому числі коли, хто і яким способом виконує моніторинг);

– необхідні коригувальні дії при виявленні порушення критичних меж;

– способу верифікації та дій з реєстрації записів.

Переваги та недоліки

Переваги методу:

– метод HACCP – це структурований процес, який забезпечує документовані свідоцтва якості ідентифікації небезпеки, управління та зниження ризику;

– метод HACCP орієнтований на вирішення практичних питань: як і де в процесі можна попередити появу небезпек і управляти ризиком;

– метод HACCP дозволяє управляти ризиком у процесі виробництва, не покладаючись тільки на контроль готової продукції;

– метод HACCP дає можливість ідентифікувати небезпеки, спричинені діями людини, і містить спосіб управління в момент вчинення помилкової дії або згодом.

Недоліки методу:

– для застосування методу HACCP необхідно, щоб небезпеки були ідентифіковані і визначено відповідний їм ризик. Також повинні бути визначені необхідні засоби управління. У процесі застосування методу HACCP необхідно з'ясувати критичні контрольні точки і контрольовані параметри, що не завжди можливо і часто вимагає застосування інших методів менеджменту ризику;

– вживання заходів тільки при виході контрольованих параметрів за встановлені межі не завжди дає ефективні результати, оскільки не дозволяє врахувати зміни середнього процесу, коли контрольований параметр змінюється поблизу границь.

Посилальння на стандарт

ІСО 22000 Системи менеджменту безпеки харчових продуктів. Вимоги до всіх організацій в ланцюзі виробництва і споживання харчових продуктів.

Оцінка токсикологічного ризику

Стислий огляд

Оцінку токсикологічного ризику застосовують для визначення схильності рослин, тварин і людей впливу екологічних небезпек. Менеджмент токсикологічного ризику необхідний на кожному етапі прийняття рішень, включаючи порівняльну оцінку та обробку ризику.

Метод оцінки токсикологічного ризику передбачає аналіз небезпек або джерел збитку і їх впливів на цільові групи населення та шляхи експозиції небезпечних впливів на ці групи. Отриману інформацію потім обробляють і отримують вірогідну оцінку ступеня та характеру шкоди.

Сфера застосування

Для оцінки впливу (таких джерел, як хімікати, мікроорганізми та ін.) на рослини, тварин і людей використовують оцінку токсикологічного ризику.

Окремі елементи цього методу, такі, як аналіз шляхів експозиції, в якому досліджують різні способи поширення небезпеки на об'єкт, можуть бути адаптовані та застосовані в різних сферах менеджменту ризику для здоров'я людини і навколишнього середовища, та корисні при ідентифікації методів обробки ризику.

Вхідні дані

Для цього методу необхідні об'єктивні дані про характер, властивості небезпек, уразливих місць цільової групи населення (або популяції) і взаємодії ідентифікованих небезпек. Ці дані зазвичай засновані на лабораторних і епідеміологічних дослідженнях.

Процес виконання методу

Процес включає перераховані нижче етапи:

а) формулювання проблеми, включаючи встановлення сфери застосування оцінки шляхом визначення цільових груп населення і типів небезпек;

б) ідентифікацію небезпек, включаючи ідентифікацію всіх можливих джерел шкоди для цільової групи населення від досліджуваних небезпек. Ідентифікація небезпек зазвичай заснована на знаннях експертів і даних з опублікованих джерел;

в) аналіз небезпек, включаючи дослідження характеру і природи небезпек та їх взаємодії з об'єктом впливу. Наприклад, при дослідженні впливу на людський організм хімічних речовин небезпеки можуть включати в себе гостру і хронічну токсичність, можливість пошкодження ДНК, що спричиняє

онкологічні захворювання, порушення ембріонального розвитку та репродукції людини. Для кожного небезпечного впливу визначають рівень впливу (Вплив), сукупність небезпек, що впливають, та яких зазанає цільова група населення (Дозу), а також, по можливості, механізм цього небезпечного впливу. Необхідно відзначити рівні, на яких немає впливу (NOEL) та є помітний негативний вплив (NOAEL). Ці рівні іноді використовують критерії прийнятності ризику.

Для оцінки експозиції хімічних речовин використовують результати тестування і будують криву Доза-Вплив (рис. 5.1). Дані зазвичай отримують на основі тестів на тваринах або з експериментів на штучно вирощених тканинах або клітинах тварин.

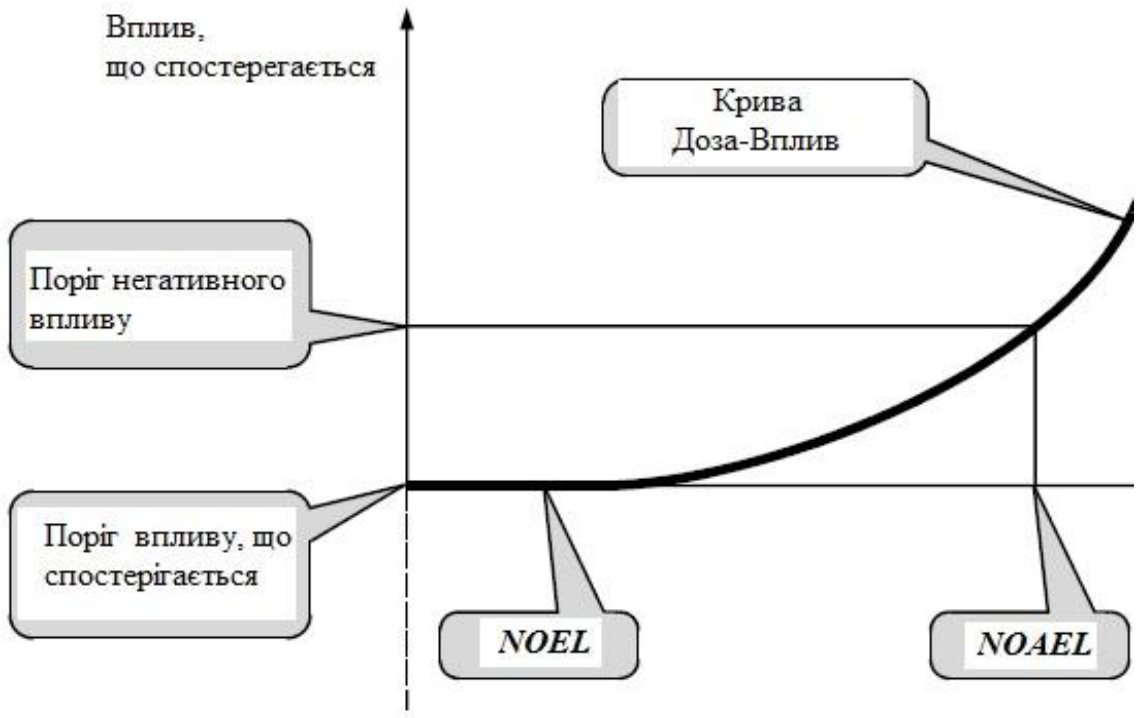

Рисунок 5.1 – Крива Доза-Вплив

Вплив інших небезпек, таких, як вплив мікроорганізмів або зміна біологічного виду, може бути визначено на основі даних спостережень та епідеміологічних досліджень. Після того як характер взаємодії збудників

хвороб або паразитів з об’єктом дослідження визначено, оцінюють ймовірність того, що в результаті схильності конкретного виду небезпеки буде завдано конкретний рівень шкоди;

г) аналіз експозиції, включаючи дослідження того, як небезпечна речовина або її залишки можуть впливати на цільову групу населення і в якій кількості. Цей етап часто містить аналіз шляхів поширення небезпек, бар’єрів і факторів, що перешкоджають та впливають на рівень експозиції. Наприклад, при дослідженні хімічних викидів аналіз експозиції передбачає визначення: наскільки великою є зона розпилення хімічних речовин; яким шляхом викиди можуть відбутися і за яких умов може виникнути прямий вплив на людей і тварин; скільки хімічних речовин осяде на рослини; які шляхи поширення отрутохімікатів, що потрапили в ґрунт; чи можуть ці хімічні речовини накопичуватися в живих організмах і в ґрунтових водах. Аналіз експозиції може містити дослідження паразитів, що потрапляють з інших регіонів, шляхи їх розповсюдження і впливу на об’єкти живої природи;

д) характеристика ризику, що включає збір та узагальнення отриманої інформації на етапах аналізу небезпек і аналізу експозиції, та оцінку ймовірності наслідків у разі спільного впливу небезпек.

У ситуації з великою кількістю небезпек і шляхів їх розповсюдження може бути проведено їх початковий аналіз, а потім – детальний аналіз небезпек та експозиції. Аналіз ризику повинен бути виконаний на основі загальних сценаріїв ризику.

Вихідні дані

Вихідні дані зазвичай характеризують рівень ризику впливу експозиції на цей об’єкт конкретної небезпеки в наявних умовах. Ризик може бути поданий у вигляді кількісної, змішаної або якісної оцінки. Наприклад, ризик онкологічних захворювань часто характеризують ймовірністю того, що людина захворіє протягом зазначеного періоду внаслідок впливу конкретних шкідливих хімічних речовин. Змішаний аналіз може бути використаний для отримання індексу ризику конкретної шкідливої хімічної речовини або шкідливого

мікроорганізму. Якісна оцінка ризику може являти собою належність ризику до одного з рівнів (високого, середнього, низького) або опис ймовірного впливу.

Переваги та недоліки

Перевага цього аналізу полягає в тому, що він забезпечує детальне розуміння проблеми і факторів, що сприяють підвищенню ризику.

Аналіз шляхів поширення дуже корисний для всіх сфер аналізу ризику. Він дозволяє ідентифікувати, як і де можна вдосконалити засоби управління або застосувати нові.

Однак для цього аналізу необхідні достовірні дані, які часто не доступні або мають високий рівень невизначеності. Наприклад, загальні дані про небезпеки, отримані на основі експериментів на тваринах, використовують для побудови кривої Доза–Вплив і екстраполюють для оцінки впливів на людину. Існують множинні моделі такої екстраполяції. Якщо об'єктом є навколишнє середовище, а не люди, і небезпеки не є хімічними, то даних, що відповідають конкретним умовам дослідження, може бути недостатньо.

Структурований аналіз сценаріїв методом «що, якщо?». Метод SWIFT

Стислий огляд

Метод SWIFT (*Structured what-if technique*) спочатку був розроблений як більш простий альтернативі дослідження HAZOP.

Це систематизований метод дослідження сценаріїв, заснований на командній роботі, в якому використовують набір слів або фраз–підказок, що допомагають у процесі наради учасникам групи ідентифікувати небезпечні ситуації і створити сценарій їх розвитку. Ведучий і група, використовуючи стандартні фрази «що, якщо» у поєднанні з підказками, досліджують, як система, елемент виробничого процесу, організація або процедура поводитимуться під впливом небезпечної події. Метод SWIFT зазвичай

застосовують для великих систем з більш високим рівнем деталізації, ніж дозволяє дослідження HAZOP.

Сфера застосування

Метод SWIFT спочатку був розроблений для дослідження небезпек хімічних та нафтохімічних підприємств, пізніше його стали широко застосовувати до систем, їх елементів, процесів, процедур і організацій в цілому. Особливо часто цей метод застосовують для дослідження наслідків змін, а також нових і змінених видів ризику.

Вхідні дані

Досліджувані системи, процедури, елементи, процеси та/або їх зміни необхідно точно визначити до початку дослідження. Слід встановити внутрішні і зовнішні цілі та сфери застосування шляхом проведення опитування й вивчення допоміжних документів, планів і графіків. Зазвичай досліджувані елемент, ситуацію або систему підрозділяють на частини, вузли або ключові компоненти, щоб спростити процес аналізу. Це рідше роблять на етапі визначення об’єктів дослідження при використанні методу HAZOP.

Іншими ключовими вхідними даними є знання експертів і досвід фахівців, що беруть участь у групових дослідженнях, до відбору яких необхідно підходити дуже ретельно. Всі причетні сторони повинні бути представлені по можливості із зазначенням досвіду роботи з аналогічними елементами, системами, їх змінами або ситуаціями.

Процес виконання методу

Процес складається з таких етапів.

а) До початку дослідження ведучий складає список слів або фраз–підказок, який може бути заснований на стандартному наборі слів і фраз або складений самостійно, спрямований на забезпечення всебічного аналізу небезпек або ризику.

б) На початку наради необхідно обговорити та узгодити зовнішні і внутрішні цілі і сфери застосування досліджуваних елемента, системи, їх змін чи ситуації.

в) Далі ведучий пропонує учасникам обговорити:

– відомі небезпеки і ризики;

– попередні досвід та інциденти;

– аідомі й існуючі засоби управління і захисні заходи;

– обов’язкові вимоги та обмеження.

г) Обговорення проходить легше, якщо запитання складені з використанням фраз «що, якщо» і слів або об’єктів–підказок. Прикладами фраз «що, якщо» можуть бути такі фрази, як «що станеться, якщо ...», «що трапиться, якщо ...», «міг хтось, чи могло щось ...». Основне завдання наради – стимулювати групу до дослідження можливих сценаріїв небезпечних подій, їх причин, наслідків і впливів.

д) Група дослідження повинна узагальнити отриману інформацію про ризик і розглянути засоби управління.

е) Опис ризику, його причин, наслідків та планованих коштів управління, схвалених групою дослідження, має бути зареєстроване.

ж) Дослідницька група повинна розглянути питання про адекватність та ефективність засобів управління, оцінити ефективність управління ризиком і дати відповідний висновок. Якщо у висновку дана незадовільна оцінка засобів управління і процесу управління ризиком, то група повинна далі більш глибоко розглянути завдання обробки ризику і визначити необхідні засоби управління.

з) У процесі подальшого обговорення необхідно використовувати запитання у формі «що, якщо» для ідентифікації наступних видів ризику.

і) Ведучий повинен використовувати список слів–підказок для управління обговоренням і допомоги у виявленні додаткових проблем і сценаріїв розвитку небезпечної події.

к) Для визначення пріоритетності необхідних дій зазвичай використовують якісний або змішаний методи оцінки ризику. Оцінку ризику

зазвичай проводять з урахуванням існуючих засобів управління та їх ефективності.

Вихідні дані

Вихідні дані включають в себе реєстр ризику і ранжирування за значущістю дії або завдання управління ризиком. Ці завдання можуть стати основою плану обробки ризику.

Переваги та недоліки

Метод SWIFT має такі переваги:

– застосовується до всіх форм елементів, систем, ситуацій, умов, організацій та видів діяльності;

– потребує мінімальної підготовки групи досліджень;

– досить швидко допомагає ідентифікувати основні небезпеки, які стають очевидними в процесі обговорення;

– системний підхід до дослідження дозволяє учасникам побачити реакцію системи на відхилення, не обмежуючись розглядом наслідків відмови компонентів;

– може бути використаний для ідентифікації способів поліпшення процесів і систем та визначення заходів, що приводять до підвищення їх надійності;

– залучення до обговорення осіб, відповідальних за існуючі засоби управління і подальші дії з обробки ризику, допомагає підвищити ефективність роботи групи;

– метод допомагає у створенні реєстру ризику та плану обробки ризику, не потребуючи великих додаткових зусиль;

– на відміну від звичайних методів, коли для оцінки ризику використовують якісні або змішані методи, приділяючи основну увагу застосуванню дії, метод SWIFT може бути використаний для ідентифікації небезпек і ризику, для яких надалі можливе застосування кількісних методів оцінки ризику.

Метод SWIFT має такі недоліки:

– для ефективного застосування цього методу необхідний досвідчений ведучий;

– необхідна ретельна підготовка обговорень, щоб час наради дослідницької групи не було витрачено даремно;

– якщо дослідницька група не має достатнього досвіду або якщо система підказок не є всебічною, то деякі ризики або небезпеки можуть бути пропущені і не ідентифіковані;

– застосування методу на загальному рівні не завжди відображає весь комплекс проблем і може не виявити деталізовані або корельовані причини.

Аналіз сценаріїв

Стислий огляд

Найменування методу «аналіз сценаріїв» дано процесу розробки описових моделей розвитку подій. Метод може бути використаний для ідентифікації ризику шляхом розгляду можливих подій у майбутньому і дослідження їх значущості та наслідків. Набори сценаріїв, що відображають, наприклад, «кращий випадок», «найгірший випадок» і «очікуваний випадок», можуть бути використані для аналізу можливих наслідків і їх ймовірності для кожного сценарію.

Можливості методу аналізу сценаріїв можна проілюструвати, розглядаючи основні зміни за минулі 50 років у технологіях, перевагах споживачів, соціальних відносинах та ін. У процесі аналізу сценаріїв важко прогнозувати ймовірність таких змін у майбутньому, проте можна аналізувати наслідки, допомогти організаціям використовувати переваги і забезпечити стійкість до прогнозованих змін.

Сфера застосування

Аналіз сценаріїв може бути корисний у прийнятті політичних рішень і плануванні майбутніх стратегій, а також при розгляді існуючих видів діяльності.

Цей метод може бути використаний для всіх трьох елементів оцінки ризику. На етапах ідентифікації та аналізу ризику набори сценаріїв, що відображають, наприклад, кращий, гірший і найбільш імовірний випадок, можуть бути використані для встановлення того, що може статися в конкретних обставинах, а також для аналізу потенційних наслідків і їх ймовірності для кожного сценарію.

Метод аналізу сценаріїв може бути використаний для прогнозування можливих загроз і їх розвитку в часі та застосований для всіх типів ризику в короткостроковій і довгостроковій перспективі.

У короткостроковій перспективі за наявності достовірних даних ймовірні сценарії можуть бути екстрапольовані на основі існуючих даних. У довгостроковій перспективі з урахуванням низької достовірності даних аналіз сценаріїв дозволяє визначити загальний характер розвитку подій.

Вхідні дані

Необхідною умовою застосування методу аналізу сценаріїв є наявність групи фахівців, що володіють розумінням характеру змін, що досліджуються (наприклад, можливих досягнень у технологіях).

Ці фахівці повинні бути здатні спрогнозувати ситуацію в майбутньому, не вдаючись до екстраполяції на основі даних минулих подій. Корисним є також використання даних літературних джерел і даних, що належать до змін.

Процес виконання методу

Структура методу аналізу сценаріїв може бути формалізованою або довільною. Після формування групи, встановлення каналів обміну інформацією, визначення досліджуваних проблем та сфери застосування методу необхідно ідентифікувати характер можливих змін. Слід також

дослідити основні тенденції та оцінити ймовірний час змін на основі експертного прогнозування.

Досліджувані зміни можуть включати:

– зовнішні зміни (наприклад, зміни технологій);

– рішення, які необхідно прийняти в найближчому майбутньому і які можуть призвести до різних результатів;

– потреби причетних сторін і можливі зміни;

– зміни в макросередовищі (обов'язкові вимоги, демографія та ін.), деякі з яких неминучі, інші можливі.

Іноді зміни можуть статися внаслідок іншої небезпечної події. Наприклад, зміна клімату призводить до змін споживчого попиту на продукти харчування, що впливає на те, які продукти харчування вигідно експортувати, а які – вирощувати в своєму регіоні.

Потім необхідно скласти перелік локальних факторів і макрофакторів або тенденцій і ранжувати спочатку за значущістю, потім за невизначістю. Особливу увагу слід приділяти факторам, які є найбільш значущими і більш невизначеними.

Ключові фактори або тенденції наносять на карту один навпроти одного, щоб показати і виявити зони розробки сценаріїв. Зазвичай пропонують набір сценаріїв, кожен з яких відповідає ймовірній зміні параметрів. Потім для кожного сценарію складають опис переходу від вихідної ситуації до розглянутого сценарію. Опис може включати ймовірні деталі, які можуть бути дуже корисними для сценарію.

Далі сценарії можуть бути використані для дослідження або оцінки вихідної проблеми. При проведенні досліджень необхідно враховувати всі суттєві, але прогнозовані чинники (наприклад, шаблони, що використовують). Потім потрібно досліджувати виконання політики або діяльності при реалізації цього сценарію й оцінити результати попереднього дослідження сценарію з використанням запитань «що, як що», заснованих на припущеннях моделей.

Після проведення оцінки запитань або припущень щодо кожного сценарію може стати очевидним, що саме необхідно змінити і як це зробити найбільш доцільно і безпечно. Можуть бути також визначені основні індикатори, що вказують на появу можливих змін.

Моніторинг основних індикаторів і вжиті відповідні заходи дозволяють забезпечити можливість внесення змін у заплановані стратегії. Оскільки сценарії охоплюють тільки окремі частини можливого розвитку майбутніх подій, важливо упевнитися, що враховано ймовірності появи конкретних сценаріїв, тобто визначено структуру ризику. Наприклад, якщо використовують сценарії кращого випадку, гіршого випадку і найбільш ймовірного випадку, необхідно зробити декілька спроб для їх класифікації та оцінити ймовірність появи кожного сценарію.

Вихідні дані

Найбільш відповідного сценарію може не бути, однак аналіз дозволяє отримати більш чітке розуміння варіантів розвитку подій і способів зміни дій при зміні індикаторів.

Переваги та недоліки

Аналіз сценаріїв враховує варіанти майбутнього розвитку подій і тому може бути більш кращим при традиційному підході до прогнозування, відповідно до якого на основі сценаріїв проводять оцінку ймовірності за шкалою (висока, середня і низька) на основі наявних даних, припускаючи, що розвиток подій буде відповідати відомим у минулому тенденціям. Це важливо в ситуації, коли недостатньо знань про досліджувану проблему для прогнозування її розвитку або коли небезпека може виникнути у віддаленому майбутньому.

З цією перевагою безпосередньо пов’язаний недолік методу аналізу сценаріїв, який полягає в тому, що в ситуації з високою невизначеністю деякі зі сценаріїв можуть бути нереальними.

Основні труднощі використання методу аналізу сценаріїв пов’язані з наявністю даних і здатністю аналітиків та осіб, що приймають рішення, розробити реальні сценарії, які можна дослідити можливими результатами.

Недолік використання методу аналізу сценаріїв для обґрунтування прийняття рішень полягає в тому, що використані сценарії можуть не мати достовірного обґрунтування; дані можуть бути гіпотетичними, а нереалістичність результатів може бути не виявлена.

Аналіз впливу на бізнес (BIA)

Стислий огляд

Метод аналізу впливу на бізнес BIA (Business Impact Analysis), також відомий як оцінка впливу на бізнес, дозволяє досліджувати ключові види відмов/порушень/руйнувань, які можуть вплинути на ключові види діяльності і процеси організації, а також ідентифікувати і кількісно визначити необхідні можливості для управління організацією в цих умовах. Процес методу BIA забезпечує узгодження і розуміння:

– ідентифікації та критичності ключових бізнес–процесів, функцій, пов’язаних ресурсів та ключових взаємозв’язків, що існують в організації;

– впливу відмов/порушень/руйнувань на можливості організації досягати встановлених критичних цілей бізнесу;

– необхідних можливостей управління впливом відмов/порушень/ руйнувань і відновленням нормального перебігу діяльності організації.

Сфера застосування

Метод BIA використовують при визначенні критичності процесів організації, часу їх відновлення (RTO – Recovery Time Objective) і необхідних ресурсів (активи, персонал, навички, технології, виробничі площі та інформація) для забезпечення досягнення встановлених цілей. Крім того, метод BIA допомагає при визначенні взаємозв’язків між процесами, внутрішніми та зовнішніми сторонами і всіма ланцюгами поставок організації.

Вхідні дані

Для застосування методу необхідні:

– група аналізу та розробки плану безперервності бізнесу;

– інформація про цілі, навколишнє середовищє, види діяльності та взаємозв’язки організації;

– докладний опис видів діяльності та функціонування організації, що включають процеси, допоміжні ресурси, взаємозв’язки з іншими організаціями, угоди про аутсорсінг, причетні сторони;

– економічні та виробничі наслідки, спричинені порушенням критичних процесів;

– підготовлені анкети;

– список опитуваних осіб у відповідних сферах діяльності організації та/або причетних сторін.

Процес виконання методу

У процесі BIA зазвичай використовують анкетування, інтерв’ю, структуровані наради або їх комбінацію, що дозволяє досягти розуміння функціонування критичних процесів, впливу порушень цих процесів і необхідного часу відновлення RTO і ресурсів.

Ключові етапи методу BIA:

– визначення критичності ключових процесів та ключових видів продукції, робіт, послуг організації на основі оцінки для них небезпек, загроз і вразливостей;

– визначення економічних і виробничих наслідків відмов/порушень/руйнувань ідентифікованих критичних процесів за певні періоди часу;

– ідентифікація взаємозв’язків із ключовими внутрішніми і зовнішніми причетними сторонами. На цьому етапі може бути корисним складання карт взаємозв’язків у системі і в ланцюзі постачань;

– визначення наявних необхідних ресурсів для забезпечення безперервності робіт після відмов/порушень/руйнувань на мінімальному допустимому для організації рівні;

– ідентифікація альтернативних способів виконання робіт і процесів, що існують, або запланованих до розробки. Альтернативні способи виконання робіт та процесів можуть бути застосовані в ситуації нестачі або відсутності необхідних ресурсів або можливостей під час відмов/порушень/руйнувань;

– визначення максимально допустимого періоду простою при відмовах/порушеннях/ руйнуваннях (МАО – Maximum Acceptable Outage Time) для кожного процесу, заснованого на ідентифікованих наслідках і критичних факторах виконуваних видів діяльності. МАО – це період часу, після закінчення якого існує загроза остаточної втрати життєздатності організації, якщо поставка продукції та/або надання послуг не будуть відновлені;

– визначення цільового часу відновлення (RTO) для будь–якого спеціалізованого обладнання, інформаційних технологій та інших активів організації. RTO являє собою час, запланований для відновлення виробництва продукції та надання послуг після відмов/порушень/руйнування, відновлення діяльності організації і відновлення спеціалізованого обладнання, інформаційних технологій або інших активів;

– встановлення рівня підготовленості критичних процесів для управління в умовах порушень, яке може включати оцінку рівня резервування процесу (наприклад, наявності запасного обладнання) або існування альтернативних постачальників.

Вихідні дані

Вихідними даними є:

– перелік ранжируваних за пріоритетами критичних процесів і відповідних взаємозалежностей;

– зареєстровані економічні та виробничі впливи, викликані порушенням критичних процесів;

– допоміжні ресурси, необхідні для ідентифікованих критичних процесів;

– можливі терміни простою та відновлення критичних процесів і взаємопов’язаних інформаційних технологій.

Переваги та недоліки

Перевагами методу BIA є:

– забезпечення розуміння критичних процесів, яке надає організації можливість досягнення встановлених цілей;

– можливість оцінки необхідних ресурсів;

– можливість перегляду виробничого процесу для підвищення стійкості організації.

Недоліками методу є:

– можлива недостатня компетентність учасників опитування, інтерв’ю або нарад;

– динаміка роботи в групі може впливати на весь аналіз функціонування критичного процесу;

– можливі спрощені або надоптимістичні оцінки вимог до відновлення;

– досягнення адекватного рівня розуміння діяльності організації може бути досить важким.

Аналіз першопричини (RCA, RCFA)

Стислий огляд

Аналіз втрат, що становлять основну частку збитку, спрямований на запобігання їх повторного виникнення, зазвичай називають аналізом першопричини (RCA – Root Cause Analysis), аналізом першопричини відмови (RCFA – Root Cause Failure Analysis) або аналізом втрат. Метод RCA використовують для дослідження втрат внаслідок різних видів відмов, у той час як аналіз втрат застосовують передусім для дослідження фінансових або економічних втрат від зовнішніх факторів або катастроф. Метод RCA спрямований на виявлення первинних причин відмови без розгляду їх зовнішніх проявів. Очевидно, що коригувальні дії не завжди ефективні і часто

потребують їх постійного поліпшення. Метод RCA зазвичай застосовують для оцінки основної складової втрат, однак його можна використовувати для аналізу більш загальних втрат із метою виявлення можливостей постійного поліпшення.

Сфера застосування

Метод RCA має багато напрямів застосування:

– із метою безпеки метод RCA використовують для дослідження нещасних випадків у сфері охорони праці та виробничої безпеки;

– у технологічних системах для аналізу надійності та технічного обслуговування використовують аналіз відмов;

– RCA виробництва застосовують для контролю якості виробничих процесів;

– RCA процесів застосовують для дослідження бізнес–процесів;

– RCA систем, що являє собою комбінацію перерахованих видів RCA, застосовують при аналізі складних систем у системах управління змінами менеджменту ризику і в системному аналізі.

Вхідні дані

Основними вхідними даними методу RCA є всі об’єктивні дані про відмови або втрати. Дані про аналогічні відмови також можуть бути розглянуті в процесі аналізу. Іншими вхідними даними можуть бути дані, отримані при перевірці конкретних гіпотез.

Процес виконання методу

Після прийняття рішення про застосування методу RCA формують групу експертів для проведення аналізу та розробки рекомендацій. Спеціалізація експертів залежить насамперед від цілей аналізу й особливостей відмови.

Методи проведення аналізу можуть істотно відрізнятися, однак основні етапи методу RCA аналогічні і включають:

– формування групи;

– встановлення сфери застосування і цілей методу RCA;

– збір даних та об’єктивних свідчень про відмову або втрати;

– проведення структурованого аналізу для визначення першопричини;

– вироблення рішень і рекомендацій;

– виконання рекомендацій;

– верифікацію позитивного результату від впровадження рекомендацій.

Застосовують такі структуровані методи аналізу:

– метод «5 чому», що полягає в багаторазовому повторенні запитання «чому?», для дослідження п’яти рівнів глибини причини відмови;

– аналіз видів і наслідків відмов;

– аналіз дерева несправностей;

– діаграму Ісікави або «риб’ячий скелет»;

– аналіз Парето;

– складання карти першопричини.

Оцінку причин часто починають із дослідження спочатку очевидних фізичних причин, далі вивчають причини, пов’язані з людським фактором, і вже потім переходять до вивчення прихованих причин управління або основних причин. Для того щоб застосування коригувальних дій було ефективним, залучені сторони повинні мати можливість управляти виявленими в процесі аналізу причинними факторами або усунути їх.

Вихідні дані

Вихідні дані методу RCA включають в себе:

– документацію щодо зібраних даних та об’єктивних свідчень;

– розглянуті гіпотези;

– висновок про найбільш ймовірні першопричини відмов і втрат;

– рекомендовані та коригувальні дії.

Переваги та недоліки

Перевагами методу є можливість:

– залучення до робочої групи технічних експертів;

– використання структурованого аналізу;

– розгляду всіх імовірних гіпотез;

– документування отриманих результатів;

– обов’язкового впровадження заключних рекомендацій.

Недоліки методу RCA:

– відсутня можливість залучення необхідних технічних експертів;

– критичні об’єктивні свідчення можуть бути втрачені в момент відмови або під час прибирання;

– обмеження за часом і ресурсами можуть не дозволити робочій групі провести всебічну оцінку ситуації;

– іноді неможливо впровадити розроблені рекомендації.

Аналіз видів і наслідків відмов, та аналіз видів, наслідків та критичності відмов (FMEA)

Стислий огляд

Аналіз видів і наслідків відмов (FMEA – Failure Mode Effect Analysis) є методом, що використовується для ідентифікації способів відмови компонентів, систем або процесів, які можуть призвести до невиконання призначеної їх функції.

Метод FMEA допомагає ідентифікувати:

– всі види відмов різних частин і компонентів системи (видами відмов можуть бути приховані відмови, конструктивні відмови, виробничі відмови та ін., які призводять до порушення працездатного стану частин та/або компонентів системи);

– наслідки відмов для системи;

– механізми відмови;

– способи досягнення безвідмовної роботи та/або пом’якшення наслідків для системи.

Розширеною версією методу FMEA є FMECA, що дозволяє оцінити критичність і значущість кожного ідентифікованого виду відмови. Критичність відмови – це сукупність ознак, що характеризують наслідки відмови.

Класифікація відмов з критичності проводиться відповідно до законодавчих та обов'язкових вимог, і таких, що встановлюються пріоритетами організації.

Аналіз критичності зазвичай є якісним або змішаним, але може бути кількісним при використанні показника фактичного відсотка відмов.

Сфера застосування

Залежно від об'єкта дослідження виділяють кілька варіантів методу: FMEA проекту або продукції, FMEA процесу, що застосовується для аналізу виробничих і складальних процесів, FMEA системи, FMEA послуги і FMEA програмного забезпечення.

Метод FMEA/FMECA може бути застосований на стадіях проектування, виробництва та експлуатації виробничої системи.

Однак для підвищення надійності внесення змін на стадії проектування системи є більш ефективним. Методи FMEA і FMECA також можуть бути застосовані до процесів і процедур, наприклад, ці методи застосовують для виявлення можливості медичних помилок і дефектів у процесі технічного обслуговування.

Методи FMEA/FMECA можуть бути використані:

– при виборі з альтернативних варіантів проекту з високою надійністю;

– для дослідження всіх видів відмов систем і процесів та їх впливу на безвідмовність досліджуваного об'єкта;

– для ідентифікації наслідків помилок персоналу (вплив людського фактора);

– при плануванні перевірок (тестів) і технічного обслуговування технічних систем;

– для поліпшення проектів процедур і процесів;

– для отримання якісної або кількісної інформації для інших методів аналізу, таких, як аналіз дерева несправностей.

Результати методів FMEA і FMECA можуть бути використані як якісні та кількісні вхідні дані для інших методів досліджень, таких, як, наприклад, аналіз дерева несправностей.

Вхідні дані

Для виконання методів FMEA і FMECA необхідна детальна інформація про елементи системи, достатня для аналізу способів і шляхів розвитку відмови кожного елемента. Для детального застосування методу FMEA до проекту елемент системи може бути розглянутий на рівні його компонентів, у той час як для FMEA системи в цілому елементи системи можуть бути визначені на укрупненому рівні (у вигляді блоків і підсистем).

Інформація може включати:

– креслення і блок–схеми аналізованої системи та її компонентів або етапи процесу;

– інформацію про функціонування кожного етапу процесу або компонента системи;

– докладний опис екологічних та інших параметрів, які можуть впливати на функціонування системи;

– відомості про результати відмов;

– хронологічні дані про відмови, включаючи доступні дані про інтенсивність відмов.

Процес виконання методу

Процес FMEA включає основні етапи.

1. Визначення сфери застосування і цілей дослідження.

2. Формування робочої групи.

3. Вивчення системи/процесу, для яких застосовують метод FMECA.

4. Розподіл системи на компоненти або етапи;

5. Визначення функції кожного етапу або компонента.

6. Визначення для кожного компонента або етапу:

– можливих відмов та їх причин;

– механізмів, що призводять до цих видів відмови;

– наслідків відмов;

– рівень безпеки або руйнівності наслідків відмови;

– способи виявлення відмови.

7. Ідентифікація особливостей проекту, що дозволяють компенсувати відмову.

При виконанні методу FMECA робоча група додатково класифікує кожну з ідентифікованих видів відмов відповідно до її критичності.

Існує декілька способів виконання аналізу критичності відмов. Загальноприйнятий метод включає визначення:

– показника критичності виду відмови;

– рівня ризику;

– рангу пріоритетності ризику.

Модель критичності виду відмови є мірою можливості того, що досліджуваний вид відмови компонента призведе до відмови системи в цілому. Критичність відмови визначають як добуток ймовірності наслідків відмови на інтенсивність виду відмови і на час функціонування системи. Цю формулу часто застосовують до відмов обладнання в ситуації, коли кожен з цих показників може бути визначений кількісно, і види відмови мають однакові наслідки.

Рівень ризику визначають як поєднання наслідків виду відмови та ймовірності цієї відмови, він може бути використаний в ситуації, коли наслідки різних видів відмов різні, його застосовують до систем і процесів, пов’язаних із обладнанням. Рівень ризику може бути поданий у якісному, змішаному або кількісному вигляді.

Ранг пріоритетності ризику (RPN – Risk Priority Number) є змішаною мірою критичності відмови, його розраховують шляхом множення рангу значущості наслідків відмови (зазвичай від 1 до 10) на ймовірність відмови і можливість виявлення проблеми. Якщо відмову важко виявити, то їй зазвичай приділяють більше уваги і надають першочергового значення. Цей метод використовують найчастіше в процесі забезпечення якості.

З моменту ідентифікації видів відмов та механізмів їх виникнення слід визначити та впровадити коригувальні дії для найбільш істотних видів відмов.

Результати виконання методу FMEA повинні бути задокументовані у вигляді звіту, який повинен містити:

– докладний опис системи, що досліджується;

– способи, використані для виконання аналізу;

– припущення, зроблені в процесі виконання аналізу;

– джерела даних;

– отримані результати, включаючи заповнені контрольні листи;

– критичність (якщо потрібно) і методи, використані для її визначення;

– рекомендації для подальших досліджень, зміни проекту або особливості, які необхідно включити до планів перевірок, випробувань та ін.

Система може бути повторно оцінена в іншому циклі FMEA, після того як всі необхідні дії щодо проведення аналізу будуть завершені.

Вихідні дані

Первинними вихідними даними методу FMEA є перелік видів відмов, механізмів виникнення відмови і його наслідків для кожного компонента системи або етапу процесу (які можуть включати в себе інформацію про ймовірність відмови). До вихідних даних також належить інформація про причини та наслідки відмов для системи в цілому. Вихідні дані методу FMECA містять результати ранжирування значущості відмов на основі оцінення ймовірності відмови системи, рівня ризику виникнення цього виду відмови або комбінації рівня ризику і «можливості виявлення» виду відмови.

Метод FMECA може бути корисний для отримання кількісних вихідних даних при використанні кількісних даних про інтенсивність відмов та їх наслідки.

Переваги та недоліки

Переваги методу FMEA/FMECA:

– метод застосовують до видів відмов, пов’язаних із помилками персоналу, порушенням працездатності обладнання та роботи систем програмного забезпечення і процесів;

– метод дозволяє ідентифікувати види відмов компонентів, причини цих відмов та їх наслідки для системи і подати їх у зручній для користувача формі;

– застосування методу допомагає уникнути дорогих модифікацій обладнання при технічному обслуговуванні за рахунок ідентифікації та усунення проблем на ранніх стадіях етапу проектування;

– метод дозволяє ідентифікувати види відмов в окремій точці і встановити вимоги до резервування та систем безпеки;

– метод дає можливість отримати вхідні дані для розробки програм моніторингу, надаючи інформацію про необхідні об’єкти моніторингу та їх особливості.

Недоліки методу:

– метод FMEA/FMECA може бути використаний тільки для ідентифікації окремих відмов, а не їх поєднання;

– без адекватного контролю і спеціальної спрямованості такі дослідження можуть бути трудомісткими і дорогими;

– застосування методу FMEA/FMECA може бути трудомістким і тривалим для складних багаторівневих систем.

Посилання на стандарти

МЕК 60812 Методи аналізу надійності систем. Метод аналізу видів і наслідків відмов (FMEA)

Аналіз дерева несправностей (FTA)

Стислий огляд

Аналіз дерева несправностей FTA – Fault Tree Analysis – метод ідентифікації та аналізу факторів, які можуть сприяти виникненню небажаної події, що досліджується (так званою кінцевою подією).

За допомогою дедукції фактори, що досліджуються, ідентифікують, вибудовують їх логічно і подають на діаграмі у вигляді дерева, яке відображає ці фактори і їх логічний зв’язок із кінцевою подією. Факторами, зазначеними в дереві несправностей, можуть бути події, пов’язані з відмовами компонентів

комп’ютерного обладнання, помилками людини або іншими подіями, які можуть призвести до небажаного результату (події). Приклад FTA наведено на рис. 5.2.

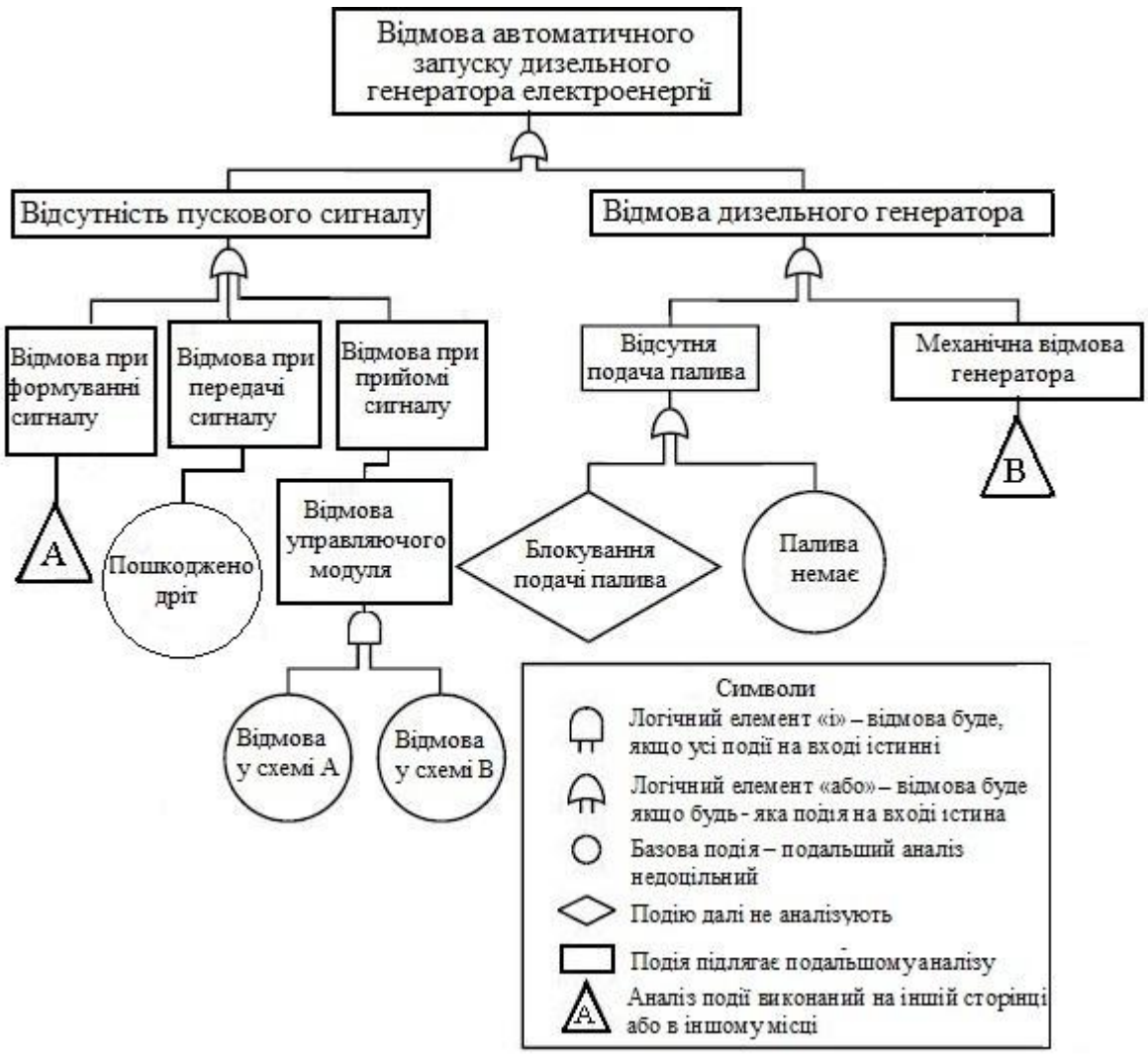

Рисунок 5.2 – Приклад методу FTA

Сфера застосування

Метод дерева несправностей може бути використаний для визначення якісної оцінки при ідентифікації причин відмови та шляхів, що призводять до кінцевої події, і кількісної оцінки при обчисленні ймовірності кінцевої події, якщо відомі значення ймовірностей початкових подій.

Цей метод може бути використаний на стадії проектування системи для ідентифікації причин відмови і, отже, вибору варіанта проекту. Метод FTA може бути використаний на стадії виробництва для ідентифікації видів основних відмов і відносної значущості шляхів, що призводять до кінцевої події. Дерево несправностей може бути також використано для аналізу поєднання подій, яке призвело до виникнення відмови, що досліджується.

Вхідні дані

Для якісного аналізу необхідне добре знання системи і розуміння причин відмови, а також розуміння того, як система може вийти з ладу. Для аналізу корисним є використання детальних схем дерева несправностей. Для проведення кількісного аналізу необхідні дані про інтенсивність або імовірність відмови всіх основних подій, зазначених у дереві несправностей.

Процес виконання методу

Виділяють такі етапи розробки діаграми дерева несправностей:

– визначення кінцевої події, яку необхідно проаналізувати. Це може бути відмова або більш загальні наслідки відмови. Після того, як наслідки відмови проаналізовано, в дерево несправностей може бути включено частину, що належить до скорочення інтенсивності та наслідків відмови;

– ідентифікацію можливих причин або видів відмов, що призводять до кінцевої події, починаючи з кінцевої події;

– аналіз ідентифікованих видів і причин відмови для визначення того, що конкретно призвело до відмови;

– послідовну ідентифікацію небажаного функціонування системи з переходом на низькі рівні системи, поки подальший аналіз не стане недоцільним. У технічній системі це може бути рівень відмови компонентів. Події та фактори на найнижчому рівні системи, що аналізуються, називають базисними подіями;

– оцінку ймовірності базисних подій (якщо є) і подальший розрахунок ймовірності кінцевої події. Для забезпечення достовірності кількісної оцінки слід показати, що повнота і якість вхідних даних для кожного елемента

достатні для отримання вихідних даних необхідної достовірності. В іншому випадку дерево несправностей є недостатньо достовірним для аналізу ймовірності, але може бути корисним для дослідження причинно–наслідкових зв’язків.

При визначенні кількісної оцінки дерево несправностей може бути спрощено за допомогою бульової алгебри, що дозволяє врахувати дублюючі види відмов.

Крім кількісної оцінки ймовірності кінцевої події метод дозволяє ідентифікувати набір мінімальних перерізів, що приводять до кінцевої події, і розрахувати їх вплив на кінцеву подію.

За винятком простих випадків, для побудови діаграми зазвичай застосовують пакет прикладних програм, що дозволяє проводити розрахунки в ситуаціях, коли відбуваються події, що повторюються в декількох місцях дерева несправностей, і коли необхідно обчислити мінімальні перерізи. Використання програмного забезпечення гарантує послідовність і правильність виконання методу та можливість його верифікації.

Вихідні дані

Вихідними даними аналізу дерева несправностей є:

– наочне подання шляхів виникнення кінцевої події і взаємодіючих шляхів у ситуації, коли одночасно можуть відбутися дві або більше подій;

– набір мінімальних перерізів (виникнення шляхів відмови системи) й оцінка ймовірності відмови системи для кожного перерізу;

– оцінка ймовірності кінцевої події.

Переваги та недоліки

Переваги методу FTA:

– надання точного, систематизованого і гнучкого підходу дозволяє аналізувати різноманітні фактори, включаючи дії персоналу та фізичні явища;

– застосування підходу «знизу уверх» дозволяє розглядати вплив тих відмов, які безпосередньо пов’язані з кінцевою подією;

– застосування особливо є доцільним для аналізу систем, що передбачають підключення великої кількості пристроїв і взаємодії з ними (систем, що мають множинні інтерфейси);

– графічне подання дозволяє спростити розуміння функціонування системи і розглянутих факторів, але оскільки деревоподібні схеми найчастіше достатньо громіздкі, їх обробка може потребувати застосування комп'ютерних програм, що забезпечує можливість розгляду більш складних логічних взаємозв'язків (наприклад, із використанням логічних операцій «І–АБО» і «АБО–І»), але при цьому ускладнює верифікацію дерева несправностей;

– логічний аналіз дерева несправностей і визначення набору мінімальних перерізів корисні при ідентифікації простих шляхів відмови в складних системах, де комбінації подій можуть привести до виникнення кінцевої події.

Недоліки методу:

– невизначеність оцінок ймовірностей базисних подій впливає на оцінку ймовірності виникнення кінцевої події. Це може призвести до високого рівня невизначеності в ситуації, коли ймовірність відмови для кінцевої події точно невідома, але достовірність оцінок істотно вища для добре вивченої системи;

– у деяких ситуаціях початкові події не пов'язані між собою, і часом важко встановити, чи враховані всі важливі шляхи до кінцевої події. Наприклад, недостатнє дослідження всіх джерел займання може призвести до невірної оцінки ризику виникнення пожежі (кінцевої події). У цій ситуації аналіз ймовірності із застосуванням методу FTA неможливий;

– дерево несправностей є статичною моделлю, в якій фактор тимчасової залежності не враховують;

– дерево несправностей може бути застосоване лише до бінарних станів (працездатного / непрацездатного);

– незважаючи на те що помилки людини можуть бути враховані у схемі дерева несправностей на якісному рівні, невідповідність ступеня та якості часто характеризує помилки людини, які в дереві несправностей врахувати достатньо складно;

– дерево несправностей не дозволяє легко врахувати і досліджувати ланцюгові реакції (ефект доміно) й умовні відмови.

Посилання на стандарти

МЕК 61025 Аналіз дерева несправностей (FTA)

Аналіз дерева подій (ETA)

Стислий огляд

Метод ETA – Event Tree Analysis – є графічним методом подання взаємовиключних послідовностей подій, що наступають за появою вихідної події, відповідно до функціонування і нефункціонування систем, розроблених для пом'якшення наслідків небезпечної події (рис. 5.3). Метод ETA може бути застосований для якісної та/або кількісної оцінки.

На рис. 5.3 подано прості розрахунки для типового дерева подій в ситуації, коли гілки дерева подій повністю незалежні.

Послідовність подій легко подати у вигляді дерева подій, і тому за допомогою ETA легко встановити, погіршують або пом'якшують наслідки події, беручи до уваги додаткові системи, функції або бар'єри.

Сфера застосування

Метод ETA може бути використаний для моделювання, обчислення та ранжування (з точки зору ризику) різних сценаріїв інциденту після виникнення початкової події.

Метод ETA може бути застосовано на всіх стадіях життєвого циклу продукції або процесу. Цей метод може бути використано на якісному рівні при мозковому штурмі, визначенні сценаріїв і після – послідовностей подій, які можуть виникнути після початкової події і при визначенні впливу на результат різних видів обробки ризику, бар'єрів або засобів управління, призначених для зниження небажаних наслідків.

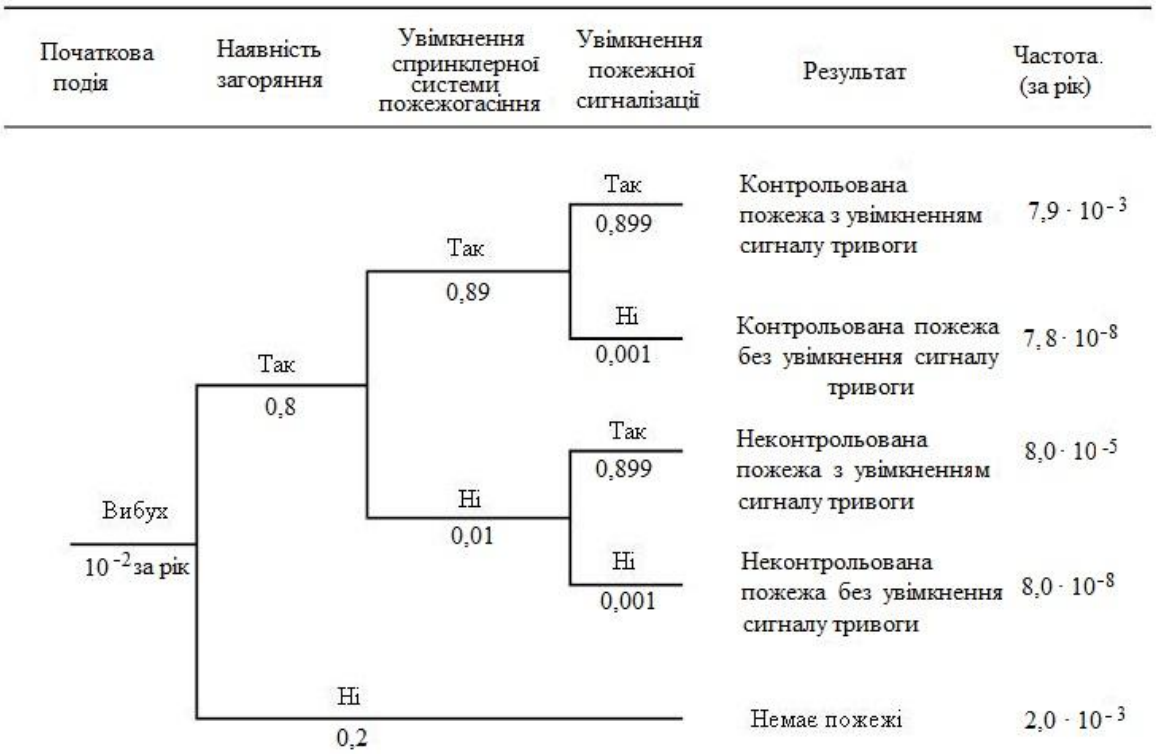

Рисунок 5.3 – Приклад дерева подій

При оцінці допустимих засобів управління найбільш доцільним є застосування методу ETA для кількісного аналізу. Найчастіше цей метод застосовують при моделюванні відмов у ситуації використання великої кількості засобів захисту. Метод ETA може бути використаний при моделюванні початку події для виявлення можливих втрат і переваг. Однак в обставинах, де необхідно знайти шляхи оптимізації та одержання найбільших переваг, частіше використовують моделювання за допомогою дерева рішень.

Вхідні дані

Вхідні дані включають в себе:

– перелік розглянутих початкових подій;

– інформацію про способи обробки, бар'єри, засоби управління і відповідні імовірності відмови (для кількісного аналізу);

– розуміння процесів нормування початкової відмови.

Процес виконання методу

Побудову дерева подій починають із вибору початкової події. Це може бути інцидент, такий, як вибух пилу, або така подія, як відмова системи енергопостачання. Далі перераховують наявні функції або системи, спрямовані на пом'якшення наслідків. Для кожної функції або системи креслять лінії для відображення її справного стану або відмови. Імовірність відмови може бути оцінена і призначена для кожної такої лінії. Цю умовну ймовірність оцінюють, наприклад, за допомогою експертних оцінок або аналізу дерева несправностей. Таким чином зображують різні шляхи розвитку подій від початкової події.

Слід враховувати, що ймовірності на дереві подій є умовними, наприклад, ймовірність спрацьовування розбризкувача системи пожежогасіння, отримана при випробуваннях у нормальних умовах, буде відрізнятися від імовірності спрацьовування цієї системи при загорянні, спричиненому вибухом.

Кожна гілка дерева являє собою ймовірність того, що всі події на цьому шляху відбудуться. Тому ймовірність результату обчислюють як добуток окремих умовних ймовірностей і ймовірності початкової події за умови незалежності подій.

Вихідні дані

Вихідні дані ETA включають в себе таке:

– якісний опис можливих проблем у вигляді комбінацій подій, що являють собою різні наслідки початкової події (ранжування наслідків);

– кількісні оцінки частоти або ймовірності появи подій і відносної значущості різних наслідків відмов, а також подій, що їм сприяють;

– перелік рекомендацій щодо зниження ризику;

– кількісні оцінки ефективності впровадження рекомендацій.

Переваги та недоліки

Переваги методу ETA:

– за допомогою методу ETA легко схематично зобразити сценарії розвитку подій після виникнення початкової події, провести аналіз

працездатного стану або відмови допоміжних систем або функцій, призначених для зниження наслідків відмови, й оцінити їх вплив;

– метод допомагає врахувати фактор часу, побачити взаємозв'язки і ланцюгові реакції, які складно досліджувати за допомогою методу дерева несправностей;

– метод графічно подає послідовність подій, що неможливо зробити за допомогою методу дерева несправностей.

Недоліи методу:

– для використання методу ETA складової частини загального процесу оцінки необхідно ідентифікувати всі можливі початкові події. Цього можна досягти за допомогою використання інших методів аналізу (наприклад, HAZOP, PHA), проте завжди залишається ймовірність того, що не враховано деякі важливі початкові події;

– метод дерева подій можна застосовувати тільки для двох станів системи (працездатного стану і відмови), в ньому важко врахувати відстрочене порушення працездатного стану системи або її відновлення;

– кожен шлях реалізації обумовлений поєднанням подій, що відбулися в попередніх точках розгалуження схеми дерева подій. Тому розглядають всі взаємозв'язки щодо можливих шляхів розвитку події. Однак деякі взаємозв'язки, наприклад, загальні компоненти, системи постачання і персонал, можуть бути не враховані при розгляді, що може призвести до надмірно оптимістичної оцінки ризику.

Аналіз причин та наслідків

Загальні положення

Аналіз причин і наслідків є поєднанням методів дерева несправностей і дерева подій.

Цей метод починають із розгляду критичної події та аналізу її наслідків за допомогою застосування поєднання логічних елементів ТАК/НІ. Ці елементи являють собою умови, за яких система, розроблена для зниження наслідків

початкової події, знаходиться в працездатному стані або в стані відмови. Причини умов або відмов аналізують за допомогою методу дерева несправностей.

Сфера застосування

Метод аналізу причин і наслідків спочатку був розроблений як інструмент перевірки надійності систем, критичних для забезпечення безпеки, який використовували для більш повного розуміння відмов системи. Так само, як і метод аналізу дерева несправностей, цей метод використовують для відображення логіки відмови, що приводить до критичної події, однак додатково до функціональних можливостей дерева несправностей цей метод дозволяє провести аналіз послідовності появи відмов. Метод також дозволяє врахувати час запізнювання при аналізі наслідків, що неможливо при використанні методу дерева подій.

Метод використовують для аналізу різних варіантів роботи системи після виникнення критичної події залежно від поведінки її підсистем (наприклад, аварійних систем). Якщо такі варіанти можна охарактеризувати кількісно, то можуть бути оцінені ймовірності можливих наслідків критичної події. Оскільки кожна послідовність у діаграмі причин і наслідків є поєднанням дерев несправностей більш низького рівня, то метод аналізу причин і наслідків може бути використаний як спосіб побудови більш складних дерев несправностей. Діаграми складні в побудові та застосуванні, тому їх доцільно використовувати, коли втрати від наслідків відмов співставлені з витраченими зусиллями.

Вхідні дані

Для застосування методу необхідне розуміння системи, видів і сценаріїв відмов.

Процес виконання методу

На рис. 5.4 наведено концептуальну діаграму типового аналізу причин і наслідків.

Процедура аналізу включає такі етапи:

1. ідентифікацію критичної (або початкової) події (еквівалентної кінцевої події дерева несправностей та початкової події дерева подій);
2. розробку та валідацію дерева несправностей для причини початкової події. При цьому слід використовувати ті самі символи, що і при аналізі дерева несправностей;
3. визначення порядку розгляду умов відмови. У цьому порядку необхідно дотримуватися логічної послідовності та відповідної часової послідовності, в якій вони виникають.
4. побудову шляхів виникнення наслідків залежно від умов. Ця діаграма подібна дереву подій, проте розгалуження дерева подій доповнюють і зображують у вигляді окремого блоку, в якому вказують умови;
5. якщо відмови для кожного блоку умов незалежні, можливе розрахування ймовірності кожного наслідку. Для цього необхідно оцінити ймовірності кожного виходу умовного блоку (із застосуванням відповідних дерев несправностей).

Ймовірність будь-якої послідовності подій, що призводить до конкретного наслідку, визначають перемноженням ймовірностей кожної послідовності умов, що призводить до розглянутого наслідку. Якщо кілька послідовностей подій призводять до одного наслідку, то ймовірності всіх послідовностей складають. Якщо є залежності між відмовами в аналізованій послідовності (наприклад, порушення енергопостачання може спричинити кілька умов відмови), то умови залежності необхідно визначити до проведення розрахунку.

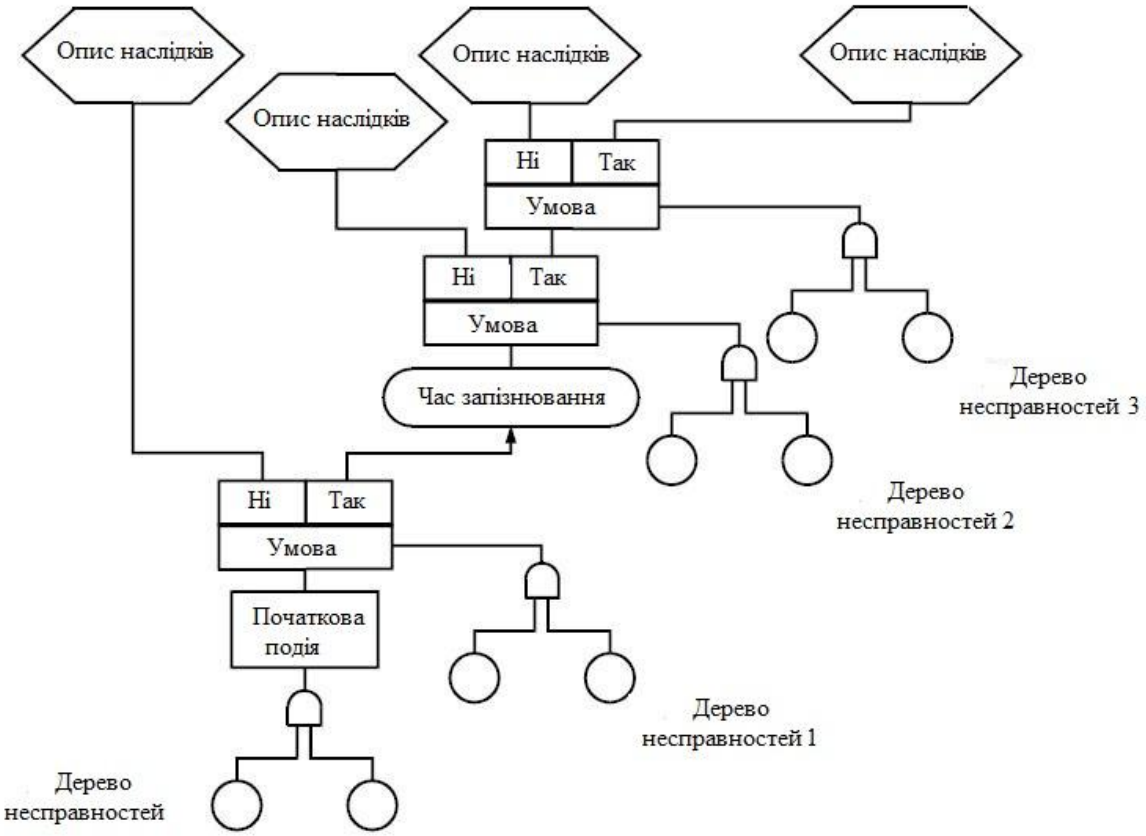

Рисунок 5.4 – Приклад аналізу причин і наслідків

Вихідні дані

Вихідними даними методу аналізу причин і наслідків є схематичне подання відмови системи із зазначенням причин і наслідків та оцінення ймовірності виникнення кожного потенційного наслідку, яка заснована на аналізі ймовірностей виникнення відповідних умов після критичної події.

Переваги та недоліки

Переваги методу аналізу причин і наслідків аналогічні загальним пріоритетам методів дерева подій і дерева несправностей. Крім того, даний метод дозволяє подолати деякі з недоліків цих методів, оскільки дозволяє аналізувати події, що розвиваються протягом тривалого періоду часу. Аналіз причин і наслідків забезпечує всебічне уявлення про систему.

Недоліком методу є його складність порівняно з методами дерева несправностей і дерева подій як при побудові схеми, так і при врахуванні залежностей у випадку кількісного аналізу.

Причинно-наслідковий аналіз (діаграма Ісікави)

Стислий огляд

Причинно-наслідковий аналіз є структурованим методом ідентифікації можливих причин небажаної події чи проблеми. Цей метод дозволяє скомпонувати можливі причини та фактори в узагальнені категорії так, щоб можна було дослідити всі можливі гіпотези. Однак застосування цього методу дозволяє ідентифікувати фактичні причини. Причини можуть бути визначені тільки на основі емпіричних даних або емпіричним шляхом. Інформацію подають у вигляді діаграми «риб'ячого скелета» (метод також називають діаграмою Ісікави) або іноді у вигляді деревоподібної схеми.

Сфера застосування

Причинно-наслідковий аналіз забезпечує структуроване графічне подання причин, що передують висновку. Залежно від об'єкта досліджень наслідок може бути позитивним (мета) або негативним (проблема).

Метод використовують для дослідження всіх можливих сценаріїв і причин, запропонованих групою експертів. Метод дозволяє досягти узгодженої думки щодо найбільш імовірних причин, які можуть бути далі перевірені дослідним шляхом або на основі наявних даних.

Найбільш доцільно застосовувати цей метод на самому початку аналізу, що дозволяє розширити діапазон уявлень про можливі причини, а потім сформулювати гіпотези, які далі слід розглянути відповідно до встановленої процедури.

Побудова причинно-наслідкової діаграми дозволяє:

– ідентифікувати можливі першопричини та/або основні причини для певного висновку, проблеми або умови;

– провести аналіз в ситуації і знайти взаємозв'язок між взаємодіючими факторами, пов'язаними з процесом що досліджується;

– проаналізувати існуючі проблеми для прийняття коригувальних дій.

Перевагами побудови причинно-наслідкової діаграми є:

– сприяння визначенню початкових причин проблеми із застосуванням структурованого підходу;

– сприяння в роботі групі експертів і більш повному використанню знань експертів про продукцію або процеси;

– застосування простого для сприйняття типу діаграми для відображення причинно-наслідкових зв’язків;

– виявлення можливих причин змін у процесі;

– ідентифікація сфер збору даних для подальших досліджень.

Причинно-наслідковий аналіз може бути використаний, як метод виконання аналізу першопричини.

Вхідні дані

Вхідними даними причинно-наслідкового аналізу є результати експертизи, досвід учасників робочої групи, раніше розроблені моделі, використані в попередніх дослідженнях.

Процес виконання методу

Причинно-наслідковий аналіз має бути виконаний групою експертів, які мають знання та досвід з досліджуваної проблеми.

Основними етапами причинно–наслідкового аналізу є:

– встановлення висновку, який необхідно проаналізувати, і розміщення його праворуч у відповідному блоці діаграми. Висновок може бути позитивним (мета) або негативним (проблема) залежно від обставин;

– визначення основних (головних) категорій причин і зазначення їх у відповідних блоках діаграми «риб’ячого скелета». При аналізі систем зазвичай виділяють такі категорії причин: персонал, обладнання, робоче середовище, процеси та ін. Категорії визначають згідно з об’єктом дослідження;

– зазначення можливих причин для кожної основної (головної) категорії на гілках і відгалуженнях для опису взаємозв’язків між ними;

– продовження дослідження шляхом альтернативної постановки запитань «чому?» або «що це викликало?» для встановлення зв’язків між причинами;

– встановлення всіх гілок і відгалужень, спрямоване на перевірку послідовності і повноти виявлених причин, і їх відношення до основного висновку;

– ідентифікація найбільш імовірних причин цього висновку на основі узгодженої думки робочої групи експертів і доступних об’єктивних свідчень.

Результати зазвичай подають у вигляді діаграми «риб’ячого скелета» (діаграма Ісікава) або у вигляді дерева. Діаграма «риб’ячого скелета» структурована шляхом поділу причин на основні (головні) категорії (подані ребрами «риб’ячого скелета») і більш дрібними відгалуженнями, що конкретизують причини цих категорій (рис. 5.5).

Зображення цієї діаграми у вигляді деревоподібної схеми аналогічно дереву несправностей, але зазвичай цю діаграму будують зліва направо, а не зверху вниз. Однак при застосуванні цієї діаграми буває важко уявити результат у кількісному вираженні й оцінити ймовірність основної події, оскільки причини більшою мірою розуміють як можливі фактори, які можуть викликати подію, що розглядається, а не відмови з відомою ймовірністю виникнення.

Причинно-наслідкову діаграму зазвичай застосовують для визначення якісних оцінок. Можна припустити, що ймовірність виникнення проблеми становить 1, і розподілити ймовірності за причинами, що узагальнюються, потім за більш дрібними причинами, ґрунтуючись на ступені довіри чи значущості. Однак найчастіше між факторами, які можуть викликати події, існує взаємозв’язок, що сприяє виникненню необхідності обробки результату більш складним способом, що робить кількісну оцінку недостовірною.

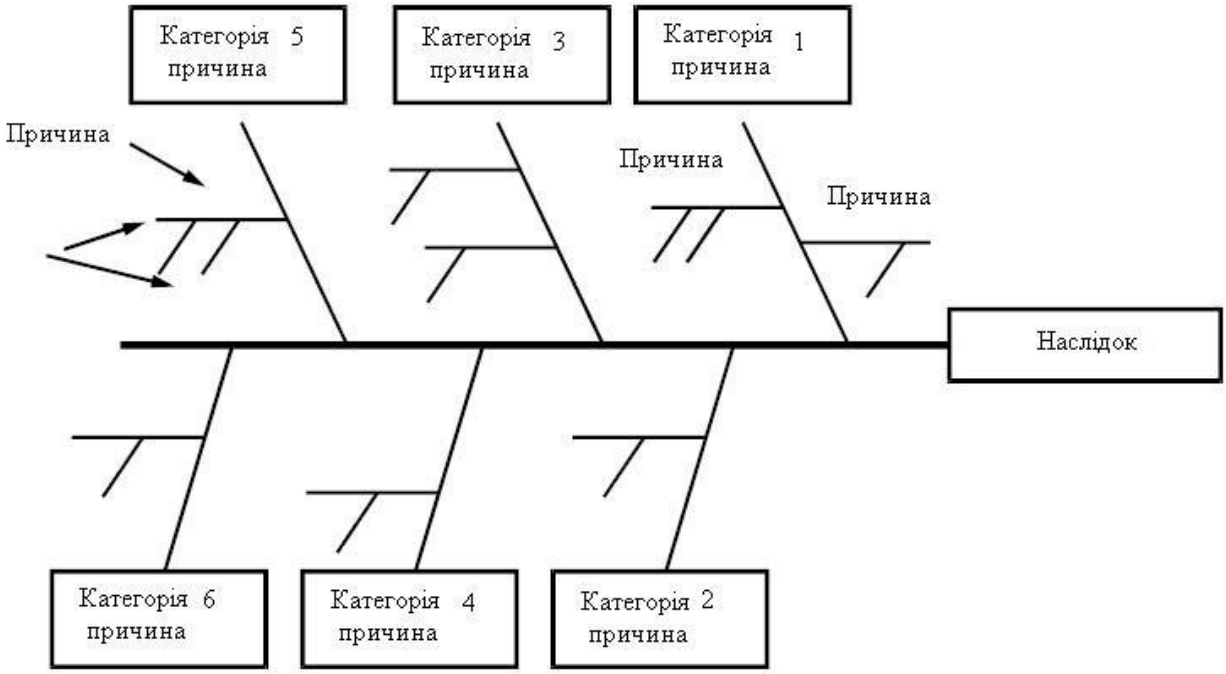

Рисунок 5.5 – Приклад діаграми Ісікава, або «риб’ячого скелета»

Вихідні дані

Вихідними даними причинно-наслідкового аналізу є діаграми у вигляді «риб’ячого скелета» або деревоподібної схеми, які показують можливі причини події, що досліджується (рис. 5.6). Отримані дані необхідно перевірити теоретично й експериментально, перш ніж будуть запропоновані подальші рекомендації.

Переваги та недоліки

Перевагами методу є:

– залучення компетентних експертів до роботи групи;

– застосування структурованого аналізу;

– розгляд усіх ймовірних припущень і гіпотез;

– графічне відображення результатів у простій для сприйняття формі;

– визначення сфер, в яких потрібні додаткові дані;

– можливість встановлення факторів, які можуть викликати події, що розглядаються як для сприятливих, так і для небажаних результатів.

Позитивний погляд на проблему може стимулювати більшу відповідальність і залучення учасників.

Метод має такі недоліки:

– група експертів може не мати необхідної компетентності;

– для розробки рекомендацій метод необхідно застосовувати тільки як частину аналізу першопричини;

– метод призначений для проведення мозкового штурму, а не самостійного аналізу;

– поділ причинних факторів на основні категорії на початку аналізу означає, що взаємозв’язки між категоріями причин можуть бути не розглянуті належно, наприклад, відмова обладнання, спричинена помилкою оператора, або помилки оператора через недоліки конструкції системи.

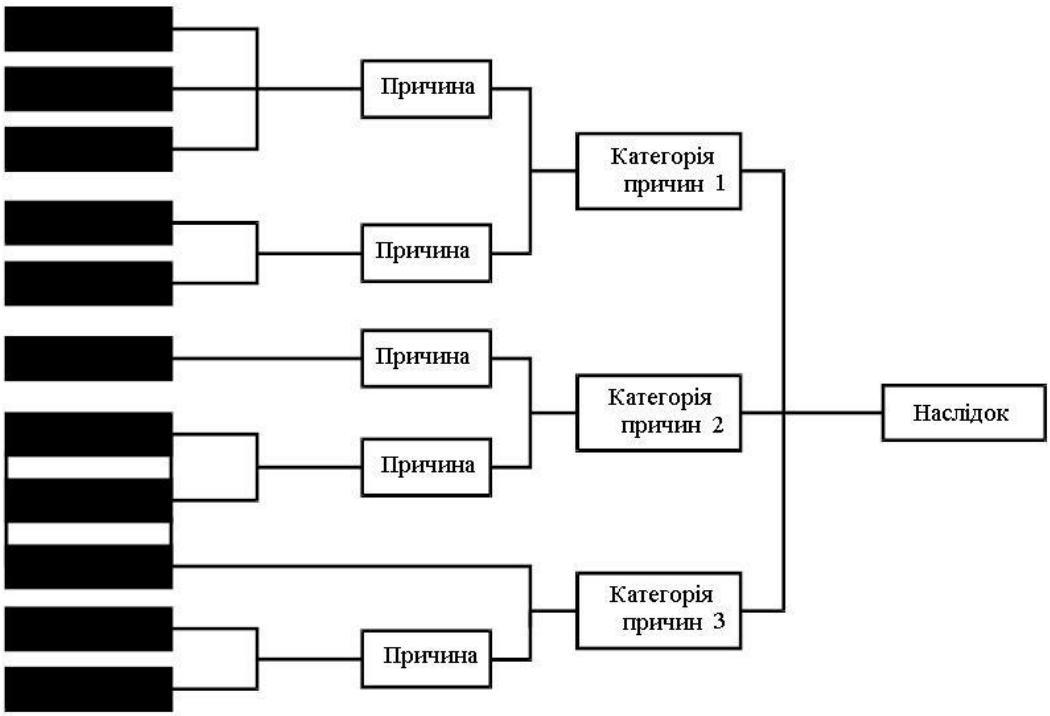

Рисунок 5.6 – Приклад подання причинно–наслідкового аналізу у вигляді дерева

Аналіз рівнів захисту (LOPA)

Стислий огляд

Метод LOPA – Layers of Protection Analysis – метод змішаної оцінки ризику, пов'язаного з небажаною подією або сценарієм. Метод спрямований на аналіз достатності заходів з управління або зниження ризику.

Метод LOPA заснований на виборі пар причин і наслідків та ідентифікації рівнів захисту, які можуть запобігти причині, що призводить до небажаного наслідку. Для визначення адекватності заходів зниження ризику до допустимого рівня необхідно провести розрахунок наслідків.

Сфера застосування

Метод LOPA може бути використаний як якісний метод дослідження рівнів захисту між небезпекою або причинними подією і результатом. Зазвичай змішаний підхід застосовують для досягнення більшої точності після HAZOP або PHA.

Метод LOPA забезпечує основу для визначення вимог до незалежних рівнів захисту (IPL – Independent Protection Layers) і рівнів повноти безпеки (рівні SIL – Safety Integrity Levels) для автоматизованих систем, як встановлено в серії стандартів МЕК 61508 та 61511, а також при визначенні вимог до рівнів повноти безпеки SIL для автоматизованих систем безпеки. Метод LOPA може бути корисний для ефективного розподілу ресурсів, спрямованих на зниження ризику, шляхом застосування аналізу зниження ризику при впровадженні кожного рівня захисту.

Вхідні дані

Вхідними даними методу LOPA є:

– основна інформація про ризик, включаючи небезпеки, причини і наслідки, аналогічно вхідним даним методу PHA;

– інформація про фактичні і планові засоби управління;

– частота причинних подій, оцінки імовірності відмови рівнів захисту, оцінки наслідків і допустимого ризику;

– частота ініціюючих причин, оцінки ймовірності відмови рівнів захисту, оцінки наслідків і допустимого ризику.

Процес виконання методу

Метод LOPA зазвичай виконує група експертів із застосуванням такої процедури:

– ідентифікації початкових причин виникнення небажаного результату і збору даних про їх частоту та наслідки;

– вибору однієї пари причина–наслідок;

– ідентифікації рівнів захисту, що запобігають причині, яка призводить до небажаного наслідку, та аналізу їх ефективності;

– sдентифікації незалежних рівнів захисту (IPL) (не всі рівні захисту є незалежними);

– оцінки ймовірності відмови кожного IPL;

– дослідження частоти початкових причин спільно з вірогідністю відмови кожного IPL і ймовірностями реалізації всіх умовних параметрів (прикладом умовного параметра є присутність або відсутність людини в зоні небезпечного впливу) для визначення частоти виникнення небажаного наслідку. При дослідженні враховують порядок значень частот і ймовірностей;

– порівняння розрахункового рівня ризику з допустимим для визначення необхідності у подальшому захисті.

Незалежний рівень захисту IPL – система пристроїв або дій, здатних попередити реалізацію сценарію, який призводить до небажаного наслідку, і забезпечити незалежність причин подій чи рівнів захисту, пов’язаних зі сценарієм. Незалежними рівнями захисту IPLs є:

– конструктивні особливості проекту;

– фізичні пристрої захисту;

– системи блокування і відключення;

– аварійна сигналізація і можливості ручного втручання оператора;

– фізичний захист при реалізації події;

– системи аварійного реагування (процедури і перевірки, які не належать до IPLs).

Вихідні дані

Вихідними даними методу є рекомендації щодо подальшого застосування засобів управління та їх ефективності для зниження ризику. Метод LOPA є одним із методів, що використовується при оцінці SIL для систем безпеки й автоматизованих систем.

Переваги та недоліки

Переваги методу LOPA:

– метод потребує для застосування меншого часу і ресурсів, ніж метод аналізу дерева несправностей, або повної кількісної оцінки ризику і є більш точним, ніж якісний метод експертних оцінок;

– метод LOPA допомагає ідентифікувати найбільш критичні рівні захисту і забезпечити їх ресурсами;

– цей метод допомагає ідентифікувати операції, системи та процеси з недостатнім рівнем захисних заходів;

– метод спрямований на найбільш серйозні небажані наслідки.

Недоліки методу:

– метод LOPA дозволяє розглядати одну пару причина-наслідок і один відповідний сценарій при одноразовому до нього зверненні. Цей метод не охоплює складні взаємодії між ризиками або засобами управління;

– кількісна оцінка ризику не завжди може бути отримана для загальних видів відмов;

– метод LOPA не застосовується до складних сценаріїв у ситуаціях з великою кількістю пар причин–наслідків або з наслідками, що зачіпають різні причетні сторони.

Посилання на стандарти

МЕК 61508 (всі частини) Функціональна безпека систем електричних, електронних, програмованих електронних систем, пов’язаних із безпекою [22].

МЕК 61511 Безпека функціональна. Система безпеки, що забезпечується приладами для сектора обробної галузі промисловості[23].

Стандарт IEC 61508

Функціональна безпека електричних, електронних і програмованих електронних систем, пов’язаних із безпекою "(Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems).

Стандарт Міжнародної електротехнічної комісії (International Electrotechnical Commission) IEC 61508 – «Функціональна безпека електричних, електронних і програмованих електронних систем, пов’язаних із безпекою» – це міжнародний стандарт, розроблений для визначення систем безпеки (Safety Related Systems – SRS) загального вигляду.

Стандарт може використовуватися для будь–яких галузей промисловості, де є необхідність у застосування програмованих систем безпеки. Дата офіційного затвердження стандарту – 2000 рік. У цілому стандарт досить складний для сприйняття не тільки через свій величезний обсяг (понад 400 сторінок густого тексту двома мовами – англійською і французькою), але й надзвичайно ускладнену і заплутану термінологію. Стандарт визначає концепцію Моделі життєвого циклу системи безпеки, аналогічну ISA 84.01–96 (рис. 5.7–5.9). Загальна схема моделі життєвого циклу, яку відтворює і структура самого стандарту IEC 61508, наведена на рис. 5.7. Модель життєвого циклу системи встановлює, що рівень допуску системи не обмежується початковим рівнем допуску, до якого входять пристрої, включаючи датчики і виконавчі механізми.

Рівень допуску системи так само, як і рівень допуску людини, повинен визначатися та підтверджуватися для всіх стадій і етапів на всьому життєвому шляху:

22. IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety–related systems

23. IEC 61511 Functional safety – Safety instrumented systems for the process industry sector

- зародження ідеї;
- попереднього обстеження й оцінки;
- проектування;
- експлуатації;
- випробування, перевірки і техобслуговування.

Стандарт є безпекою від «неприпустимого ризику». Іншими словами, абсолютної безпеки досягти неможливо, можна тільки знизити ризик до допустимого рівня. Стандарт визначає чотири рівні інтегральної безпеки (Safety Integrity Level – SIL) залежно від конкретної імовірності відмови виконання необхідної функції (Probability of Failure on Demand – PFD).

Рівні безпечного допуску SIL за стандартом IEC 61508:

4 – захист від загальної катастрофи;

3 – захист обслуговуючого персоналу і населення;

2 – захист від травматизму;

1 – захист устаткування та продукції.

Модель життєвого циклу електричної, електронної і програмованої електронної системи безпеки (E / E / PES) наведено на рис. 5.7.

При цьому необхідно розуміти, що, наприклад, прийняття рівня допуску SIL1 означає, що рівень небезпеки процесу та обмеження на економічні втрати при відмові системи захисту низькі настільки, що системі дозволено 10 % відмов виконання функцій захисту. Відповідно, 90 %-ва надійність означатиме, що з кожних десяти випадків перевищення, наприклад, рівня в ємності, в одному випадку з цих десяти відбудеться переповнення ємності. Фактор зниження ризику також потребує правильної інтерпретації. Наприклад, збільшення фактора зниження ризику до 100 і більше років при рівні допуску SIL2 зовсім не означає, що ця конкретна система здатна пропрацювати без небезпечних відмов і помилкових спрацьовувань сотню років. Це значення означає, що із сотні одночасно працюючих систем одна система протягом одного року призведе процес до небезпечної відмови.

Зрештою, завдання рівня допуску SIL ґрунтується на необхідній величині зниження ризику, яка визначається під час аналізу небезпеки процесу.

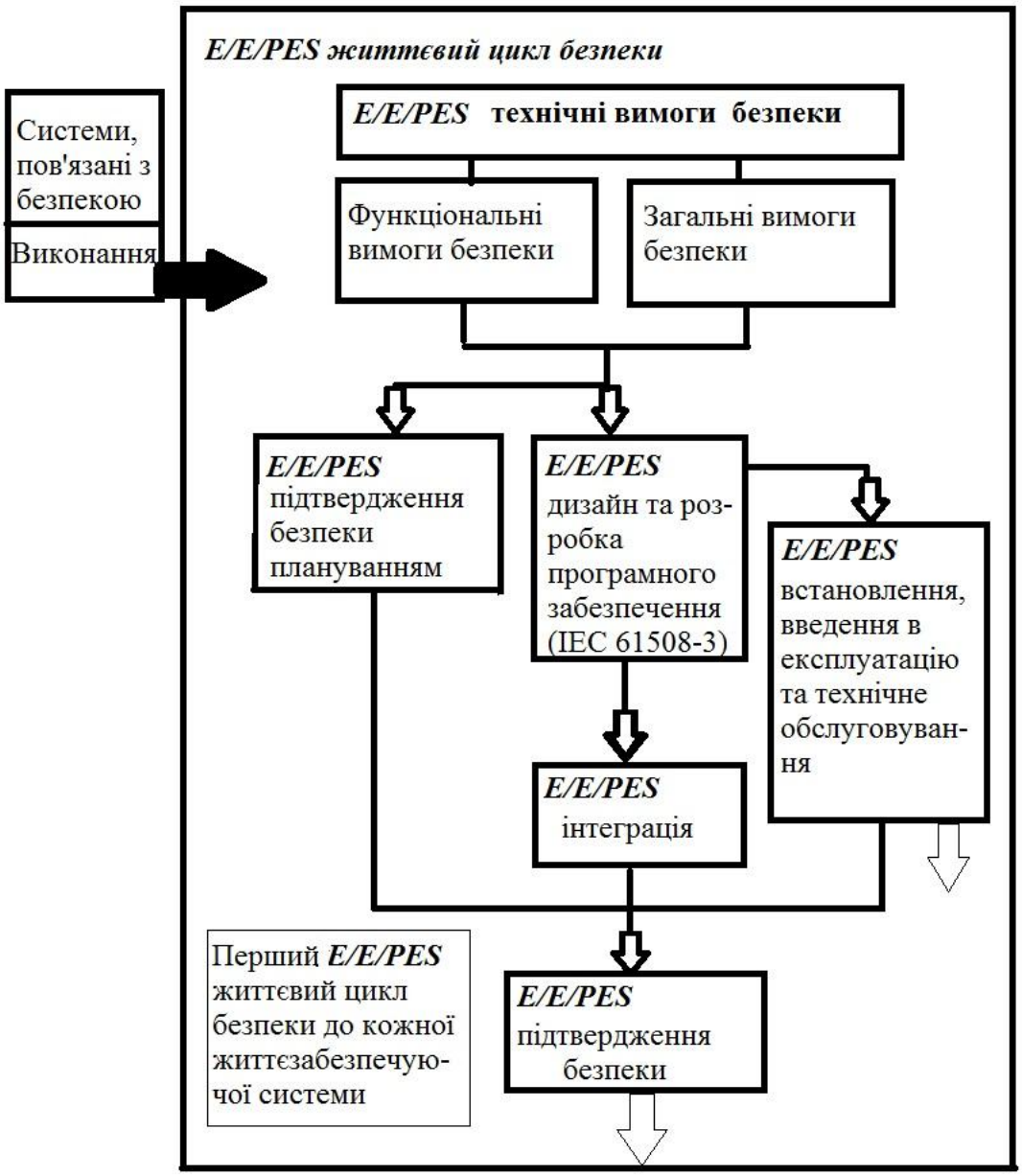

Рисунок 5.7 – Модель життєвого циклу програмного забезпечення

Звичайно, кожне підприємство має право самостійно приймати рішення і встановлювати свої вимоги до систем безпеки на основі власної технічної політики. Однак сучасні стандарти безпеки встановлюють і вимагають від підприємств відповідності розпорядженням, виробленим на основі досвіду

експлуатації та аналізу причин аварій великої кількості вибухопожежонебезпечних виробництв. Це означає, що в будь–якому випадку вибір рівня

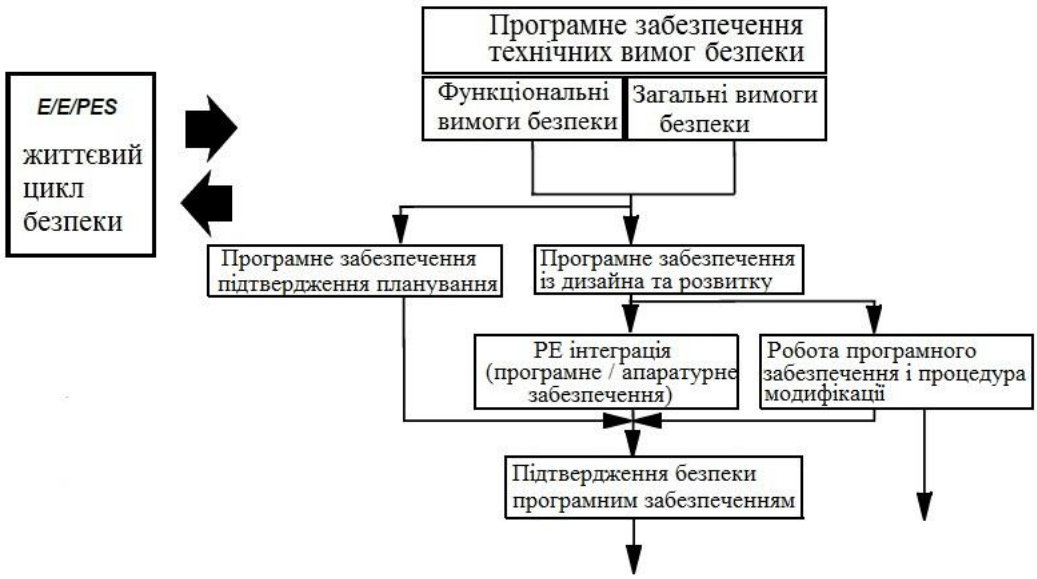

Рисунок 5.8 – Взаємодія моделей життєвого циклу електричної, електронної і програмованої електронної системи безпеки (E / E / PES) та програмного забезпечення

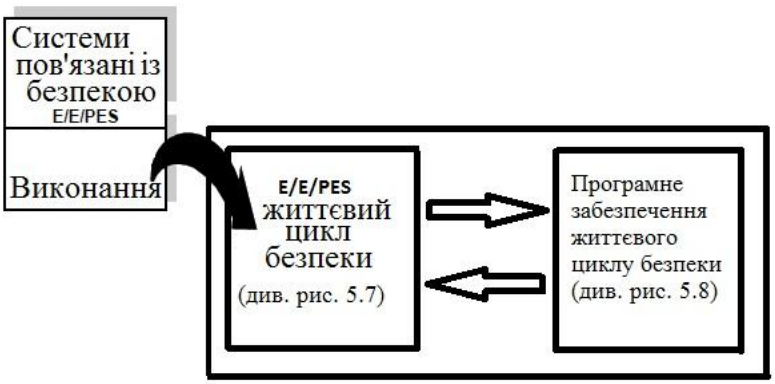

Рисунок 5.9 – Взаємодія моделей життєвого циклу системи безпеки (E / E / PES) і програмного забезпечення

інтегральної безпеки і відповідної йому системи захисту повинен бути ретельно проаналізований, обгрунтований і точно задокументований. Діаграма ризиків і рівні допуску стандарту IEC 61508 наведені на рис. 5.10.

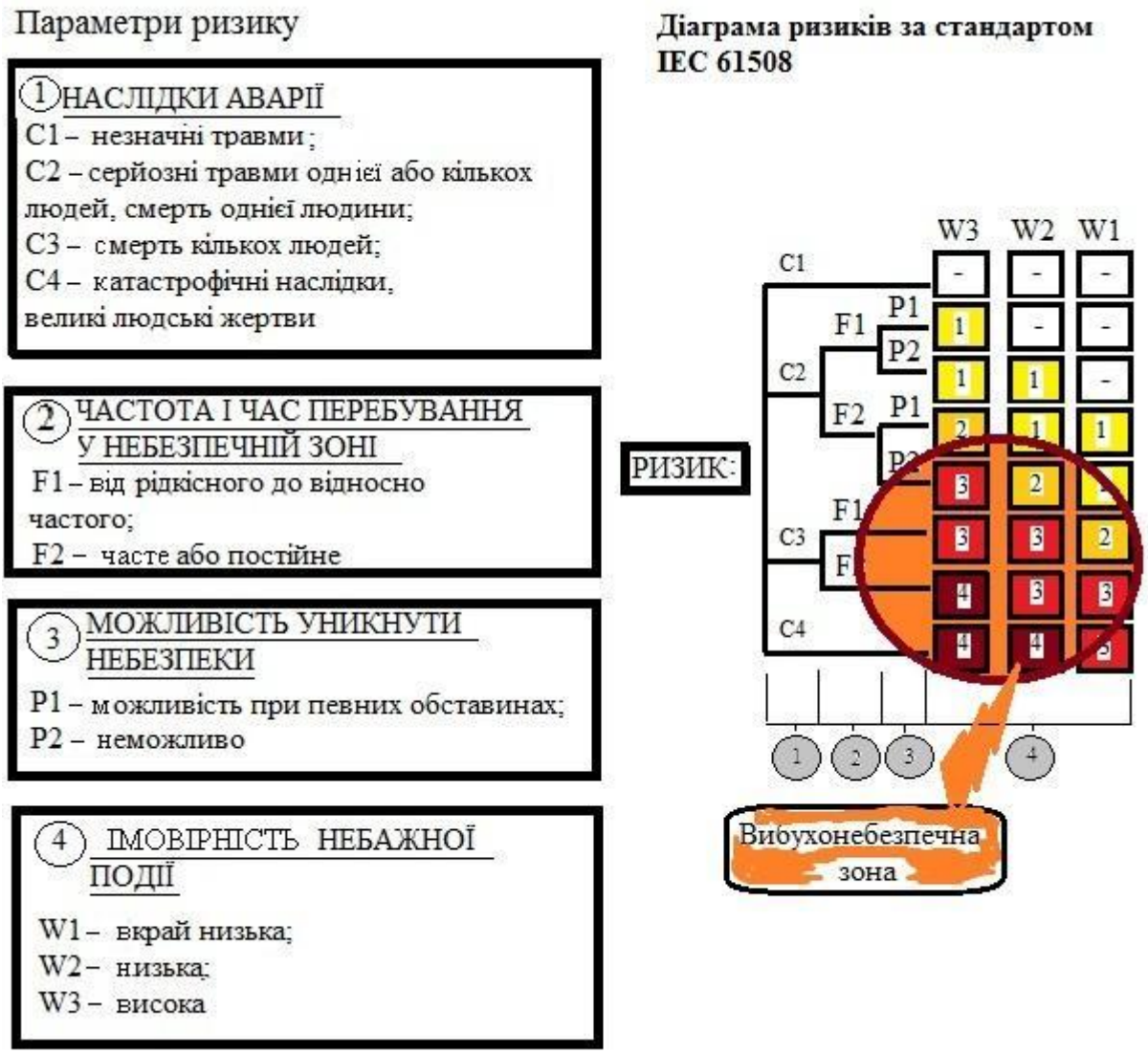

Рисунок 5.10 – Діаграма ризиків і рівні допуску стандарту IEC 61508

Стандарт містить вимоги до професійної підготовки та кваліфікації фахівців, що визначають рівень вимог до систем безпеки для конкретного процесу. На відміну від усіх попередніх стандартів безпеки, стандарт IEC 61508 передбачає безпосередню участь технологічного персоналу в забезпеченні функцій безпеки. Разом з тим у стандарті є застереження, що конкретні вимоги до технологічного та обслуговуючого персоналу повинні встановлюватися в галузевих стандартах (і в стандартах підприємства), які повинні розроблятися з урахуванням загальної методології безпеки, що визначається цим стандартом.

У найзагальнішому вигляді стандарт IEC 61508 визначає таке:

1) модель розвитку системи безпеки;

2) два підходи до систем безпеки:

– забезпечення захисту і безперервності контролю за середньою частотою небезпечних відмов;

– забезпечення захисту і контролю за середньою імовірністю небезпечної відмови протягом зумовленого інтервалу часу;

3) концепцію безпечного допуску;

4) чотири рівні безпечного допуску (SIL).

Структура і параметри ризику стандарту IEC 61508 запозичені з німецького стандарту DIN 19250. При цьому структури діаграм параметрів ризику для DIN і IEC повністю збігаються. Параметри ризику за стандартом IEC 61508 наведено на рис. 5.10:

Травматизм

C1 – незначні травми;

C2 – серйозні травми однієї або кількох людей, смерть однієї людини;

C3 – смерть кількох людей;

C4 – катастрофічні наслідки, великі людські втрати.

Тривалість перебування в небезпечній зоні

F1 – від рідкісного до відносно частого;

F2 – часте або постійне.

Запобігання небезпеки

P1 – можливо при певних обставинах;

P2 – неможливо.

Імовірність небажаної події

W1 – вкрай низька;

W2 – низька;

W3 – висока.

Стандарт IEC 61511 Функціональна безпека. Система безпеки приладів для переробного сектора промисловості.

Стандарт IEC 61511 Functional Safety: Safety Instrumented Systems for the Process Industry Sector – це міжнародний стандарт, розроблений для спільного використання з IEC 61508, який визначає загальні вимоги безпеки. В 2004 р. МЕК прийняла стандарт безпеки технологічних процесів IEC 61511.

Стандарт IEC 61508 спочатку призначався для виробників і постачальників устаткування. Стандарт IEC 61511 призначений для проектувальників систем безпеки, фахівців з їх інтегрування в процес розробників і користувачів систем управління виробничими і технологічними процесами.

Стандарту IEC 61511 мають відповідати системи безпеки, призначені для захисту технологічних процесів у нафтовій, газовій, хімічній, нафтохімічній та інших галузях промисловості. Сенсори, логічні пристрої та виконавчі елементи стандартом IEC 61511 визначено як складові елементи системи безпеки. Стандарт також розглядає інтерфейси з іншими рівнями контролю та управління на відповідність загальним вимогам безпеки виробництва і навіть людської спільноти (рис. 5.11).

Аналогічно стандарту IEC 61508 стандарт IEC 61511 визначає дві основні концепції, що є в основі його практичного застосування:

1) життєвий цикл системи безпеки;

2) інтегральний рівень безпеки.

Концепція рівнів захисту згідно з IEC 61511

Стандарт охоплює повний життєвий цикл системи:

1) проектування;

2) складання;

3) впровадження;

4. експлуатацію;

5) обслуговування;

6) модифікацію;

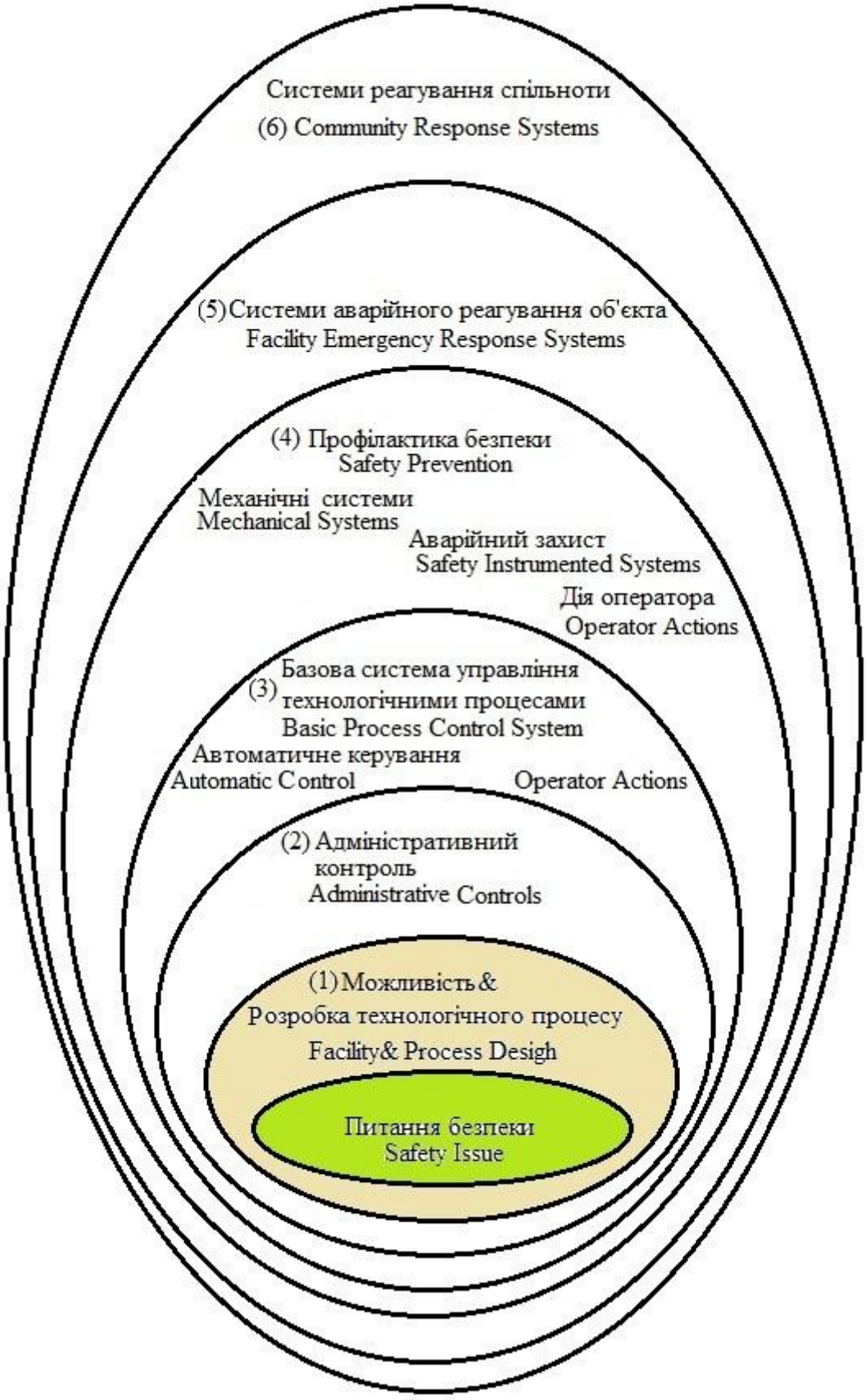

Рисунок 5.11 – Рівні контролю та управління на відповідність загальним вимогам безпеки виробництва (людської спільноти)

7. списання системи.

При розгляді життєвого циклу системи:

- кількісно оцінюються ризики технологічного процесу;
- визначаються вимоги до системи безпеки, що включає сенсори і виконавчі елементи;
- розглядаються та проектуються рівні управління і захисту;
- визначається архітектура системи безпеки, що забезпечує захист від ризиків процесу.

Так само, як і стандарт IEC 61508, стандарт IEC 61511 має 4 рівні інтегрального допуску. Але на відміну від стандарту загального призначення IEC 61508, стандарт IEC 61511 не рекомендує розглядати катастрофічні процеси, що відповідають найвищому рівню вимог SIL4 як сфері застосування програмованих електронних систем.

Ідентифікація інтегрального рівня безпеки SIL

Рівень допуску системи безпеки може розглядатися як статистичне подання відповідності системи заданому інтегральному рівню безпеки. При цьому необхідно чітко розуміти, що ці вимоги ставляться передусім до кожної окремої функції, що включає в себе і сенсори, і логічні пристрої, і виконавчі елементи. Некоректно стверджувати, що окрема одиниця обладнання має якийсь власний інтегральний рівень безпеки.

Деякий компонент обладнання системи може бути схвалений щодо застосування за певним рівнем SIL, але наявність сертифіката становить лише незначну частину загальних зусиль з безпеки, оскільки на відповідність необхідному рівню повинні бути перевірені значення ймовірностей відмови всіх комплексних критичних функцій у конкретному додатку. І тільки потім можуть бути визначені значення інтегральних показників надійності всього програмно–технічного комплексу системи. Система тільки тоді здатна досягти необхідного рівня інтегральної безпеки, коли весь технологічний цикл було розглянуто на відповідність цьому рівню.

Необхідно впевнитися і закріпити документально таке:

- архітектура системи відповідає специфікації;
- всі компоненти системи знаходяться на своїх місцях і правильно працюють;
- функції системи реалізовані відповідно до Технічного завдання;
- документацію розроблено відповідно до проекту.

Тільки в такому випадку може з'явитися впевненість, що SIL дійсно є інтегральним показником створеної системи і враховує всі життєво необхідні фактори:

- рівень допуску та окремих пристроїв і системи в цілому;
- опис та ідентифікацію можливих відмов і відмов спільного походження;
- процедури попередніх і періодичних випробувань;
- вимоги до експлуатації;
- метрологічне забезпечення;
- діагностику та технічне обслуговування;
- навчання та кваліфікацію персоналу.

Аналіз дерева рішень

Стислий огляд

Метод аналізу дерева рішень дозволяє послідовно подати альтернативні варіанти рішень з їх вихідними даними і відповідною невизначеністю. Як і при виконанні аналізу дерева подій, побудову слід починати з початкової події або рішення, що прийнято. Далі необхідно побудувати шляхи розвитку подій, визначити результати, що можуть бути отримані при реалізації подій, і різні рішення, які можуть бути прийняті.

Сфера застосування

Метод дерева рішень зазвичай застосовують в управлінні ризиком проектних рішень та в інших випадках, коли необхідно вибрати найкращий

спосіб дій у ситуації невизначеності. Графічне подання може бути обґрунтуванням прийнятих рішень.

Вхідні дані

Вхідними даними є план проекту із зазначенням пунктів, за якими необхідно прийняти рішення, інформація про можливі результати прийнятих рішень і події, що впливають на ці рішення.

Процес виконання методу

Побудову дерева рішень починають із початкового рішення, наприклад, рішення про відновлення проекту А або проекту В. Оскільки можлива реалізація двох гіпотетичних проектів, то далі можуть відбутися відповідні події і можуть бути прийняті різні рішення. Цей процес подають у формі дерева за аналогією з деревом подій. Імовірність подій може бути оцінена разом з оцінкою витрат та/або ефективності остаточного результату обраного шляху розвитку подій.

Інформація щодо найкращого шляху прийняття рішень має логічну форму, отже, можливий розрахунок найбільшого середнього значення, розрахованого як добуток всіх умовних ймовірностей на цьому шляху прийняття рішень на значення отриманого результату.

Вихідні дані

Вихідними даними методу є:

– логічний аналіз ризику, що відображає різні варіанти можливих рішень;

– очікуване значення ризику для кожного можливого шляху рішень.

Переваги та недоліки

Переваги методу:

– метод забезпечує точне графічне подання всіх деталей вирішення проблеми;

– метод дозволяє розрахувати кращі шляхи вирішення проблеми.

Недоліки методу такі:

– великі дерева рішень занадто складні для обміну інформацією із зацікавленими сторонами;

– застосування діаграми дерева рішень може призвести до зайвого спрощення ситуації.

Аналіз впливу людського фактора (HRA)

Стислий огляд

Метод HRA – Human Reliability Assessment – застосовують для оцінки впливу дій людини, в тому числі помилок оператора, на роботу системи.

У багатьох процесах існує можливість помилки оператора, особливо якщо у нього недостатньо часу для прийняття рішень. Імовірність того, що події розвиватимуться так, що призведуть до серйозних проблем, повинна бути малою. Проте в деяких випадках дія оператора може бути єдиним захистом, що запобігає катастрофічним наслідкам відмови.

Значущість оцінки дій оператора підтверджується подіями, в яких критичні помилки оператора сприяли катастрофічному розвитку подій. Ці події показують неприйнятність оцінок ризику, які враховують лише технічні та програмні засоби системи. Вони показують небезпеку ігнорування помилок оператора. Більш того, оцінка дій оператора дозволяє виявити помилки, які можуть негативно впливати на продуктивність, і визначити способи усунення цих помилок та інших відмов (технічних і програмних засобів).

Сфера застосування

Метод HRA може бути використаний в якісному, а також у кількісному вигляді. Якісна оцінка дій оператора може бути використана для ідентифікації його можливих помилок і їх причин, що дозволяє знизити ймовірність таких помилок. Крім того, метод HRA може бути використаний для отримання кількісних даних про відмови, пов’язані з помилками оператора, для застосування FTA або інших методів.

Вхідні дані

Вхідними даними методу HRA є:

– інформація для визначення завдань, що виконуються операторами;

– дані про типові помилки, що зустрічаються на практиці, і їх причини;

– експертні оцінки помилок оператора (людини) та їх кількісне вираження.

Процес виконання методу

Процес HRA включає такі етапи:

– постановку завдання. Визначення типів дій оператора (людини), які повинні бути досліджені й оцінені;

– аналіз завдання. Визначення способів виконання завдання і допоміжних засобів, необхідних для його виконання;

– аналіз помилки оператора. Визначення відмов, що виникають у процесі виконання завдання, можливих помилок оператора і способів їх усунення;

– подання. Визначення того, як ці помилки при виконанні завдання в поєднанні з іншими подіями, пов’язаними з устаткуванням, програмним забезпеченням і іншими факторами, можуть бути використані для розрахунку ймовірності відмови системи в цілому;

– попередню перевірку. Визначення помилок або завдань, що потребують детальної кількісної оцінки;

– кількісну оцінку. Визначення ймовірності помилок оператора і відмов при виконанні завдання;

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

– скорочення помилок. Визначення способів скорочення кількісних помилок оператора;

– документування. Визначення інформації та деталей аналізу HRA, які повинні бути зареєстровані.

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

Вихідні дані

Вихідними даними методу є:

– перелік помилок, які можуть відбутися, і методи їх скорочення (переважно через модернізацію системи);

– види помилок, причини і наслідки типових помилок;

– якісна чи кількісна оцінка ризику розглянутих помилок.

Переваги та недоліки

Переваги методу HRA:

– метод HRA забезпечує формалізований спосіб дослідження помилок оператора при оцінці ризику для систем, в яких персонал відіграє важливу роль;

– формалізоване дослідження видів помилок оператора і способів їх усунення, дозволяє зменшити ймовірність відмов, спричинених цими помилками.

Недоліки методу такі:

– складність і різноманіття способів поведінки операторів створює значні труднощі при визначенні простих видів відмови та оцінки їх ймовірності;

– неможливо описати багато дій операторів за допомогою понять «працездатний» і «непрацездатний» стан. Метод HRA важко застосувати в ситуації з частковими відмовами або відмовами через прийняття невідповідних рішень (приклад на рис. 5.12).

Аналіз «краватка-метелик»

Стислий огляд

Аналіз «краватка–метелик» є схематичним способом опису та аналізу шляху розвитку небезпечної події від причин до наслідків. Цей метод поєднує дослідження причин події за допомогою дерева несправностей і аналіз наслідків за допомогою дерева подій. Однак основну увагу методу «краватка–метелик» сфокусовано на бар'єрах між причинами і небезпечними подіями, небезпечними подіями та наслідками. Діаграми «краватка–метелик» можуть

бути побудовані на основі виявлених несправностей і дерев подій, але частіше їх будують безпосередньо в процесі проведення мозкового штурму.

Сфера застосування

Аналіз «краватка–метелик» використовують для дослідження ризику на основі демонстрації діапазону можливих причин і наслідків. Метод необхідно застосовувати в ситуації, коли складно провести повний аналіз дерева несправностей, або коли дослідження більшою мірою спрямоване на створення

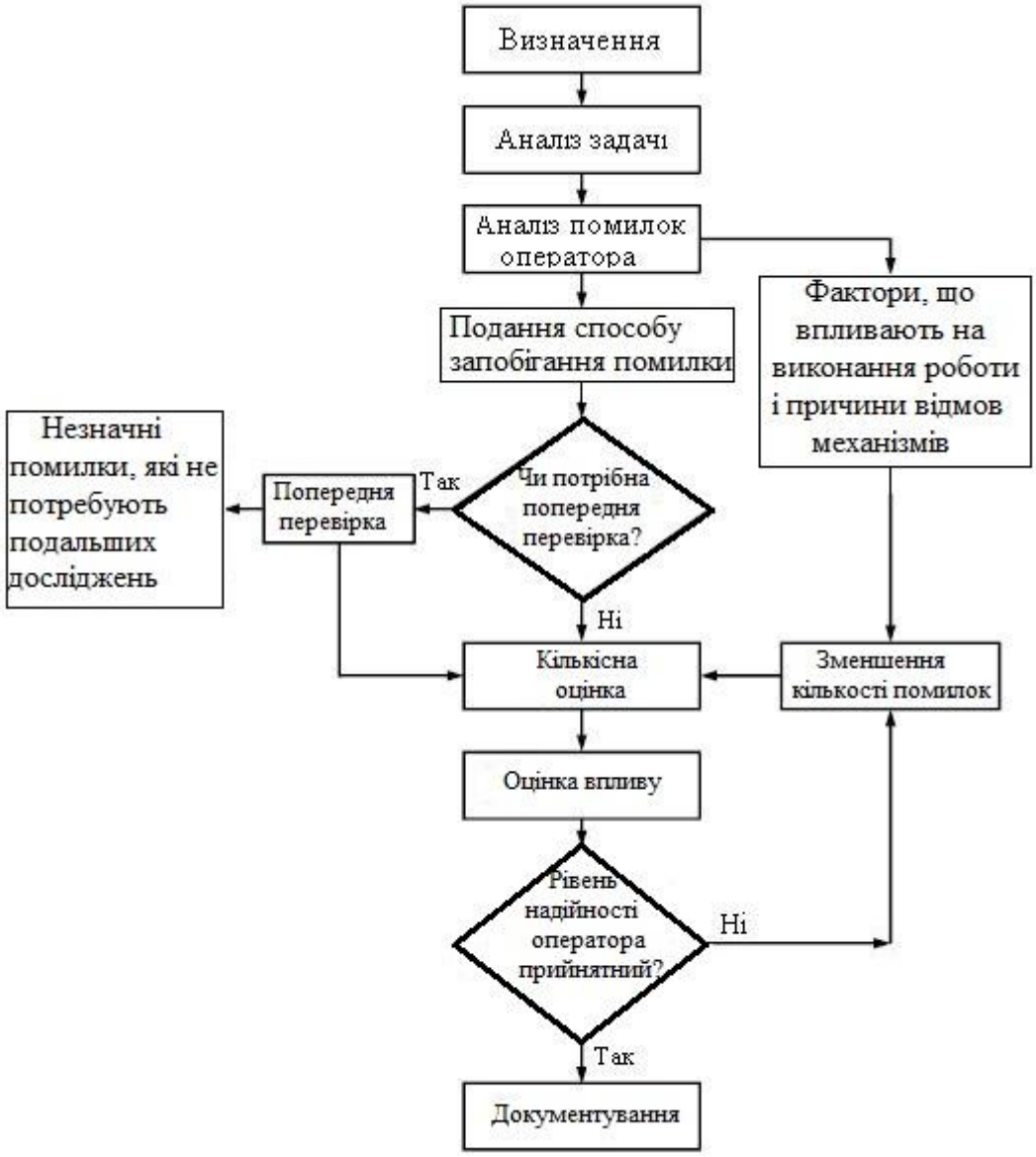

Рисунок 5.12 – Приклад аналізу впливу людського фактора

бар’єрів або засобів управління для кожного шляху відмови. Метод може бути корисний у ситуації, коли існують точно встановлені незалежні шляхи, що призводять до відмови. Аналіз «краватка-метелик» часто значно простіший для розуміння, ніж аналіз дерева подій або дерева несправностей, і, отже, він може бути корисний для обміну інформацією при використанні більш складних методів.

Вхідні дані

Вхідними даними методу є інформація про причини та наслідки небезпечних подій, ризиків, бар’єрів та засоби управління, які можуть їм запобігти, пом’якшити або стимулювати.

Процес виконання методу

Аналіз «краватка-метелик» слід будувати згідно з такими процедурами.

1. Визначення небезпечної події, обраної для аналізу, і відображення її центрального вузла «краватки-метелика».

2. Складання переліку причин події за допомогою дослідження джерел ризику (або небезпеки).

3. Ідентифікація механізму розвитку небезпеки до критичної події.

4. Проведення лінії, яка відокремлює причину від події, що дозволяє сформувати лівий бік метелика. Додатково можуть бути ідентифіковані і включені в діаграму фактори, які можуть призвести до ескалації небезпечної події та її наслідків;

5. Нанесення поперек лінії вертикальних перешкод, відповідних бар’єрам, які запобігають небажаним наслідкам. Якщо визначено фактори, які можуть спричиняти ескалацію небезпечної події, то додатково можуть бути подані бар’єри, що відвертають подібну ескалацію. Цей підхід може бути використаний для позитивних наслідків, коли перепони відображають засоби управління, що стимулюють появу і розвиток події.

6. Ідентифікація в правому боці метелика різних наслідків небезпечної події і проведення ліній, що з’єднують центральну подію з кожним можливим наслідком.

7. Зображення бар’єрів перешкод у напрямку до наслідку. Цей підхід може бути використаний для позитивних наслідків, коли перепони відображають засоби управління, що забезпечують появу сприятливих наслідків.

8. Відображення під діаграмою «краватка-метелик» допоміжних функцій управління, що належать до засобів управління (таких, як навчання і перевірка), і поєднання їх із відповідним засобом управління.

У діаграмі «краватка-метелик» можуть бути застосовані деякі види кількісної оцінки, наприклад, у ситуації, коли незалежні шляхи і відома ймовірність конкретних наслідків або результатів (рис. 5.13). Подібна кількісна оцінка необхідна для забезпечення ефективності управління. Однак потрібно враховувати, що в багатьох ситуаціях шляхи та бар’єри взаємозалежні, і засоби управління можуть бути пов’язані з обраним методом оцінки, отже, ефективність управління є невизначеною. Кількісну оцінку для аналізу «краватка–метелик» часто виконують за допомогою методів FTA і ETA.

Вихідні дані

Вихідними даними методу є проста діаграма, що показує основні шляхи небезпечних подій і встановлені бар’єри, спрямовані на запобігання або пом’якшення небажаних наслідків та/або посилення і прискорення очікуваних наслідків.

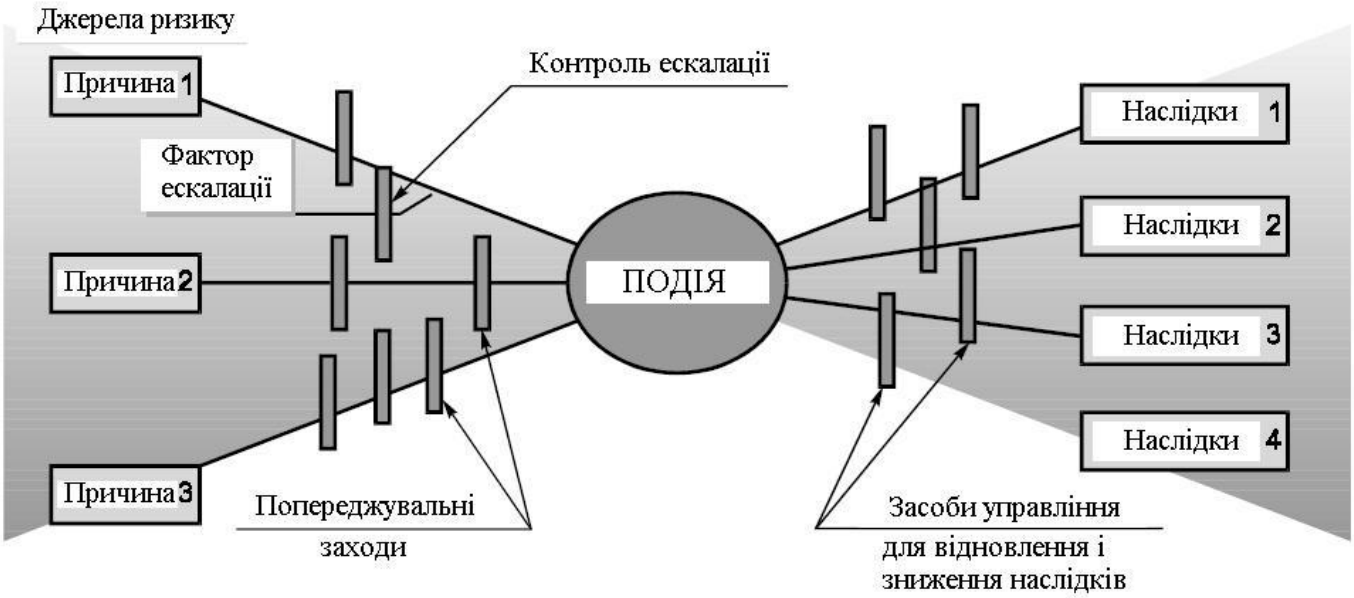

Рисунок 5.13 – Приклад діаграми «краватка–метелик» для небажаних наслідків

Переваги та недоліки

Переваги методу аналізу «краватка-метелик»:

– метод забезпечує наочне, просте і зрозуміле графічне подання проблеми;

– метод орієнтований на засоби управління, спрямовані на попередження та/або зменшення наслідків небезпечних подій, і оцінку їх ефективності;

– метод може бути застосований щодо сприятливих наслідків;

– застосування методу не потребує залучення висококваліфікованих експертів.

Недоліки методу такі:

– метод не дозволяє відображати сукупності причин, що виникають одночасно і спричиняють наслідки (випадок, коли в дереві несправностей, що відбиває лівий бік діаграми, знаходиться логічний елемент «І»);

– метод може подати складні ситуації в надмірно спрощеному вигляді, особливо при застосуванні кількісної оцінки.

Технічне обслуговування, спрямоване на забезпечення надійності (RCM)

Стислий огляд

Технічне обслуговування, спрямоване на забезпечення надійності (RCM), є методом визначення політики проведення технічного обслуговування, спрямованої на попередження відмов і способів її впровадження для досягнення необхідного рівня безпеки, експлуатаційної готовності та економічності функціонування для всіх типів устаткування.

Метод RCM широко й успішно застосовують у різних галузях промисловості. Метод RCM забезпечує прийняття рішень щодо встановлення ефективних вимог до технічного обслуговування обладнання відповідно до вимог безпеки та експлуатації обладнання, а також економічних наслідків ідентифікованих відмов і механізмів, що призводять до відмови. Результатом застосування методу є рішення про виконання завдань технічного обслуговування або інших дій, таких, як внесення функціональних змін у продукцію або процес. Детальний опис використання та застосування RCM наведено в МЕК 60300–3–11.

Сфера застосування

Цей метод можна застосовувати до завдань, пов’язаних із забезпеченням безпеки персоналу, охороною навколишнього середовища, експлуатаційними або економічними проблемами. Вибір критеріїв залежить від особливостей продукції і способів її використання. Наприклад, процес виробництва має бути економічно доцільним, і тому його ефективність залежить від витрат, пов’язаних із виконанням встановлених екологічних вимог; у тому числі до захисного обладнання ставлять більш високі експлуатаційні вимоги, але менш суворі критерії в галузі безпеки, економіки та екології. Метод дає найбільші переваги, якщо аналіз спрямований на види відмов, що призводять до серйозних наслідків у сфері безпеки, екології, економіки або функціонування обладнання.

Метод RCM використовують для забезпечення ефективного технічного обслуговування і зазвичай застосовують на етапі проектування і розробки, а потім впроваджують на етапі виробництва і технічного облуговування.

Вхідні дані

Для успішного застосування методу RCM необхідне знання обладнання, виробничого середовища, конструкції досліджуваного об’єкта, взаємодіючих із ним систем, підсистем та елементів обладнання, а також можливих відмов та їх наслідків.

Процес виконання методу

Основними етапами виконання методу RCM є:

– ініціювання та планування;

– аналіз функціональних відмов;

– вибір завдань технічного обслуговування;

– впровадження;

– постійне поліпшення.

Метод RCM заснований на методах досліджень у сфері ризику, тому що включає етапи оцінки ризику.

В даному випадку тип оцінки ризику – це аналіз видів, наслідків та критичності відмов (FMECA), що потребує спеціального підходу при використанні в цій сфері застосування.

Ідентифікацію ризику зазвичай застосовують у ситуаціях, коли частота та/або наслідки відмов можуть бать усунені або зменшені виконанням технічного обслуговування. При цьому ідентифікують функціональні й експлуатаційні вимоги та відмови устаткування і компонентів, які можуть призвести до невиконання цих вимог.

Аналіз ризику включає оцінку частоти кожної відмови без виконання технічного обслуговування. Наслідки встановлюють шляхом визначення впливу відмови. Матриця ризику, що поєднує в собі частоту відмов та їх наслідки, дозволяє встановити категорії та рівні ризику. Далі необхідно провести оцінку ризику шляхом вибору відповідної політики управління щодо

кожного виду відмови. Весь процес RCM необхідно задокументувати для подальшого аналізу. Збір даних про відмови і даних, пов’язаних із технічним обслуговуванням, дозволяє проводити моніторинг результатів та впроваджувати необхідні удосконалення.

Вихідні дані

Метод RCM дає можливість встановити завдання в галузі технічного обслуговування, такі, як моніторинг технічного стану, планові ремонт і заміна, виявлення відмов або поточне технічне обслуговування. Інші можливі дії, які можуть настати слідом після цього аналізу, передбачають модернізацію обладнання, внесення змін до експлуатаційних документів та процедури технічного обслуговування та/або проведення додаткового навчання. В рамках аналізу також необхідно ідентифікувати періодичність виконання завдань і необхідні ресурси.

Посилання на стандарти

IEC 60300–3–11 Управління загальною надійністю. Частина 3–11. Керівництво з застосування. Технічне обслуговування, спрямоване на забезпечення надійності.

Аналіз прихованих дефектів і аналіз паразитних кіл (SA)

Стислий огляд

Аналіз прихованих дефектів (SA – Sneak Analysis) є методом ідентифікації помилок проектування. До прихованих дефектів можуть належати неявні дефекти комп’ютерного обладнання, програмного забезпечення або їх поєднання, що можуть спричинити подію або перешкоджати реалізації очікуваної події і не є наслідком відмови компонентів. Ці дефекти мають випадковий характер і можуть бути не виявлені під час випробувань і тестування. Приховані дефекти можуть призвести до невідповідного виконання технологічних операцій, відмови системи, затримок у роботі програм і навіть травмування або загибелі персоналу.

Сфера застосування

Аналіз паразитних кіл (SCA – Sneak Circuit Analysis) був розроблений наприкінці 1960–х років для НАСА з метою перевірки функціональних можливостей проекту. Цей метод був використаний для виявлення паразитних електричних кіл, а також для розробки рішень з ізолювання кожної функції. У міру технологічного прогресу методи аналізу паразитних кіл також удосконалювалися. Аналіз прихованих дефектів включає і значно перевищує за обсягами аналіз паразитних кіл. Він дозволяє виявляти проблеми як у технічних, так і в програмних засобах. Методи аналізу прихованих дефектів можуть об’єднувати різні типи аналізу, наприклад аналіз дерева несправностей, аналіз видів і наслідків відмов (FMEA), оцінку надійності та ін., в один аналіз, а отже, менше витрат за часом і коштами.

Вхідні дані

Для аналізу прихованих дефектів характерним є застосування різних методів (деревоподібні схеми, схеми типу «ліс», допоміжні фрази або запитання, що допомагають фахівцеві, який проводить аналіз, ідентифікувати наявність прихованих дефектів) для виявлення конкретного типу проблеми. Деревоподібні схеми і схеми типу «ліс» – це топологічні угруповання досліджуваної системи. Кожна деревоподібна схема являє собою підфункцію і показує всі вхідні дані, які можуть вплинути на вихідні дані розглянутої функції системи. Схеми типу «ліс» будують шляхом об’єднання деревоподібних схем, які беруть участь у формуванні вихідних даних конкретної системи. Належно побудована схема типу «ліс» відображає вихідні дані системи з урахуванням всіх пов’язаних з ними вхідних даних. Поряд з іншими вхідними даними вони стають вхідними даними для аналізу.

Процес виконання методу

Виконання методу передбачає такі етапи:

– підготовку даних;

– побудову деревоподібної схеми;

– Оцінку шляхів схеми;

– Складання заключних рекомендацій та звіту.

Вихідні дані

Паразитне коло – це непередбачений спосіб або логіка функціонування системи, які за певних умов можуть ініціювати несприятливу функцію або пригнічувати сприятливу функцію.

Паразитне коло може бути присутнім у технічних засобах, програмному забезпеченні, дії оператора або їх поєднаннях. Паразитне коло не є результатом відмови технічних засобів, а є прихованим станом, ненавмисно включеним в систему, програмним продуктом або наслідком помилки оператора. Існує чотири категорії паразитних кіл:

1. Паразитні канали: непередбачені канали, по яких струм, енергія або логічні послідовності проходять у непередбаченому напрямку.

2. Паразитний хронометраж: виникнення подій у непередбаченій або суперечливій послідовності.

3. Паразитні показання: невизначена або помилкова індикація режиму функціонування системи, яка може призвести до збою системи або стати причиною небажаної дії оператора.

4. Паразитні позначки: невідповідні або неточні позначки функцій системи, наприклад вводів системи, органів керування, каналів передачі інформації, що можуть спричинити введення оператором невірних керуючих команд у систему.

Переваги та недоліки

Переваи методу такі:

– аналіз прихованих дефектів дозволяє ідентифікувати помилки проектування;

– при спільному використанні з дослідженням HAZOP метод дає можливість отримати найкращі результати;

– метод може бути застосований до систем, які мають різні стани, наприклад, до виробництва безперервної або напівнеперервної дії.

Метод має такі недоліки:

– процес аналізу може відрізнятися від того, чи застосовується він до електричних кіл, технологічних установок, механічного обладнання або програмних засобів.

– метод залежить від правильності побудови деревоподібних схем.

Марківський аналіз

Стислий огляд

Марківський аналіз застосовують у ситуації, коли майбутній стан системи залежить тільки від її поточного стану. Цей метод зазвичай використовують для аналізу ремонтопридатності систем, які можуть працювати в багатьох режимах, і в ситуаціях, коли застосування аналізу надійності окремих блоків системи є недоцільним. Метод може бути застосований до більш складних систем, використовуючи більш високий порядок процесів Маркова, і обмежений тільки моделлю, математичними обчисленнями і припущеннями.

Процес марківского аналізу є кількісним методом і може бути дискретним (використання ймовірностей переходу між станами) або безперервним (використання коефіцієнтів інтенсивності переходу зі стану в стан). Марківський аналіз може бути виконаний вручну, однак характеристики методу дозволяють використовувати для нього комп’ютерні програми.

Сфера застосування

Марківський аналіз може бути використаний для систем із різною структурою (ремонтопридатних і неремонтопридатних), включаючи:

– системи з паралельними незалежними компонентами;

– системи з послідовними незалежними компонентами;

– системи з розподіленим навантаженням;

– резервовані системи, включаючи випадок, коли може відбутися відмова функцій перемикання;

– деградуючі системи.

Марківський аналіз використовують також для розрахування експлуатаційної готовності, включаючи розрахування необхідних компонентів запчастин для ремонту.

Вхідні дані

Вхідними даними марківського аналізу є:

– перелік різних станів системи, підсистеми або компонента (наприклад, повне функціонування, часткове функціонування (погіршення стану), відмова;

– точне розуміння можливих переходів, які необхідно змоделювати. Наприклад, при відмові шини автомобіля необхідно досліджувати стан запасного колеса і, отже, частоти його перевірок;

– швидкість переходу з одного стану в інший, зазвичай подана або ймовірністю переходу для дискретних подій, або інтенсивністю відмов (λ) і (або) інтенсивністю відновлення (μ) для безперервних подій.

Процес виконання методу

Марківський аналіз заснований на понятті «стану» (наприклад, працездатний і непрацездатний стан) і переходу між цими станами в часі в припущенні постійної ймовірності переходу. Стохастичну матрицю ймовірностей переходу використовують для опису переходів між станами та необхідних обчислень.

Для ілюстрації застосування марківського аналізу розглянемо складну систему, яка може знаходитися тільки в трьох станах: працездатному, погіршеному і непрацездатному, позначених як стани *S1, S2, S3* відповідно. У будь-який момент часу система знаходиться в одному з трьох станів. У табл. 5.3 наведено ймовірність того, що в наступний момент часу система буде перебувати в стані S_i, де і може бути 1, 2 або 3.

Таблиця 5.3 – Матриця Маркова

Стан в наступний момент часу	Стан в поточний момент часу		
	$S1$	$S2$	$S3$
$S1$	0,95	0,30	0,2
$S2$	0,04	0,65	0,6
$S3$	0,01	0,05	0,2

Цей масив ймовірностей називається матрицею Маркова або матрицею переходу. Слід зазначити, що сума в кожному стовпці матриці дорівнює 1, тому що це сума ймовірностей всіх можливих станів у кожному випадку. Система також може бути подана діаграмою Маркова, в якій кола відображають стан, а стрілки – переходи з відповідною ймовірністю (рис. 5.14).

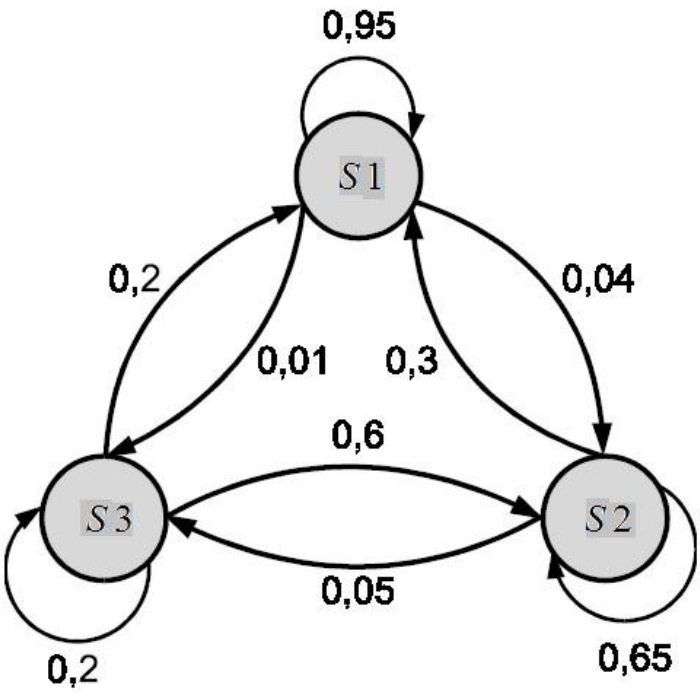

Рисунок 5.14 – Приклад діаграми Маркова для системи

Стрілки, замкнуті на одному стані, зазвичай не показують. У цьому прикладі вони наведені для повноти подання.

Якщо P_i – ймовірність перебування системи в стані i, для $i = 1, 2, 3$, то:

$$P1 = 0{,}95P1 + 0{,}30P2 + 0{,}20P3; \quad (5.1)$$

$$P2 = 0{,}04P1 + 0{,}65P2 + 0{,}60P3; \quad (5.2)$$

$$P3 = 0{,}01P1 + 0{,}05P2 + 0{,}20P3. \quad (5.3)$$

Ці три рівняння залежні, і система рівнянь не може бути розв'язана. Для розв'язання необхідно одне з наведених рівнянь виключити, замінивши його таким рівнянням:

$$1 = P1 + P2 + P3. \quad (5.4)$$

Отримані значення становлять 0,85; 0,13 і 0,02 відповідно для станів 1, 2, 3. Система є повністю функціонуючою протягом 85 % часу, в погіршеному – стані протягом 13 % часу і в стані відмови протягом 2 % часу .

Розглянемо ситуацію, коли система складається з двох послідовних елементів. Для працездатності системи обидва елементи повинні перебувати в працездатному стані. Елементи можуть бути у працездатному стані або в стані відмови. Працездатність системи залежить від стану елементів.

Можливі такі стани елементів:

– стан 1 – обидва елементи знаходяться в працездатному стані;

– стан 2 – один елемент відмовив і знаходиться на відновленні, а інший перебуває в працездатному стані;

– стан 3 – обидва елементи відмовили і знаходяться на відновленні.

Якщо інтенсивність відмови кожного елемента взяти рівною λ, а інтенсивність відновлень – рівною μ, і вони є постійними, то діаграму стану переходу можна подати у вигляді рис. 5.15.

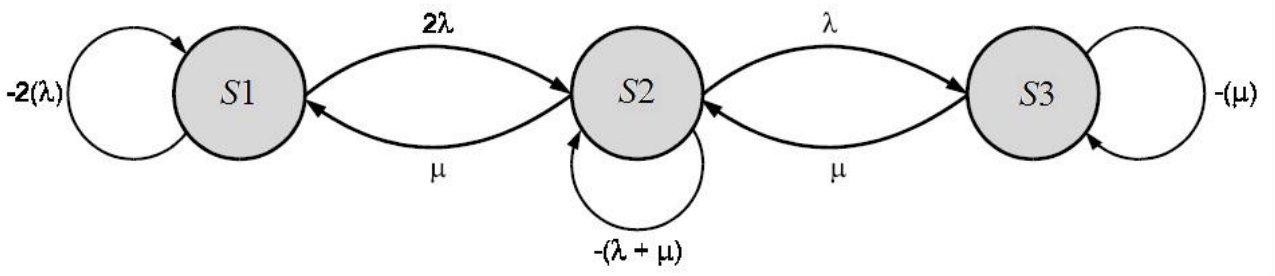

Рисунок 5.15 – Приклад діаграми станів переходу

При цьому інтенсивність переходу зі стану 1 в стан 2 дорівнює 2λ, оскільки відмова будь–якого з двох елементів надає системі стану 2.

Нехай P_i *(t)* – ймовірність перебування системи в початковому стані і в момент часу *t;* P_i *(t +* δt*)* – ймовірність перебування системи в кінцевому стані в момент часу *(t +* δt*)*.

Необхідно відзначити, що нульові значення виникають тому, що переходи неможливі із стану 1 в стан 3 або зі стану 3 у стан 1. Крім того, сума в колонці дорівнює нулю при визначенні інтенсивності.

У цьому випадку система рівнянь має такий вигляд:

$$dP1/dt = 2\,\lambda\,P1\,(t) + \mu\,P2\,(t), \qquad (5.5)$$

$$dP2/dt = 2\lambda\,P1\,(t) + -\,(\lambda + \mu)\,P2\,(t) + \mu\,P3\,(t\ \mathrm{t}), \qquad (5.6)$$

$$dP3/\,dt = \lambda\,P2\,(t) + -\mu\,P3\,(t). \qquad (5.7)$$

Для простоти можна припустити, що необхідна працездатність відповідає стійкому стану системи.

Якщо δt прямує до нескінченності, dP_i/dt прямує до нуля, що дозволяє спростити рівняння. Також необхідно використовувати додаткове рівняння (див. 5.4). Тоді рівняння $A\,(t) = P1\,(t) + P2\,(t)$ можна записати у вигляді:

$$A = P1 + P2, \qquad (5.8)$$

Отже,
$$A = (\mu 2 + 2\,\lambda\,\mu) / (\mu 2 + 2\,\lambda\,\mu + \lambda 2). \qquad (5.9)$$

Вихідні дані

Вихідними даними марківського аналізу є ймовірності перебування системи в різних станах, а отже – оцінки ймовірностей відмови та/або безвідмовної роботи істотних компонентів системи (табл. 5.4).

Таблиця 5.4 – Кінцева матриця Маркова

Кінцевий стан	Початковий стан		
	$P1(t)$	$P2(t)$	$P3(t)$
$P1(t+\delta t)$	-2λ	M	0
$P2(t+\delta t)$	2λ	$-(\lambda+\mu)$	μ
$P3(t+\delta t)$	0	λ	$-\mu$

Переваги та недоліки

Перевагою марківського аналізу є можливість обчислення ймовірностей станів систем із відновленням і множинними станами деградації.

Недоліки Марківського аналізу:

– метод заснований на припущенні про постійність ймовірностей переходу та наявнасті тільки двох можливих станів елементів системи (відмови і відновлення);

– у методі використано припущення, що всі розглянуті події статистично незалежні, таким чином, майбутні стани не залежать від минулих станів, за винятком безпосередньо попереднього стану;

– для застосування методу необхідно знати всі ймовірності переходу;

– робота з методом неможлива без знання операцій із матрицями;

– отримані результати важкі для розуміння персоналом, який не має відповідних технічних знань, навичок і досвіду.

Порівняння

Марківський аналіз аналогічний аналізу мережі Петрі за можливістю забезпечення моніторингу та спостереження за станами системи, але на відміну від мережі Петрі метод допускає існування декількох станів в один і той самий час.

Посилальння на стандарти

МЕК 61078 Методи аналізу надійності. Метод структурної схеми надійності.

МЕК 61165 Застосування марківських методів ISO / IEC 15909 (всі частини). Програмне забезпечення та системне проектування. Мережі Петрі високого рівня.

Моделювання методом Монте-Карло

Стислий огляд

Багато систем занадто складні для дослідження впливу невизначеності з використанням аналітичних методів. Однак такі системи можна досліджувати, якщо розглядати вхідні дані у вигляді випадкових змінних, повторюючи велику кількість обчислень N (ітерацій), для отримання результату з необхідною точністю.

Метод може бути застосований у складних ситуаціях, які важкі для розуміння і розв'язання за допомогою аналітичних методів. Моделі систем можуть бути розроблені з використанням таблиць та інших традиційних методів. Існують і більш сучасні програмні засоби, що задовольняють високим вимогам, багато з яких відносно недорогі. Якщо модель розробляють і застосовують вперше, то необхідна для методу Монте–Карло кількість ітерацій може зробити отримання результатів дуже повільним і трудомістким. Однак сучасні досягнення комп'ютерної техніки і розробка процедур генерації даних за принципом латинського гіперкуба дозволяють зробити тривалість обробки незначною у багатьох випадках.

Сфера застосування

Метод Монте-Карло є способом оцінки впливу невизначеності оцінки параметрів системи у багатьох ситуаціях. Метод зазвичай використовують для оцінки діапазону зміни результатів і відносної частоти значень в цьому діапазоні для кількісних величин, таких, як вартість, тривалість, продуктивність, попит та ін. Моделювання методом Монте-Карло може бути використано для двох різних цілей:

– трансформування невизначеності для звичайних аналітичних моделей;

– розрахунку ймовірностей, якщо аналітичні методи не можуть бути використані.

Вхідні дані

Вхідними даними для моделювання методом Монте–Карло є добре опрацьована модель системи, інформація про тип вхідних даних, джерела невизначеності і необхідних вихідних даних.

Вхідні дані та відповідну їм невизначеність розглядають у вигляді випадкових змінних із відповідними розподілами. З цією метою використовують рівномірні, трикутні, нормальні і логарифмічно нормальні розподіли.

Процес моделювання Монте-Карло

Процес включає такі етапи:

1) визначення моделі або алгоритму, що найбільш точно описують поведінку досліджуваної системи;

2) багаторазове застосування моделі з використанням генератора випадкових чисел для отримання вихідних даних моделі (моделювання системи). За необхідності моделюють вплив невизначеності.

Модель записують у формі рівняння, що виражає співвідношення між вхідними та вихідними параметрами. Значення, відібрані вхідні дані, отримують виходячи з відповідних розподілів ймовірностей, що характеризують невизначеність даних;

3) за допомогою комп’ютера багаторазово використовують модель (часто до 10 000 разів) із різними вхідними даними і отримують вихідні дані. Вони можуть бути оброблені за допомогою статистичних методів для отримання оцінок середнього, стандартного відхилення, довірчих інтервалів.

Розглянемо систему, що складається з двох паралельних елементів. При цьому для функціонування системи достатньо, щоб функціонував один елемент. Імовірність безвідмовної роботи першого елемента становить 0,9, а другого – 0,8.

Дані моделювання наведено в табл. 5.5.

Таблиця 5.5 – Результати застосування методу Монте–Карло до системи з двох паралельних елементів

	Елемент 1		Елемент 2		
Номер ітерації	Випадкове число	Елемент функціонує	Випадкове число	Елемент функціонує	Система
1	0,577 243	Так	0,059 355	Так	1
2	0,746 909	Так	0,311 324	Так	1
3	0,541 728	Так	0,919 765	Ні	1
4	0,423 274	Так	0,643 514	Так	1
5	0,917 776	Ні	0,539 349	Так	1
6	0,994 043	Ні	0,972 506	Ні	0
7	0,082 574	Так	0,950 241	Ні	1
8	0,661 418	Так	0,919 868	Ні	1
9	0,213 376	Так	0,367 555	Так	1
10	0,565 657	Так	0,119 215	Так	1

Для кожного елемента генератор випадкових чисел формує псевдовипадкове число з інтервалу від 0 до 1, яке зіставляють з імовірністю безвідмовної роботи елемента, потім визначають працездатність системи. При 10 повтореннях процедури результат 0,9, швидше за все, не буде досягнутий. Зазвичай обчислення продовжують до досягнення необхідного рівня точності. У цьому прикладі значення 0,9 799 для ймовірності безвідмовної роботи системи досягнуто після проведення 20 000 ітерацій.

Наведена модель може бути розширена різними способами, наприклад шляхом:

– зміни моделі взаємодії елементів у системі (наприклад, другий елемент знаходиться в резерві і вводиться в експлуатацію відразу після відмови першого елемента);

– заміни фіксованої ймовірності безвідмовної роботи на змінну (наприклад, яка підпорядковується трикутниковому розподілу), коли ймовірність безвідмовної роботи не може бути точно визначена;

– використання параметра потоку або інтенсивності відмов у поєднанні з генератором випадкових чисел для генерації напрацювань на відмову або до

відмови (експоненціальний розподіл, розподіл Вейбулла або інший розподіл) і часу відновлення. Цей Монте-Карло може бути застосований для оцінки невизначеності фінансових прогнозів, результатів інвестиційних проектів, при прогнозуванні вартості і графіка виконання проекту, порушень бізнес–процесу і заміни персоналу.

Даний метод застосовують у ситуаціях, коли результати не можуть бути отримані аналітичними методами або існує висока невизначеність вхідних або вихідних даних.

Вихідні дані

Вихідними даними можуть бути значення характеристик, як показано в наведеному вище прикладі, або розподіл ймовірності або частоти відмови, або виходом може бути ідентифікація основних функцій моделі, які надають основний вплив на вихідні дані.

Метод Монте-Карло зазвичай використовують для оцінки розподілу вхідних або вихідних результатів або характеристик розподілу, в тому числі для оцінки:

– імовірності встановлених станів;

– значень вихідних величин, для яких встановлені межі, відповідно до деяких рівнів довіри, які не повинні бути порушені.

Аналіз взаємозв’язку вхідних і вихідних величин може виявити відносне значення факторів роботи системи та ідентифікувати способи зниження невизначеності вихідних величин.

Переваги та недоліки

Переваги методу Монте-Карло:

– метод може бути адаптований до будь–якого розподілу вхідних даних, включаючи емпіричний розподіл, побудований на основі спостережень за відповідними системами;

– моделі відносно прості для роботи і можуть бути за необхідності розширені;

– метод дозволяє врахувати будь–які впливи і взаємозв’язки, включаючи такі тонкі, як умовні залежності;

– для ідентифікації сильних і слабких впливів може бути застосований аналіз чутливості;

– моделі є зрозумілими, а взаємозв’язок між входами і виходами – прозорим;

– метод допускає застосування ефективних моделей дослідження багатокомпонентних систем, таких, як мережа Петрі;

– метод дозволяє досягти необхідної точності результатів;

– програмне забезпечення методу є доступним і відносно недорогим.

Недоліки методу полягають у такому:

– точність рішень залежить від кількості ітерацій, які можуть бути виконані (цей недолік стає менш значущим зі збільшенням швидкодії комп’ютера);

– метод припускає, що невизначеність даних можна описати відомим розподілом;

– великі і складні моделі можуть становити труднощі для фахівців з моделювання і ускладнювати залучення зацікавлених сторін.

Метод не може адекватно моделювати події з дуже високою або дуже низькою ймовірністю появи, що обмежує його застосування при аналізі ризику.

Посилання на стандарти

МЕК 61649 Критерії згоди, довірчі інтервали і нижні довірчі межі для розподілу Вейбулла (IEC 61649 Weibull analysis).

Керівництво ISO / IEC 98–3:2008 Невизначеність вимірювання. Частина 3. Керівництво за вираженням невизначеності вимірювання.

Байєсівський аналіз і Мережа Байєса

Стислий огляд

Створення байєсівського аналізу приписують преподобному Томасу Байєсу. Для оцінки повної ймовірності він запропонував об’єднати апріорні дані з апостеріорними.

Загальний вигляд теореми Байєса:

$$P(A \mid B) = \{P(A)\, P(B \mid A)\} / \Sigma P(B \mid E_i)\, P(E_i), \quad (5.10)$$

де $P(X)$ – ймовірність події X; $P(X \mid Y)$ – ймовірність події X за умови, що відбулася подія Y; E_i – i–а подія.

У найпростішій формі теорему Байєса можна записати:

$$P(A \mid B) = \{P(A)\, P(B \mid A)\} / P(B). \quad (5.11)$$

Байєсівський аналіз відрізняється від класичної статистики припущенням, що параметри розподілів є не постійними, а випадковими змінними. Імовірність Байєса можна легко зрозуміти, якщо розглядати її як ступінь впевненості в певній події в протилежність класичному підходу, заснованому на об’єктивних свідченнях. Оскільки підхід Байєса заснований на суб’єктивній інтерпретації ймовірності, то він може бути корисний при виборі рішення та розробці мереж Байєса (або мереж довіри).

Мережа Байєса є графічною моделлю, що являє собою змінні та їх імовірнісні взаємозв’язки. Мережа складається з вузлів – випадкових змінних і стрілок, що пов’язують батьківський вузол з дочірнім вузлом (батьківський вузол – це змінна, яка безпосередньо впливає на іншу дочірню змінну).

Сфера застосування

Теорії та мережі Байєса широко застосовують з причини їх інтуїтивної зрозумілості та завдяки наявності відповідного програмного забезпечення. Мережі Байєса використовують у різних галузях: медичній діагностиці, моделюванні зображень, генетиці, розпізнаванні мови, економіці, дослідженні космосу і в сучасних пошукових системах. Їх можуть застосовувати в будь-якій сфері, де потрібне встановлення невідомих змінних за допомогою використання структурних зв’язків і даних. Мережі Байєса можуть бути застосовані для вивчення причинних зв’язків, поглиблення розуміння проблемної сфери та прогнозування наслідків втручання в систему.

Вхідні дані

Вхідні дані для аналізу та мережі Байєса подібні вхідним даним для моделі Монте-Карло. Для мережі Байєса (рис. 5.16) основними етапами є:

– визначення змінних системи;

– визначення причинних зв’язків між змінними;

– визначення умовних і апріорних ймовірностей;

– додавання об’єктивних свідчень до мережі;

– оновлення довірчих оцінок;

– визначення апостеріорних довірчих оцінок.

Процес виконання методу

Теорія Байєса може бути застосована різними способами. У наведеному прикладі розглянуто побудову таблиці Байєса для проведення медичних досліджень з визначення наявності у пацієнта захворювання (табл. 5.6). До початку досліджень передбачається, що у 99 % населення цього захворювання немає, у 1 % – захворювання є (апріорна інформація). Достовірність тесту така, що якщо у людини є захворювання, то результати тестів позитивні в 98 %. Якщо у людини захворювання відсутнє, результати тесту позитивні в 10 %.

Таблиця 5.6 – Таблиця Байєса

Ознака	Апріорна ймовірність	Умовна ймовірність правильності тесту	Добуток ймовірностей	Апостеріорна ймовірність
Є захворювання	0,01	0,98	0,0098	0,0901
Немає захворювання	0,99	0,10	0,0990	0,9099
Сума	1		0,1088	1

Застосовуючи теорему Байєса, результат визначають множенням апріорної ймовірності на умовну ймовірність. Апостеріорні ймовірності визначають діленням значення окремого результату на суму результатів. Результати розрахунку показують, що стосовно позитивного результату тесту апріорне значення зросло з 1 до 9 %. Більш того, велика ймовірність того, що навіть при позитивному результаті тесту наявність захворювання

малоймовірна. Аналіз рівняння (0,01 · 0,98) / ((0,01 · 0,98) + (0,99 · 0,1) показує, що позитивний результат за відсутності захворювання важливий для апостеріорних значень.

Розглянемо таку мережу Байєса:

Згідно з умовними апріорними ймовірностями, визначеними в таблицях, і позначеннями *Y* – позитивний, а *N* – негативний, позитивний результат вказує на наявність захворювання.

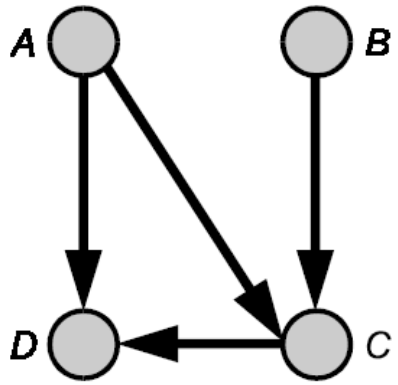

Рисунок 5.16 – Приклад мережі Байєса

Таблиця 5.7 – Апріорні ймовірності для вузлів *A* і *B*

P (A = Y)	*P (A = N)*	*P (B = Y)*	*P (B = N)*
0,9	0,1	0,6	0,4

Таблиця 5.8– Умовні ймовірності, визначені для вузла *C* з вузлами *A* і *B*

A	*B*	*P(C = Y)*	*P(C = N)*
Y	*Y*	0,5	0,5
Y	*N*	0,9	0,1
N	*Y*	0,2	0,8
N	*N*	0,7	0,3

Таблиця 5.9 – Умовні ймовірності, визначені для вузла *D* з вузлами *A* і *C*

A	*C*	*P (D = Y)*	*P (D = N)*
Y	*Y*	0,6	0,4
Y	*N*	1,0	0,0
N	*Y*	0,2	0,8
N	*N*	0,6	0,4

Для визначення апостеріорної ймовірності *P (A | D = N, C = Y)* необхідно спочатку обчислити *P (A, B | D = N, C = Y)*.

Використовуючи правило Байєса, значення ймовірності *P (D | A, C)* × *P (C | A, B)* × *P (A)* × *P (B)* необхідно визначити за формулою, як показано нижче в таблиці, при цьому в останньому стовпці вказані нормалізовані ймовірності, сума яких дорівнює 1, як показано в попередньому прикладі.

Таблиця 5.10 – Апостеріорна ймовірність для вузлів *A* і *B* з вузлами *D* і *C*

A	*C*	*P (D = Y)*	*P (D = N)*
Y	*Y*	0,4 · 0,5 · 0,9 · 0,6 = 0,110	0,4
Y	*N*	0,4 · 0,9 · 0,9 · 0,4 = 0,130	0,48
N	*Y*	0,8 · 0,2 · 0,1 · 0,6 = 0,010	0,04
N	*N*	0,8 · 0,7 · 0,1 · 0,4 = 0,022	0,08

Для отримання *P (A | D = N, C = Y)* всі значення *B* підсумовують.

Таблиця 5.11 – Апостеріорна ймовірність для вузла *A* з вузлами *D* і *C*

P (A=Y|D=N, C=Y)	*P (A=N|D=N, C=Y)*
0,88	0,12

Отримані результати свідчать, що апріорна ймовірність *P (A = N)* збільшилася з 0,1 до 0,12 (апостеріорні дані) і зміни є незначними. З іншого

боку, значення ймовірності $P\ (B = N|D = N,\ C = Y)$ змінилося з 0,4 до 0,56. Ця зміна вже більш істотна.

Вихідні дані

Байєсівський підхід може бути застосований такою самою мірою, що і класична статистика, з отриманням широкого діапазону вихідних даних, наприклад при аналізі даних для отримання точкових оцінок і довірчих інтервалів. Мережі Байєса використовують для отримання апостеріорних розподілів. Графічні подання вихідних даних забезпечують простоту розуміння моделі, при цьому дані можуть бути легко змінені для дослідження кореляції та чутливості параметрів.

Переваги та недоліки

Переваги методу такі:

– для використання методу достатньо знання апріорної інформації;

– логічно виведені твердження легкі для розуміння;

– застосування методу засноване на формулі Байєса;

– метод є спосібом використання суб'єктивних імовірнісних оцінок.

Недоліи методу такі:

– визначення всіх взаємодій у мережах Байєса для складних систем не завжди можна здійснити.

– підхід Байєса потребує знання безлічі умовних ймовірностей, які зазвичай отримують експертними методами. Застосування програмного забезпечення засноване на експертних оцінках.

Криві FN

Стислий огляд

Криві *FN* є способом графічного подання ймовірності подій, що викликають певний рівень небезпечних впливів для встановленої групи населення. Найчастіше ці криві відображають частоту заданої кількості жертв.

Криві *FN* відображають накопичену частоту *F*, при якій на *N* або більше представників населення буде зроблено вплив. Великі значення *N*, які можуть

виникнути з високою частотою F, становлять значний інтерес, оскільки ймовірність подій у цьому випадку велика (див.рис. 1.3).

Сфера застосування

Криві FN є способом подання результатів аналізу ризику. Багато подій мають високу вірогідність результатів із низькими наслідками і низьку ймовірність з високими наслідками. Криві FN дозволяють відобразити рівень ризику, який являє собою лінію, що описує швидше деякий діапазон, ніж окрему точку, що становить пару значень ймовірності та наслідки.

Криві FN можуть бути використані для порівняння значень ризику, наприклад, порівняння прогнозованого ризику з критеріями у вигляді кривої FN або для порівняння прогнозованого ризику з накопиченими даними про інциденти, або з критеріями прийняття рішення (також у вигляді кривої FN). Криві FN можуть бути використані при проектуванні систем, процесів або для управління існуючими системами.

Вхідні дані

Вхідними даними є:

– сукупності пар значень ймовірності та наслідків за певний період часу;

– вихідні дані, отримані в результаті кількісного аналізу ризику, що надають кількісні оцінки ймовірності для конкретних випадкових подій;

– дані накопичених записів і кількісної оцінки ризику.

Процес виконання методу

На основі наявних даних будують графік із зазначенням по осі абсцис кількості жертв (встановленого рівня небезпечних впливів, наприклад смертності), по осі ординат – ймовірності N або більшої кількості жертв. Внаслідок великого діапазону значень на осях зазвичай застосовують логарифмічний масштаб.

Криві FN можуть бути побудовані з використанням даних фактичних втрат у минулому або обчислені і побудовані на основі оцінок, отриманих методом імітаційного моделювання. Використовувані дані і зроблені припущення можуть означати, що дані двох типів кривої FN являють собою

різну інформацію та повинні бути використані окремо і для різних цілей. Теоретичні криві *FN* переважно застосовують при проектуванні системи, статистичні криві *FN* – при управлінні існуючими системами.

Застосування цих підходів окремо може потребувати значних витрат часу, тому зазвичай їх об’єднують. На основі емпіричних даних відзначають точками на графіку відому кількість жертв у відомих подіях / інцидентах за вказаний проміжок часу і за допомогою кількісного аналізу ризику доповнюють графік іншими точками шляхом екстраполяції або інтерполяції.

Якщо необхідно досліджувати нещасні випадки або аварії з низькою частотою виникнення або значущими наслідками, то для належного аналізу слід розглянути тривалі періоди часу і достатню кількість даних. Це допомагає також виявити сумнівні дані, якщо, наприклад, початкова подія змінилася в часі.

Вихідні дані

Вихідними даними є графік, що подає ризик у діапазоні значень наслідків, який можна порівнювати з критеріями, відповідними цій досліджуваній групі населення і конкретному збитку.

Переваги та недоліки

Застосування кривих *FN* є доцільним для подання інформації про ризик, який можуть застосувати керівництво і розробник системи, для обґрунтування прийняття рішень щодо рівня ризику і безпеки. Їх застосування доцільне також для подання інформації як про частоту, так і про наслідки в зручній для сприйняття формі.

Можливе застосування кривих *FN* для порівняння ризику в аналогічних ситуаціях за наявності достатніх даних. Їх не слід застосовувати для порівняння різних типів ризиків із різними характеристиками й обставинами.

Недолік застосування кривих *FN* полягає в тому, що вони не надають інформації про діапазон впливів або результатів пригод, крім відомостей про кількість осіб, які зазнали впливу. Також неможливо встановити різні способи

розвитку подій, які можуть призвести до певного збитку. Криві *FN* відображають конкретний тип наслідків, зазвичай – загибель людей. Крива *FN* є не методом оцінки ризику, а методом подання результатів оцінки ризику.

Криві *FN* є добре розробленим методом подання результатів оцінки ризику, проте для їх підготовки може знадобитися залучення кваліфікованих аналітиків, а отримані результати часто важкі для інтерпретації та оцінки ризику фахівцями, які не мають відповідної компетенції.

Індекси ризику

Стислий огляд

Індекс ризику – це міра ризику, що являє собою кількісну оцінку ризику, отриману із застосуванням балових оцінок на основі порядкових шкал. Індекси ризику застосовують для впорядкування значень ризику на основі подібних критеріїв, щоб їх можна було порівнювати. Балові оцінки застосовують до кожного компонента ризику, наприклад, до характеристик (джерел) забруднення, діапазону можливих способів впливу вибуху та його впливу на реципієнтів.

Індекси ризику є принципово якісним підходом, що застосовується для ранжирування та порівняння ризиків. У багатьох випадках, коли застосовувана модель або система недостатньо добре вивчена, або її не можна належно подати, переважно використовують якісний підхід.

Сфера застосування

Індекси ризику застосовують для класифікації видів ризику, пов’язаних із діяльністю, якщо система добре вивчена. Вони дозволяють об’єднати ряд факторів, які визначають рівень ризику в єдину балову оцінку рівня ризику.

Індекси ризику застосовують для безлічі різних видів ризику, зазвичай як засіб розмежування при класифікації ризику відповідно до його рівня. Індекси ризику застосовують для визначення видів ризику, що потребують подальшої детальної і, можливо, кількісної оцінки.

Вхідні дані

Вхідні дані отримують за результатами аналізу системи або докладного опису сфери застосування, що потребує доброго розуміння усіх джерел ризику, можливих способів реалізації небезпечних подій та їх об’єктів впливу. При отриманні показників ризику можуть бути додатково використані такі методи, як аналіз дерева несправностей, аналіз дерева подій і загальний аналіз рішень.

Оскільки вибір порядкових шкал є певною мірою довільним, то для підтвердження достовірності індексу ризику необхідно мати достатньо даних.

Процес виконання методу

Першим етапом є вивчення та опис системи. Потім визначають балові оцінки для кожного компонента так, щоб їх можна було об’єднати для отримання комплексного індексу ризику.

Метод індексів ризику є змішаним методом оцінки ризику. Наприклад, при вирішенні екологічних завдань присвоюють балові оцінки джерелам, способам і реципієнту(-ам) впливу, враховуючи, що в деяких випадках може бути кілька способів і реципієнтів впливу для кожного джерела ризику. Окремі балові оцінки об’єднують згідно зі схемою, яка враховує фізичну суть системи. Важливо, щоб балові оцінки для кожної частини системи (джерел, способів і реципієнтів) були внутрішньо узгодженими і враховували їх взаємозв’язок. Бали можуть бути присвоєні компонентам ризику (наприклад, ймовірності, впливу, наслідкам) або факторам, що збільшують ризик.

Бали можна складати, віднімати, множити та/або ділити відповідно до моделі ризику високого рівня. Слід враховувати кумулятивні ефекти за допомогою додавання балів (наприклад, додавання балів різним способам реалізації ризику). До порядкових шкал абсолютно незастосовані математичні формули. Тому, після того як система балових оцінок розроблена, достовірність моделі повинна бути підтверджена за допомогою її перевірки на відомій системі. Отримання показника ризику здійснюється ітеративним методом, і тому може знадобитися розгляд кількох різних систем для об’єднання балів, перед тим як достовірність моделі можна буде вважати прийнятною.

Невизначеність можна розглядати із застосуванням аналізу чутливості та варіюванням балових оцінок, для того щоб з'ясувати, до яких параметрів є найбільша чутливість.

Вихідні дані

Вихідні дані – це ряд чисел (комплексних індексів), які належать до конкретного джерела, і які можна порівнювати з індексами ризику, отриманими для інших джерел тієї самої системи, або які можуть бути змодельовані.

Переваги та недоліки

Цей метод має такі переваги:

– індекси ризику доцільно застосовувати для ранжирування різних ризиків;

– індекси ризику дозволяють об'єднувати безліч факторів, що впливають на рівень ризику, в єдину балову оцінку рівня ризику.

Метод має такі недоліки:

– якщо достовірність процесу (моделі) та їх вихідних даних не підтверджена належно, то результати можуть бути недостовірними. Той факт, що вихідні дані є числовим виразом значення ризику, може бути невірно тлумачено та використано, наприклад, при подальшому аналізі ефективності витрат;

– у багатьох випадках, в яких застосовують індекси ризику, відсутня основоположна модель, що дозволяє визначити лінійність або нелінійність (наприклад, логарифмічний характер) окремих балових шкал факторів ризику або інший їх вид, а також модель об'єднання факторів. У цих випадках ранжування є спочатку ненадійним, і перевірка його достовірності згідно з фактичними даними особливо важлива.

Матриця наслідків і ймовірностей

Стислий огляд

Матриця наслідків і ймовірностей є засобом поєднання якісних або змішаних оцінок наслідків та ймовірностей і застосовується для визначення або

ранжирування рівня ризику. Формат, рядки і колонки матриці залежать від сфери застосування, при цьому дуже важливо, щоб розроблена матриця відповідала ситуації, що розглядається.

Сфера застосування

Матрицю наслідків і ймовірностей застосовують для ранжирування ризиків, їх джерел та заходів з обробки ризику на підставі рівня ризику. Матрицю зазвичай застосовують як засіб попередньої оцінки, якщо було виявлено кілька видів ризику, наприклад, для визначення того, який ризик потребує подальшого або більш докладного аналізу, який ризик необхідно обробляти в першу чергу, а який слід розглядати на більш високому рівні менеджменту. Цю матрицю також застосовують для відбору видів ризику, які не потребують подальшого розгляду, а також для визначення прийнятності чи неприйнятності ризику відповідно до матриці.

Застосування матриці наслідків і ймовірностей сприяє обміну інформацією про загальне сприйняття якісних рівнів ризику в організації. Спосіб, яким встановлюють рівні ризику, і правила прийняття рішення, що належать до нього, мають відповідати особливостям організації та її діяльності.

Форму матриці наслідків і ймовірностей застосовують для аналізу критичності в FMECA або для встановлення пріоритетів після застосування дослідження HAZOP. Її також можна застосовувати в ситуаціях, коли недостатньо даних для докладного аналізу, або у випадку, коли ситуація не виправдовує витрат часу і зусиль на проведення кількісного аналізу.

Вхідні дані

Вхідними даними до процесу є шкали наслідків і ймовірностей, встановлені відповідно до вимог споживача, та матриця, яка їх об’єднує.

Шкала (або шкали) наслідків повинна охоплювати весь діапазон типів наслідків, що досліджуються (наприклад, фінансові втрати, безпека, довкілля або інші параметри залежно від сфери застосування), і враховувати можливість наслідків: від максимально можливих до найменш імовірних.

Як вибірковий приклад наведено табл. 5.12.

Шкала може мати будь-яку кількість точок. Найбільш поширені шкали, що мають 3, 4 або 5 точок.

Шкала ймовірності також може мати будь–яку кількість точок. Визначення ймовірності необхідно вибирати настільки точними й однозначними, наскільки це можливо. Якщо для визначення різних ймовірностей застосовують числові значення, то мають бути наведені одиниці виміру. Шкала ймовірності повинна охоплювати діапазон, відповідний проведеному дослідженню, з урахуванням того, що найнижча ймовірність має бути прийнятною для найбільшого наслідку, в іншому випадку всю діяльність, пов’язану з найбільшим наслідком, розглядають як неприпустиму.

Таблиця 5.12 – Приклад матриці критеріїв наслідків

Рейтинг	Фінансовий вплив	Повернення інвестицій	Здоров'я та безпека	Навколишнє і соціальне середовище	Репутація організації	Законодавче переслідування
6	100 у.о. + втрати або дохід	300 у.о. + втрати або дохід	— велика кількість жертв; — значні і незворотні наслідки для 10 осіб	— незворотна довгострокова втрата для довкілля; — соціальний шок, можливість широкомасштабного протесту населення	— міжнародний резонанс протягом декількох днів; — сукупні втрати підтримки з боку причетних сторін, втрата капіталовкладень; — зміна керівництва департаментів та меж впливу	— судове переслідування з відшкодуванням оплати в 50 у.о. + вартість збитків; — покарання пов'язане з позбавленням волі керівництва організації; — пролонгована заборона на діяльність з боку влади;
5	10-99 у.о. + втрати або дохід	30-293 у.о + втрати або дохід	— одиничні жертви; — деякі незворотні наслідки для одного або більше осіб	— пролонгована дія на навколишнє середовище; — підвищений інтерес до проблеми з боку соціуму, що вимагає значних коштів щодо виправлення ситуації	— національний резонанс протягом декількох днів; — частковий вплив на репутацію причетних сторін; — втрата підтримки причетних сторін і додаткових інвестицій	— відшкодування збитків у 10 у.о.; - проведення розслідування органами влади; — втручання в діяльність
4	1-9 у.о. + втрати	3-29 у.о. + втрати або дохі	— великі ушкодження	— велике		
3	100-900 у.о втрати дохід					
2	10					
1						

Як вибірковий приклад наведено табл. 5.13.

Матрицю побудовано із зазначенням наслідків по одній осі та ймовірності по іншій осі. В табл. 5.14 показана частина приблизної матриці зі шкалою з 6 точок для наслідків і шкалою з 5 точок для ймовірностей.

Таблиця 5.13 – Приклад матриці оцінки ризику

Рейтинг	Критерії
Ймовірно	- з великою ймовірністю відбудеться; - станеться з періодичністю « раз на тиждень »
Можливо	- може відбутися короткостроково, але з періоди - станеться з періодичністю « раз на тижд
Малоймовірно	- може статися, теоретично; - частота
Рідко	- може статися випадково; - очікувана періодичність по - тільки відбудеться
Неймовірно	- може статися з ймов - відбудеться

Таблиця 5.14 – Приклад матриці критеріїв імовірності

Клас ймовірності							
	E	IV	III	II	I	I	I
	D	IV	III	III	II	I	I
	C	V	IV	III	II	II	I
	B	V	IV	III	III	II	I
	A	V	V	IV	III	II	II
		1	2	3	4	5	6
		Клас наслідків					

Рівні ризику, встановлені для елементів таблиці, залежать від визначень, що застосовуються для шкал ймовірності та наслідків. Матриця може бути побудована з переважним впливом наслідків (як показано) або ймовірностей, або вона може бути симетричною, залежно від випадку застосування. Рівні ризику можуть бути пов’язані з правилами прийняття рішення за допомогою,

наприклад, рівня уваги з боку керівництва, або шкали часу, який потрібен для відповідного реагування.

Оціночні шкали і матриця можуть бути розроблені і на основі кількісних шкал. Наприклад, щодо надійності шкала ймовірностей може відображати наближене значення інтенсивності відмов, а шкала наслідків – витрати, спричинені відмовою, у грошових одиницях.

Застосування цього методу потребує наявності фахівців відповідної компетентності (переважно – дослідної групи) і всіх наявних даних для обґрунтування експертних висновків про наслідки та ймовірності.

Процес виконання методу

Для ранжирування ризиків користувач повинен перш за все підібрати опис наслідків, які найкраще відповідають ситуації, визначити ймовірність, з якою ці наслідки відбудуться. Потім визначити за допомогою матриці рівень ризику.

Багато небезпечних подій можуть мати діапазон результатів із різними відповідними ймовірностями. Незначні проблеми зазвичай відбуваються частіше, ніж катастрофічні події. Тому можна ранжувати часто одержувані результати, найбільш серйозні або інші поєднання ймовірності та наслідків.

У багатьох випадках потрібно приділяти увагу найбільш серйозним можливим результатам, оскільки вони становлять найбільшу загрозу і є найбільш значними. У деяких випадках необхідно ранжирувати як звичайні проблеми, так і малоймовірні катастрофи як окремі види ризику. При цьому слід розглядати ймовірність, пов’язану з обраним наслідком, а не ймовірність події в цілому.

Рівень ризику, який визначається за матрицею, може бути пов’язаний із правилом прийняття рішень, наприклад, про необхідність проведення обробки ризику.

Вихідні дані

Вихідними даними є клас кожної небезпечної події або перелік небезпечних подій із зазначенням рівня значущості.

Переваги та недоліки

Перевагами методу є:

– відносна простота використання;

– забезпечення швидкого ранжирування ризику за рівнями значущості.

Метод має такі недоліки:

– матриця повинна бути розроблена для конкретних обставин, тому що важко скласти універсальну матрицю, яку організація може застосувати в будь–яких обставинах;

– як правило, важко однозначно встановити необхідні шкали;

– застосування матриці є вельми суб'єктивним і значною мірою залежить від фахівця, що виконує оцінку;

– ризики можна об'єднувати (тобто не можна встановити, що певна кількість низьких ризиків або низький ризик, виявлений певну кількість разів, еквівалентні середньому ризику);

– поєднання або порівняння рівнів ризику для різних категорій наслідків становить певні труднощі;

– результати залежать від рівня деталізації аналізу. Чим докладніший аналіз, тим більше сценаріїв, кожен з яких має більш низьку ймовірність. Все це призводить до недооцінки фактичного рівня ризику. Спосіб, яким групують сценарії при описі ризику, має бути однаковим і визначеним на початку дослідження.

Аналіз ефективності витрат (аналіз «витрат і вигод»)

Стислий огляд

Аналіз ефективності витрат використовують для оцінки ризику в ситуації, коли необхідно порівняти очікувані витрати із загальними очікуваними вигодами (доходами та перевагами) і вибрати кращий або найбільш вигідний

варіант рішення. Цей метод є неявною частиною багатьох систем оцінки ризику.

Аналіз може бути якісним або кількісним або поєднувати в собі кількісні та якісні елементи. Кількісний аналіз ефективності витрат включає в себе всі сумарні витрати і доходи всіх причетних сторін у грошовому вираженні, які потрапляють в сферу застосування аналізу і приведені за періоди часу, в який накопичуються витрати і доходи. Вхідними даними для прийняття рішень про ризик є отримана чиста приведена вартість (NPV). Позитивне значення NPV зазвичай означає, що подія має статися. Однак в окремих випадках для негативного ризику, особливо що включає ризик для життя людини або значну шкоду довкіллю, може бути застосований принцип ALARP (рис. 5.17). Цей принцип дозволяє розділити ризик на три рівні: рівень, вище якого негативний ризик неприпустимий і не повинен бути прийнятий, інакше як в екстраординарних обставинах; рівень, нижче якого ризик незначний, і необхідно лише проводити моніторинг для підтримки низького ризику; і центральна зона, де ризик слід утримувати настільки низьким, наскільки реально можливо (ALARP). До більш низьких рівнів ризику може бути застосований суворий аналіз ефективності витрат, однак якщо значення ризику близько до неприпустимого, принцип ALARP допускає, що необхідно провести обробку ризику, якщо витрати на обробку істотно не перевищували отриману вигоду.

Сфера застосування

Аналіз ефективності витрат може бути використаний для вибору між різними рішеннями, пов’язаними з ризиком.

Наприклад:

– як вхідні дані при рішенні про необхідність обробки ризику;

– при аналізі різних форм обробки ризику і виборі найкращого варіанта;

– при виборі способу дії.

Вхідні дані

Вхідні дані включають в себе інформацію про витрати та вигоди для відповідних причетних сторін і про оцінку невизначеності цих витрат і вигод. Необхідно розглядати матеріальні та нематеріальні витрати і вигоди.

Рисунок 5.17 – Концепція ALARP

Витрати охоплюють витрачені ресурси та втрати, пов’язані з отриманням негативних результатів, вигоди охоплюють позитивні результати і зекономлені ресурси, пов’язані з можливістю уникнути негативних результатів.

Процес виконання методу

На початку процесу ідентифікують причетні сторони, які можуть зазнати витрат або отримати вигоди. В повний аналіз ефективності витрат включають всі причетні сторони.

Далі ідентифікують прямі і непрямі вигоди та витрати всіх відповідних причетних сторін, пов'язаних зі сферою застосування аналізу. Прямі вигоди – це вигоди, отримані безпосередньо від виконаних дій. Непрямі (або допоміжні) вигоди мають зазвичай випадковий характер, але можуть істотно впливати на розв'язання задачі. Прикладами непрямих вигод можуть бути підвищення репутації, задоволеність персоналу та «душевний спокій» (їх часто важко врахувати при прийнятті рішень).

Прямі витрати – це витрати, безпосередньо пов'язані з розпочатими діями. Непрямі витрати – це додаткові, допоміжні та неокупні витрати, такі, як втрата рентабельності, втрата часу вищого керівництва організації або відвернення капіталу від інших інвестицій. Застосовуючи аналіз ефективності витрат до рішень про необхідність обробки ризику, необхідно також враховувати витрати і вигоди, пов'язані з обробкою і прийняттям ризику.

При кількісному аналізі ефективності витрат після ідентифікації всіх матеріальних та нематеріальних витрат і вигод визначають їх вартість у грошовому вираженні (включаючи нематеріальні витрати і вигоди). Існують різні стандартні методи розрахунку їх вартості, засновані на таких способах розрахунку, як «готовність заплатити» і «використання замісників». Якщо, як часто трапляється, витрат зазнали за короткий проміжок часу (наприклад рік), а вигоди можуть бути отримані в довгостроковий період часу, то зазвичай для оцінки та порівняння вигод необхідно привести їх до «єдиного моменту часу». Всі витрати і вигоди подають у вигляді приведеної вартості. Для знаходження загальної чистої приведеної вартості (NPV) об'єднують всі витрати і вигоди всіх причетних сторін. Позитивне значення NPV означає, що дія вигідна. Для цілей аналізу також можна використовувати відношення витрат до вигод .

Якщо існує невизначеність у рівні витрат або вигод, то вони окремо або разом можуть бути співвіднесені з відповідними їм ймовірностями.

У якісному аналізі ефективності витрат не вживають спроб знайти вартість у грошовому вираженні для нематеріальних витрат і вигод. Замість приведення їх до єдиного моменту часу, що дозволяє підсумувати витрати і вигоди, співвідношення між витратами і вигодами розглядають якісно.

Аналогічним методом є аналіз рентабельності. Він передбачає встановлення точно певних вигод або результатів у грошовому вираженні декількома альтернативними способами. Аналіз досліджує тільки витрати і найменш дорогі шляхи досягнення вигод.

Вихідні дані

Вихідними даними аналізу ефективності витрат є інформація про відносні витрати і вигоди при різних варіантах рішень чи дій. Вихідні дані можуть бути виражені кількісно у вигляді чистої приведеної вартості (NPV), внутрішнього коефіцієнта рентабельності (IRR) або у вигляді відношення приведеної вартості вигод до приведеної вартості витрат. Якісно вихідні дані зазвичай подають у формі таблиці, в якій зіставляють різні типи витрат і вигод.

Переваги та недоліки

Переваги аналізу ефективності витрат:

– метод дозволяє порівнювати витрати і вигоди, використовуючи єдині метричні одиниці (гроші);

– аналіз забезпечує прозорість прийняття рішення;

– аналіз потребує збору докладної інформації щодо всіх можливих аспектів прийнятого рішення. Може бути корисний у підвищенні обізнаності та при обміні знаннями про проблему.

Недоліки методу:

– кількісний аналіз витрат і вигод може давати істотно різні результати залежно від методів визначення економічних значень для неекономічних вигод;

– у деяких випадках важко визначити дійсну ставку дисконтування майбутніх витрат і вигод;

– вигоди для великої групи населення оцінити достатньо важко, особливо якщо вони пов’язані з користю для суспільства;

– застосування дисконтування коштів, вигода від яких може бути отримана в довгостроковій перспективі, має незначний вплив на рішення залежно від обраної ставки дисконтування.

Метод не підходить для розгляду ризику, що зачіпає майбутні покоління, якщо встановлені дуже низькі або нульові ставки дисконту.

Мультикритеріальний аналіз рішень (MCDA)

Стислий огляд

Метою цього методу є використання ранжирування критеріїв для об’єктивної та прозорої оцінки різних варіантів рішень. У кінцевому підсумку необхідно визначити і розставити за пріоритетністю доступні варіанти рішень. Аналіз передбачає розробку матриці варіантів і критеріїв, які слід ранжувати й об’єднати для виконання загальної оцінки кожного варіанта рішення.

Сфера застосування

Метод MCDA може бути використаний для:

– порівняння декількох варіантів вирішення при первинному аналізі, в результаті якого необхідно визначити можливі найбільш кращі та невідповідні варіанти рішень;

– порівняння варіантів рішень за наявності декількох, іноді суперечливих критеріїв;

– досягнення компромісного рішення в ситуації, коли різні причетні сторони мають суперечливі цілі або цінності.

Вхідні дані

Вхідними даними є набір варіантів рішень для проведення аналізу. Критерії, засновані на поставлених цілях, можуть бути однаково застосовані до всіх варіантів рішень, щоб диференціювати їх між собою.

Процес виконання методу

Зазвичай процес включає в себе виконання групою компетентних фахівців, які представляють причетні сторони, таких дій:

1) встановлення мети;

2)визначення якісних ознак (критеріїв, показників оцінки або якісних характеристик виконання роботи) відповідно до кожної мети;

3) структурування якісних ознак за ієрархічним принципом;

4) розробки варіантів рішень, які необхідно оцінити відповідно до обраних критеріїв;

5) визначення важливості критеріїв і призначення для кожного з них вагового коефіцієнта;

6) оцінки альтернативних варіантів рішень з урахуванням критеріїв, що може бути подана у вигляді матриці балових оцінок;

7) об’єднання множинних балових оцінок для кожної якісної ознаки в єдину балову оцінку, що враховує безліч якісних ознак;

8) оцінки отриманих результатів.

Існують різні методи, відповідно до яких кожному критерію може бути призначено ваговий коефіцієнт, і різні способи об’єднання оцінок за критеріями для кожного варіанта рішення в єдину балову оцінку. Наприклад, оцінки можуть бути об’єднані у вигляді зваженої суми або зваженого виробу з використанням аналізу ієрархій та методу визначення ваг і ранжирування, основаного на попарних порівняннях. Всі ці методи припускають, що перевага якого-небудь критерію не залежить від значень інших критеріїв. Там, де це припущення не відповідає дійсності, застосовують інші моделі.

Оскільки оцінки мають суб’єктивний характер, то доцільним є проведення аналізу чутливості для встановлення тієї міри, до якої вагові коефіцієнти і оцінки впливають на загальний порядок переваг серед варіантів.

Вихідні дані

Вихідними даними методу є результати ранжирування варіантів спаданням уподобань. Якщо в процесі аналізу була складена матриця, в якій

осями є зважені критерії та оцінки кожного варіанта за критеріями, то варіанти, що не відповідають особливо значущим критеріям, можуть бути виключені.

Переваги та недоліки

Переваги методу такі:

– метод забезпечує просту структуру ефективного прийняття рішень та подання припущень і висновків;

– метод дозволяє вирішувати складні проблеми, вирішення яких неможливо за допомогою аналізу ефективності витрат;

– метод дозволяє раціонально досліджувати проблему пошуку оптимального рішення;

– метод дозволяє досягти компромісу в ситуації, коли причетні сторони мають різні цілі і, отже, критерії;

Недоліки методу такі:

– метод може зазнати впливу упередженого та неповного вибору критеріїв для прийняття рішення;

– більшість багатокритеріальних проблем не мають остаточного або однозначного рішення;

– алгоритми розрахунку, за якими визначають вагові коефіцієнти критеріїв щодо встановлених переваг або об’єднують різні думки, можуть приховувати ідеологічну основу прийняття рішення.

Метод Файн-Кінні

Стислий огляд

Широко застосовуваним методом оцінки професійного ризику є так званий метод Файн-Кінні. Отримані результати пропонуються до аналізу в зручній формі ступеня важкості шкоди за кольоровими індикаторами (табл. 5.15).

Сфера застосування

Метод застосовується у попередньому аналізі РНА та інших щодо визначення орієнтованого рівня ризику на робочому місці за суб'єктивними показниками.

Вхідні дані

Результати анкетування та опитування працівників.

Таблиця 5. 15 – Ступень важкості шкоди за кольоровими індикаторами[24]

Імовірність	**Ступінь важкості шкоди**		
	Помірна	Середня	Вкрай висока
Вкрай неймовірно	Дуже легкий 1	Невеликий 2	Середній 3
Ймовірно	Невеликий 2	Середній 3	Високий 4
Високо ймовірно	Середній 3	Високий 4	Вкрай високий 5

24. *Viacheslav Berezutskyi, Natalia Berezutskaya*. Indicators in risk management. Postep w inzynierii bezpieczenstwa. Redakcja naukowa Krystyna A. Skibniewska, Marian Lutostanski [Monografy] . Wydawnictwo UWM ul. Jana Heweliusza 14, 10-718 Olsztyn, - 2016. - P. 108-117. ISBN 978-83-7299-995-5

Процес виконання методу

Підхід, який використовується у цьому методі, заснований на комбінації ступеня схильності працівника до впливу шкідливого чинника на робочому місці, ймовірності виникнення загрози на робочому місці і наслідків для здоров'я та/або безпеки працівників у тому випадку, якщо загроза здійсниться.

Цей метод виражається формулою:

$$R = \text{Схильність} \cdot \text{Імовірність} \cdot \text{Наслідки}. \quad (5.12)$$

У методі Файн-Кінні ступінь схильності варіюється від 0 (= ніколи немає схильності) до 10 (= постійна схильність), ймовірність варіюється від 0 (= абсолютно неможливо) до 10 (= це станеться), наслідки варіюються від 1 (= мінімальні пошкодження) до 100 (= катастрофа) згідно з таким.

Схильність:

- 10 – постійна;
- 6 – регулярна (щодня);
- 3 – час від часу (щотижня);
- 2 – іноді (щомісяця);
- 1 – рідко (щорічно);
- 0,5 – дуже рідко;
- 0 – ніколи.

Імовірність:

- 10 – очікувано, що це трапиться;
- 6 – дуже ймовірно;
- 3 – незвично, але можливо;
- 1 – неймовірно;
- 0,5 – можна собі уявити, але неймовірно;
- 0,2 – майже неможливо;
- 0,1 – неможливо;
- 0 – абсолютно неможливо.

Наслідки :

• 100 – катастрофа, багато жертв;

• 40 – аварія, кілька жертв;

• 15 – дуже важкі, 1 людина загинула (відразу або через якийсь час);

• 7 – важкі, інвалідність;

• 3 – серйозні, травма та невихід на роботу;

• 1 – мінімальні, достатньо надання першої допомоги.

Проводити аналіз ризиків таким способом потрібно відповідно до класифікації ризиків у сфері ЗБР за ступенем серйозності.

Ризик :

• > 400 – вкрай високий ризик, негайне припинення діяльності;

• 200 - 400 – високий ризик, необхідні негайні удосконалення;

• 70 - 200 – серйозний ризик, необхідні удосконалення;

• 20 - 70 – можливий ризик, необхідно приділити увагу;

• 0 - 20 – невеликий, можливо прийнятний ризик.

Вихідні дані

Метод Файн–Кінні класифікує професійний ризик за п’ятьма групами:

1) дуже легкий;
2) невеликий;
3) середній;
4) високий;
5) вкрай високий.

Переваги та недоліки

Перевага методу – метод не потребує спеціальних знань фахівців, що проводять аналіз, а тому може бути використаний у будь-якій організації щодо попередньої оцінки ризиків на робочих місцях.

Недолік методу – у суб’єктивності оцінки, а тому – можливому значному рівні помилки.

Запитання для самоконтролю

1. В чому полягає суть методу мозкового штурму?

2.Хто бере участь у проведенні структурованого або частково структурованого інтерв'ю?

3. Метод Дельфі. Які недоліки та переваги цього методу?

4. В якій сфері аналізу ризиків застосовується метод контрольних листів?

5. Які вхідні дані необхідні для застосування методу попереднього аналізу небезпек (PHA)?

6. Чого очікують від групи дослідження за методом HAZOP?

7. Із чого починають застосування методу аналізу небезпеки і критичних контрольних точок?

8. Що означає «Вплив» та «Доза» у методі оцінки токсикологічного ризику?

9. Які стандартні фрази використовують у методі структурованого аналізу сценаріїв?

10. До яких етапів аналізу ризику може бути застосований метод аналізу сценаріїв?

11. В яких випадках використовують метод аналізу впливу на бізнес?

12. На що спрямоване застосування методу аналізу першопричини?

13. В якому випадку використовують метод аналізу видів і наслідків відмов; аналізу видів, наслідків та критичності відмов?

14. У чому полягає процес використання методу аналізу дерева несправностей?

15. Чи можна використовувати метод аналізу дерева подій для кількісної оцінки ризику?

16. Які два методи поєднані у методі аналізу причин та наслідків?

17. В якому вигляді подають інформацію у методі причинно–наслідкового аналізу?

18. У чому полягає процес виконання методу аналізу рівнів захисту?

19. Які вхідні дані необхідні для виконання методу аналізу дерева рішень?

20. Які події враховуються у методі аналізу впливу людського фактора?

21. Які методи поєднуються при виконанні аналізу ризику методом «краватка–метелик»?

22. Що аналізується у методі технічного обслуговування?

23. Коли та для чого було розроблено метод аналізу прихованих дефектів і аналіз паразитних кіл?

24. Які два основні поняття використовуються у марківському аналізі?

25. З яких етапів складається процес аналізу ризику у методі Монте–Карло?

26. Які дані використовуються у байєсівському аналізі ?

27. Які події відображаються у методі кривих FN?

28. В яких випадках використовують метод індексів ризику?

29. На якому етапі аналізу використовують метод – матриці наслідків і ймовірностей?

30. Які вхідні дані використовують у методі аналізу ефективності витрат (аналіз «витрат і вигод»)?

31. З чого складається процес виконання методу мультикритеріального аналізу рішень?

32. Які властивості та показники використовуються при розрахунках ризику у методі Файн–Кінні?

Тема 6. СИСТЕМНИЙ АНАЛІЗ СИСТЕМИ « ЛЮДИНА – ТЕХНІКА – СЕРЕДОВИЩЕ »

6.1. Методичні засади визначення небезпечності об’єктів та процесів.

6.2. Надійність технічних систем.

6.3. Глобальний (загальносистемний) ризик відмови системи після модернізації.

6.4. Надійність оператора.

6.5. Фактори надійності оператора.

6.6. Фактори середовища.

6.7. Ергономічні фактори.

6.1. Методичні засади визначення небезпечності об’єктів та процесів

Основним методичним принципом визначення безпечної поведінки є системно–структурний підхід, а методом – системний аналіз. У широкому розумінні поняття «системний аналіз» – сукупність методичних засобів, які використовуються для підготовки та обґрунтування рішень стосовно складних понять.

Системний аналіз, що використовується для оцінки системи «людина – техніка – середовище» (СЛТС) – це сукупність методів визначення небезпек, які виникають у системі в цілому або на рівні її компонентів. Вони передбачають застосування математичного апарату теорії імовірності і методів неформального аналізу (експертизи, опитування, евристичні методи).

Системний аналіз як метод дослідження виник наприкінці 50–х років минулого століття у складі наукової дисципліни «Безпека систем». Концепція безпеки систем зародилася у галузі ракетобудування і набула широкого застосування в авіабудівництві та аерокосмічних дослідженнях, а згодом – ядерній енергетиці, хімічній промисловості та інших галузях.

Безпека систем спрямована на виявлення небезпек, застосування засобів

запобігання та контролю цих небезпек протягом життєвого циклу системи.

Системний аналіз дає змогу виявити можливі небезпечні ситуації у системі, описати якісно і кількісно, прогнозувати їх виникнення та можливі наслідки, а отже, запобігти їм. Для цього використовуються методи теорії імовірності, статистичного аналізу та інші.

Системний аналіз включає дослідження:

- апріорні, що проводяться до виникнення небезпечних подій у СЛТС;
- апостеріорні, що проводяться після виникнення небезпечних подій у СЛТС.

Аналіз небезпек починається з досліджень, що дозволяють ідентифікувати джерела небезпеки, далі проводять детальний якісний аналіз. Вибір методу якісного аналізу визначається поставленою метою, складністю об'єкта тощо. Цей аналіз ґрунтується на розрахунках ймовірностей виникнення небезпек і статистичних показників. Кількісною оцінкою небезпеки є ризик. Методичні прийоми, що застосовуються для розрахунку ризику, наведені у попередніх темах.

Якісні методи аналізу небезпек включають:

- попередній аналіз небезпек;
- аналіз наслідків відмов;
- аналіз небезпек за допомогою дерева наслідків;
- аналіз небезпек методом потенціальних відхилень;
- аналіз помилок персоналу;
- причинно–наслідковий аналіз та інші.

Попередній аналіз небезпек включає:

- вивчення технічних характеристик системи, об'єкта, процесу джерел енергії та матеріалів, що використовуються, їх руйнівних властивостей;
- установлення відповідності технічної документації та актуального стану об'єктів та процесів принципам і нормам безпеки;
- ідентифікацію небезпек системи та її компонентів.

Аналіз наслідків відмов полягає у виділенні окремих компонентів системи

та виявленні для кожного з них можливих відмов, їх ранжуванні за ступенем небезпечності, вивченні небезпечних подій та розробці запобіжних заходів. Це переважно якісний метод ідентифікації небезпек, що ґрунтується на системному підході і має прогностичний характер.

Аналіз небезпек за допомогою дерев причин орієнтується на потенційно небезпечні події. Він полягає у виявленні усіх факторів, що можуть сприяти її виникненню. За результатами цього аналізу будують орієнтовний граф – «дерево».

Аналіз небезпек за допомогою дерева наслідків потенційної події досліджує групу подій, що призводять до небезпечних подій.

Аналіз небезпек методом потенційних відхилень досліджує режим функціонування системи, об'єктів, процесів, або їх компонентів, що відхиляються від нормативного.

Аналіз помилок персоналу полягає у відборі системи й виду робіт та ідентифікації серед них виду потенційної помилки, прогнозуванні наслідків і можливих заходів до її виправлення, оцінки імовірності помилки та її виправлення, розрахунку ризику, вибору шляхів до його зменшення.

Причинно–наслідковий аналіз виявляє причини небезпечної події, що відбулася. Він завершується прогнозом імовірних небезпечних подій і розробкою заходів щодо їх усунення. В ньому використовуються методи:

- прямі – коли за переліком причин установлюються можливі наслідки;
- зворотні – коли за небезпечними наслідками виявляються їх причини.

Найчастіше у системному аналізі СЛТС застосовуються методи, що ґрунтуються на *теорії імовірності*. Вони дозволяють не тільки встановити причину, але й прогнозувати небезпечну подію.

Теорія імовірності описує *масові події*. Масовими називають такі події, що мають місце у сукупності великої кількості практично рівноправних об'єктів. Імовірність їх виникнення (або не виникнення) обумовлена комплексом умов і незначною мірою визначається природою об'єктів. При цьому подія може відбутися, а може не відбутися. Тобто подія має випадковий характер.

Відповідно до теореми, сформульованої французьким математиком Борелем, частота появи будь-якої випадкової події за умови необмеженої кількості експериментів зводиться до імовірності цієї події. Ця теорема може бути записана у вигляді рівності

$$\lim P\{m/n \to P\} = 1, \quad n \to \infty, \tag{6.1}$$

де P – імовірність події; n – кількість незалежних дослідів; m – кількість появ події.

Подія, імовірність появи якої близька до одиниці, називається практично достовірною. А подія, імовірність появи якої близька до нуля – практично неможливою. Процеси, що виникають у системі, стан якої у кожний момент часу є випадковим, називається *стохастичними*. У СЛТС вони мають місце під час аварій, при перевтомі оператора та інших відхиленнях стану як системи в цілому, так і її компонентів. Найпростішими зі стохастичних процесів є *дискретні*. Вони повторюються через певні проміжки часу.

Стохастичні процеси з дискретним параметром називаються *стохастичними послідовностями* або *випадковими ланцюгами.* Окремий їх вид – *ланцюги Маркова* або *марківські стохастичні процеси.*

Ланцюгом Маркова називається така послідовність подій, в якій умовні імовірності наслідків кожної наступної події залежать тільки від наслідків безпосередньої події і не залежать від наслідків подій, що відбулися раніше. Якщо ці імовірності не залежать від номера події, то ланцюги Маркова називаються *однорідними*.

Застосування цього методу для аналізу небезпечних подій дозволяє визначити імовірність їх появи і запропонувати упереджуючі заходи щодо виникнення небезпек.

Наприклад, в якійсь СЛТС відбулася низка небезпечних подій (по черзі вийшли з ладу окремі її елементи). При цьому система перейшла у стан A_1, A_2… A_k. Результат кожної з таких подій залежить тільки від наслідків попередньої

події. Проаналізуємо імовірності їх появи у майбутньому, які позначимо P_{11}, $P_{12}…P_{1k}$. Використовуючи метод однорідних ланцюгів Маркова, отримаємо матрицю (таблицю) переходу:

$$\pi = \begin{pmatrix} P_{11} & \cdots & P_{1n} \\ \vdots & \ddots & \vdots \\ P_{k1} & \cdots & P_{kn} \end{pmatrix} \qquad (6.2)$$

.

Ця матриця показує, якщо система знаходилася у стані A_1, то у наступний події вона з імовірністю 1/2 залишиться у тому ж стані A_{11} і з імовірністю 1/3 перейде у стан A_{21} , у стан A_{k1} вона перейде із імовірністю 1/6. Якщо система вже знаходиться у стані A_{21}, то при наступній події вона не зможе перейти у стан A_{11} , а з імовірністю 2/3 залишиться у тому самому стані. З імовірністю 1/3 перейде у стан $A_{k1.}$ Зі стану A_{k11} система перейде з ймовірностями 1/2 у стан A_{11} або A_{21}.

Для аналізу безпеки об’єктів успішно використовується метод «дерев».

Це багатоетапний процес виявлення небезпечних ситуацій і їх причин, який за структурою нагадує дерево з розгалуженими гілками. Границі розгалуження дерева визначаються метою аналізу. Це графоаналітичний метод. До його переваг належить можливість зосередити увагу тільки на тих елементах системи і подіях, що безпосередньо є джерелом небезпеки. Існують різноманітні прийоми виявлення небезпечних ситуацій:

– із застосуванням дерев відмов;

– із застосуванням дерев подій;

– небезпечності і працездатності та ін.

При побудові методу «дерев» розрізняють три види подій:

1) основну подію – це вихідна подія, що відбиває дію або стан елемента, який визначає безпеку функціонування всієї системи, тобто подія з якої починається «дерево небезпек»;

2) провідна подія відбиває стан системи при реалізації небезпек, це подія,

що обмежує «дерево небезпек»;

3) допоміжні події, до яких належать проміжні, несуттєві, але достатньо вивчені й умовні події.

Наприклад, «дерево подій» має таку структуру:

- реалізація небезпеки – верхня частина дерева;
- тіло дерева – послідовні події, що ведуть до реалізації небезпеки і поєднані між собою певною логікою;
- стовбур – події, що ґрунтуються на статистичних або теоретичних даних щодо їх виникнення. Ці події впливають на границі розгалуження дерева (рис. 6.1).

Техніка побудови «дерев», що застосовуються для аналізу СЛТС і її складових, докладно висвітлена.

Аналіз видів, наслідків та критичності відмов елементів системи

Безпека життєдіяльності людини у СЛТС визначається великою кількістю складових. Однією з найважливіших є *надійність виробництва*. Надійність виробництва залежить від надійності технічних засобів, технологій і людини. Надійність виробництва визначається також надійністю будівельних конструкцій виробничих споруд, транспортних засобів, енергетичних систем і т. ін. Якою б досконалою не була СЛТС, і які питання не вирішувала, якщо вона не надійна, тобто часто виходить із ладу, *ефективність* її експлуатації буде низькою, а отже, небезпечною для людини і навколишнього середовища. Ефективність СЛТС розуміють як здатність системи досягати поставленої мети у заданих умовах із певною якістю.

У спрощеному вигляді ефективність функціонування СЛТС можна оцінити за виразом

$$W_{\text{с}}(t,\tau) = W_{\text{м}}(t,\tau) \cdot W_{\text{о}}(t,\tau) \cdot W_{\text{е}}(t,\tau), \qquad (6.3)$$

де $W_м$ (t ,τ) – ефективність функціонування машини; $W_о$ (t ,τ) – показник ефективності функціонування оператора; $W_е$ (t ,τ) – показник, що характеризує вплив середовища на ефективність функціонування системи.

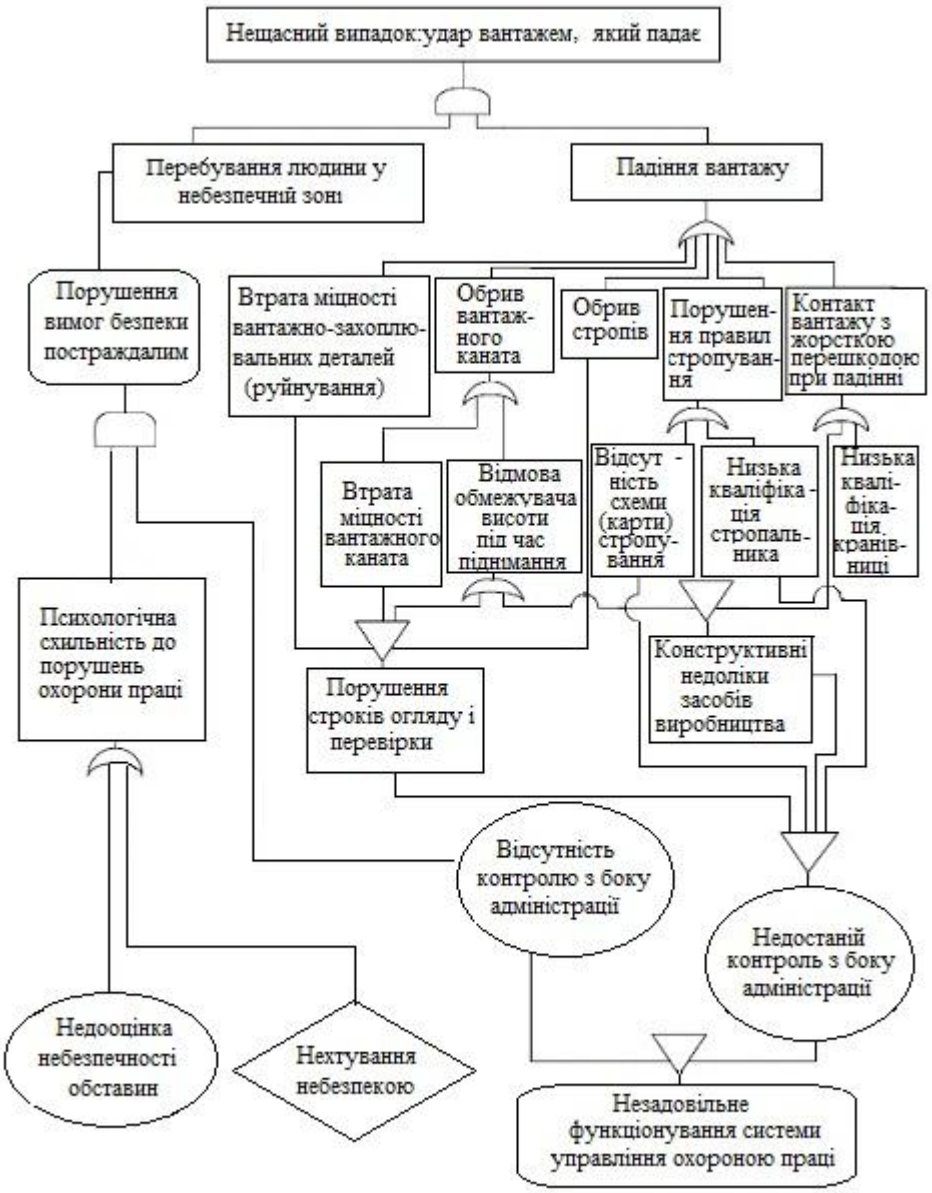

Рисунок 6.1 – Логічне дерево виникнення небезпеки удару робітника вантажем крана

Отже, ефективність функціонування СЛТС залежить від ефективності роботи як технічних ланок, так і оператора. Ефективність функціонування

СЛТС, насамперед оцінюється за показниками *надійності* й *ергономічності*, а також *ризику* виникнення небезпечних ситуацій.

6.2. Надійність технічних систем

Надійність системи розуміють, як властивість виконувати функції протягом певного часу у заданих умовах роботи. Критерії, що використовуються при оцінці надійності, наведені в табл. 6.1.

Таблиця 6.1 – Критерії оцінки надійності СЛТС та її елементів

Техніка	Людина	СЛТС
1. Імовірність безвідмовної роботи, $P(t)$ 2. Коефіцієнт готовності, $K_г$ 3. Коефіцієнт відновлення техніки, що відмовила, $P_{відн}$	1. Імовірність безпомилкової роботи, $P_{оп}$ 2. Коефіцієнт готовності оператора, $K_{оп}$ 3. Імовірність своєчасного виконання роботи, $P_{св}$ 4. Імовірність виправлення допущених помилок, $P_{випр}$	1. Імовірність виконання системою завдання, $P_{лм}$

Оцінка надійності виконується:

– при проектуванні СЛТС – для прогнозування очікуваного рівня надійності (проектна оцінка надійності);

– при експлуатації СЛТС – для визначення фактично досягненого рівня надійності (фактична оцінка надійності).

Оцінка надійності може виконуватися різними методами: *аналітичними* (розрахунковими), *експериментальними* і *шляхом моделювання*.

Надійність технічних засобів або їх елементів може оцінюватися якісно і кількісно. Якість технічного засобу розуміють, як здатність виконувати задані функції у встановлених умовах використання.

Класифікацію кількісних методів оцінки надійності СЛТС наведено на рис. 6.2.

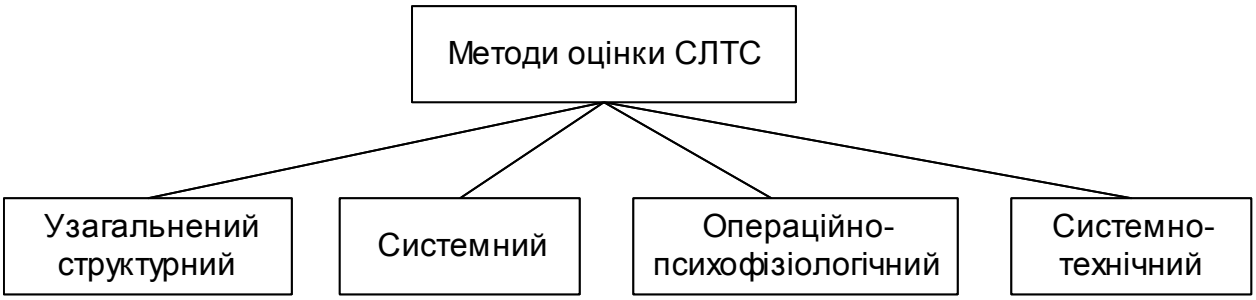

Рисунок 6.2 – Класифікація методів оцінки надійності СЛТС

При застосуванні *структурного методу* діяльність СЛТС розглядається як ряд ієрархічних рівнів, кожний з яких поданий певною структурою.

Системний метод ґрунтується на аналізі й оцінці надійності СЛТС, апаратури (приладів), безвідмовності операторів за різними функціональними рівнями (обслуговуючого, біологічного тощо).

Операційно–психологічний метод передбачає розчленування діяльності оператора на окремі дії, для яких відомі вихідні значення часу, точності та надійності виконання. На підставі цього здійснюється синтез структури діяльності й отримання інтегральних характеристик надійності СЛТС.

Системотехнічний метод розрізнює оцінку надійності систем із різними типами комплектації. На підставі цих умов визначається надійність СЛТС.

Кількісно надійність реалізується через безвідмовність, відновлюваність і довговічність. Поняття *відмови* є основним поняттям теорії надійності. Відмову розуміють, як випадкову подію, у разі якої система або її елементи повністю

або частково втрачають свою працездатність, внаслідок чого задані їм функції не використовуються.

Відмови класифікують так:

– за часом;

– за наслідками;

– за причинами виникнення;

– за характером виявлення тощо.

За часом існування і характером усунення відмови поділяються на стійкі і тимчасові. *Стійкі відмови* усуваються тільки в результаті ремонту (заміни елемента, що відмовив) або регулювання. *Тимчасові відмови* можуть зникати самостійно без втручання обслуговуючого персоналу. Тимчасові відмови, що повторюються багаторазово, називаються переміжними.

При класифікації за наслідками розрізняють *повні* і *часткові* відмови. Повна відмова виключає можливість продовжувати роботу технічного засобу. Наприклад, припинення надходження палива до паливного насоса призводить до зупинки двигуна.

Відмови технічних засобів виникають за рахунок *зносу, старіння* або через несприятливий збіг умов роботи. Знос – повільні зміни розміру й форми робочих поверхонь окремих деталей технічного засобу, що відбуваються під час його експлуатації. Старінням технічних засобів називають структурні зміни матеріалів, із яких виготовлені його деталі. Залежність *інтенсивності відмов* від терміну експлуатації технічного засобу наведено на рис. 6.3.

Причиною відмов технічних засобів можуть бути також недоліки конструктивних рішень, порушення технологічних норм їх виготовлення. Основними критеріями *безвідмовності технічних засобів* є імовірність $P(t)$ безвідмовної роботи й інтенсивність відмов.

Під імовірністю безвідмовної роботи розуміють імовірність того, що час T безвідмовної роботи засобу буде більше заданого системі часу t

$$P(t) = P\ (T > t). \qquad (6.3)$$

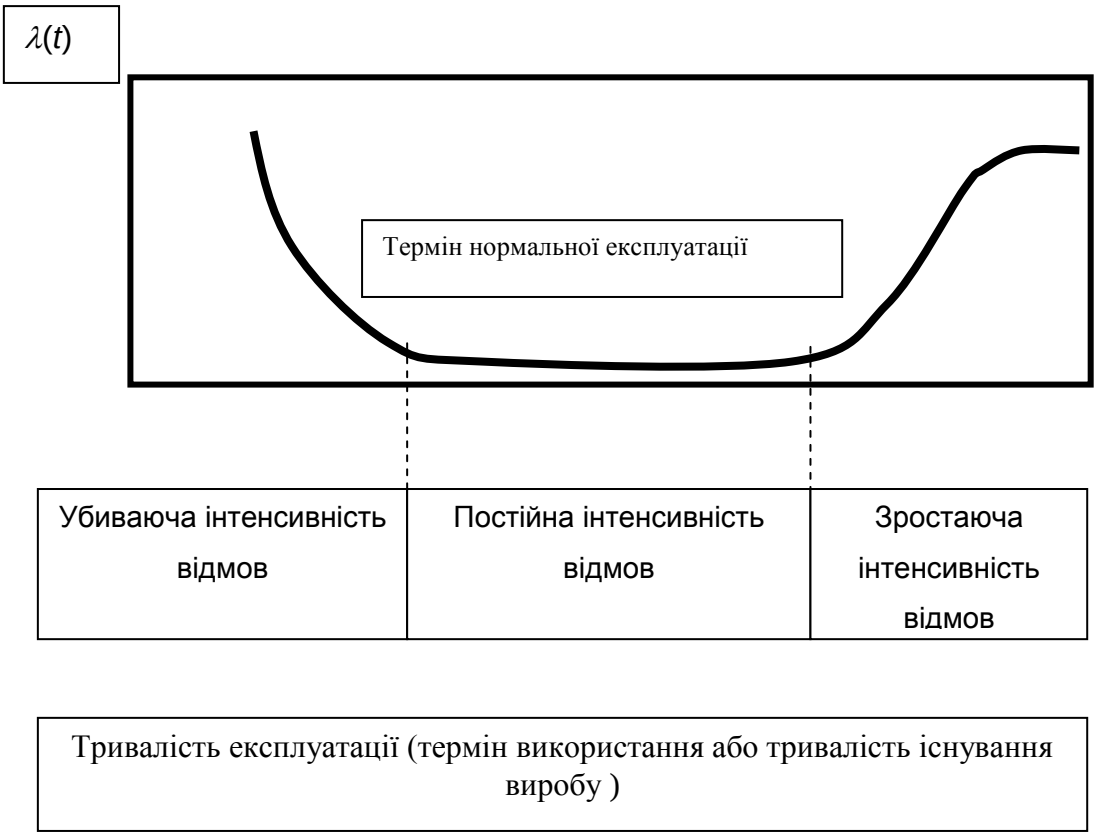

Рисунок 6.3 – Залежність *інтенсивності* відмов від терміну експлуатації технічного засобу

Імовірність безвідмовної роботи технічного засобу в будь-який час експлуатації (t) розраховується за результатами статистичної обробки даних, отриманих під час випробувань системи на надійність

$$P(t) = N_o - n(t)/N_o, \qquad (6.4)$$

де $P(t)$ – імовірність безвідмовної роботи засобу за час t; N_0 – загальна кількість засобів; $n(t)$ – число засобів, що відмовили на час роботи t.

Відмова як подія протилежна події безвідмовної роботи, визначається

$$q\,(t) = 1 - P(t), \qquad (6.5)$$

де q (t) – відмова.

Із зростанням терміну роботи від t_1 до t_2 технічного засобу імовірність його відмови безперервно зростає.

Найбільш повною характеристикою надійності елементів системи є *інтенсивність відмов*. Інтенсивність відмов визначається як відношення кількості засобів, що відмовили за одиницю часу, їх кількості, що залишилися працювати

$$\lambda(t) = dn/N_u(t)dt, \qquad (6.6)$$

де $\lambda(t)$ – інтенсивність відмов; dn – кількість засобів, що відмовила за час dt; $N_u(t)$ – кількість засобів, що пропрацювали час dt.

Імовірність відмов пов'язана з імовірністю безвідмовної роботи. Цей зв'язок отримав назву *загального закону надійності : характер зміни імовірності безпомилкової роботи технічного засобу у часі при прийнятих допущеннях залежить тільки від характеру зміни у часі інтенсивності відмов.* Його відбиває вираз

$$P(t) = e^{-\int_o^t \lambda(t)dt} \qquad (6.7)$$

де λ – інтенсивність відмов.

При $\lambda(t)$ = const формула набуває вигляду $P(t) = e^{-\lambda(t)}$.

Ця закономірність отримала назву *експоненційного закону надійності.*

Інтенсивність відмов системи, що складається з k елементів, визначають як суму інтенсивностей відмов окремих елементів. Для таких систем

$$P(t) = \prod_{i=1}^{k} P_i = \ell - \sum_{i=1}^{k} \lambda(t) \, . \qquad (6.8)$$

Використовуючи поняття згаданої вище теорії надійності, для СЛТС неперервного типу показником надійності є імовірність безвідмовного,

безпомилкового й своєчасного перебігу виробничого процесу за термін *t*. Надійність такої системи може бути подана у вигляді:

$$P_{\text{л,м, 1}}(t) = P_{\text{т}}(t) + [1 - P_{\text{т}}(t)]\, K_{\text{оп}}\, [P_{\text{оп}}\, P_{\text{св}} + (1 - P_{\text{випр}}\, (t_{\text{л}})], \qquad (6.9)$$

де $P_{\text{т}}(t)$ – імовірність безвідмовної роботи технічних засобів; $K_{\text{оп}}$ – коефіцієнт готовності оператора; $P_{\text{св}}$ – імовірність своєчасного виконання оператором необхідних дій; $P_{\text{випр}}$ – імовірність виправлення помилкових дій.

Для СЛТС змішаного типу формула для розрахунку надійності має вигляд

$$P_{\text{л,м, 2}} = K_{\text{оп}}\, [P_{\text{т}}\, P_{\text{оп}}\, P_{\text{св}} + (1 - P_{\text{т}})\, P_{\text{від}}\, P_{\text{оп}}\, P_{\text{св}} + P_{\text{оп}}) P_{\text{т}}\, P_{\text{випр}}], \qquad (6.10)$$

де $P_{\text{від}}$ – імовірність відмови техніки.

Для СЛТС дискретного типу розрахунок надійності виконують за формулою

$$P_{\text{л,м, 3}} = K_{\text{г}} P_{\text{т}} P_{\text{оп}} P_{\text{св}} + (1 - P_{\text{т}} K_{\text{г}})\, P_{\text{від}} P_{\text{оп}} P_{\text{св}} + (1 - P_{\text{оп}})\, P_{\text{т}} P_{\text{випр}}\,, \quad (6.11)$$

де $K_{\text{г}}$ – коефіцієнт готовності техніки.

Поряд із характеристиками імовірності безвідмовної роботи надійність технічних засобів визначається *коефіцієнтом готовності* $K_{\text{оп}}$

$$K_{\text{оп}} = T_{\text{о}} / T_{\text{о}} - T_{\text{п}}\,, \qquad (6.12)$$

де T_0 – час безвідмовної роботи технічного засобу за термін T; $T_{\text{п}}$ – середній час простою технічного засобу.

Розглянуті кількісні оцінки надійності функціонування технічних засобів ґрунтувалися на імовірності відмов. Іншим підходом є *визначення їх надійності за наслідками*. Він дає можливість зв’язати відмову технічного засобу з аварією

системи, готовністю її до подальшого використання. Ця залежність, наприклад, для випадку відмови польотів літаків цивільної авіації визначається за формулою

$$F(A/Q)q = \beta\,(1-\delta)(1-\eta)[(1-v) + v(1-\xi)]q, \qquad (6.13)$$

де η – імовірність відмови, яка не порушує режиму польоту; $F(A/Q)q$ – умовна імовірність наслідку A; ξ – парирування відмови після її виявлення; q – імовірність відмови технічного засобу; v – імовірність своєчасного виявлення відмови льотчиком; β– імовірність відмови технічного засобу,що визначається на підставі статистичних даних; δ – надійність роботи системи резервування.

Для випадку, пов'язаного з ремонтом авіатехніки (Д), рівняння має вигляд

$$F\,(\text{Д} / Q)\,q = q\,. \qquad (6.14)$$

Зв'язок між надійністю й відсутністю стійких відмов має вигляд

$$P(t) = K_{\text{г}} P_{\text{у}}(t)\, P_n\,(t), \qquad (6.15)$$

де $P_{\text{у}}(t)\ P_{\text{п}}\ (t)$ – імовірність відсутності стійких відмов, що перемежаються за час t.

Поряд з оцінкою надійності технічних систем з точки зору безпеки життєдіяльності людини важливе значення має такий показник, як *безпечність праці оператора* в СЛТС. Він оцінюється імовірністю безпечної роботи

$$P_{\text{бт}} = 1 - \sum_{i=1}^{n} P_{\text{вин}i}\ .\ P_{\text{пом}i}\,, \qquad (6.16)$$

де $P_{\text{вин}i}$ – імовірність виникнення небезпечної або шкідливої для людини виробничої ситуації *i*–го типу; $P_{\text{пом}i}$ – імовірність неправильних дій оператора в *i*–й ситуації; *n* – кількість небезпечних ситуацій.

Небезпечні та шкідливі ситуації можуть створюватися через технічні причини (несправність машин, аварійна ситуація, несправність захисних засобів тощо), стан умов праці та ін.

6.3. Глобальний (загальносистемний) ризик відмови системи після модернізації

Розглянемо дії особи, що приймає рішення (ОПР), які можуть призвести до повної відмови системи після її модернізації зі стану часткової відмови. Припустимо, система не задовольняє свого керівника за економічним критерієм отримання прибутку та критерієм необхідності великих вкладень на утримання системи[25]. Керівник приймає рішення про модернізацію системи за схемою (рис. 6.4).

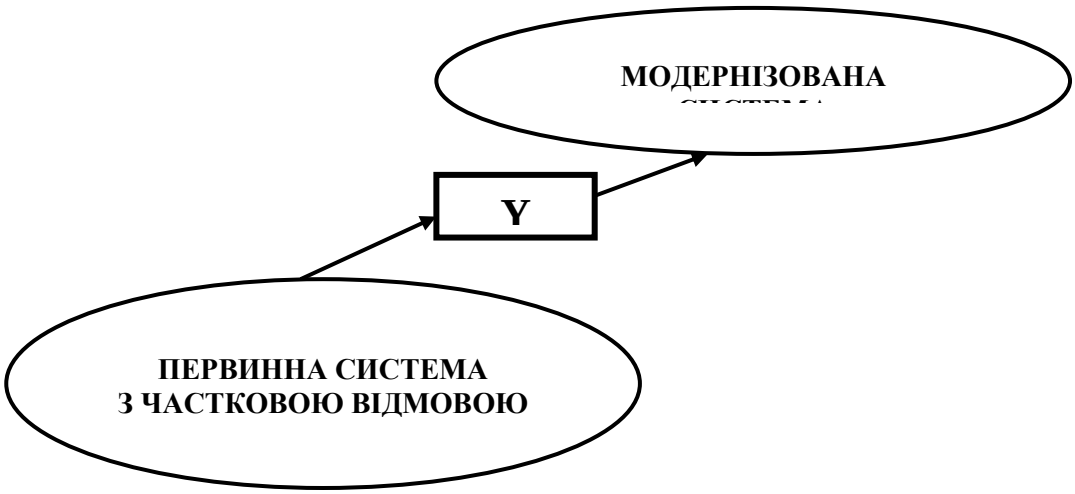

Рисунок 6.4 – Схема модернізації системи з частковою відмовою

25. Загальносистемний ризик відмови системи після модернізації. *Адаменко М.І., Березуцький В.В., Кучук Н.Г та ін.//* Системи обробки інформації : збірник наукових праць. – Х . : Харківський університет повітряних сил імені Івана Кожедуба, 2015. – Вип.10 (135). – С.113 – 118.

При цьому система 1 – це первинна система з частковою відмовою. Оператор модернізації *Y* – сукупність рішень ОПР, необхідних для втілення. Система 2 – модернізована система.

Припустимо, що оператор ОПР застосував найбільш логічні з її точки зору дії:

– підвищила вартість проїзду;

– знизила заробітну плату працівникам;

– знизила витрати на ремонт рухомого складу.

Після застосування оператора перетворення і внаслідок дій ОПР пасажиропотік повністю перейшов на альтернативний вид транспорту через неможливість оплати проїзду, звільнилися найбільш досвідчені фахівці, яких не влаштовує рівень заробітної плати, вийшла з ладу вагома частина рухомого складу. Як наслідок маємо, що модернізована система є системою з глобальною відмовою.

Зрозуміло, що приклад є надто примітивним, але він дозволяє зробити два дуже важливих висновки.

По–перше, стратегічним задумом ОПР могло бути з самого початку руйнування системи як результат дій модернізації. Як мотиви можна припустити таке: ОПР мала на увазі, що первинна система не може бути ефективно реструктуризована і підлягає знищенню за заміною іншою, що кардинально відрізняється.

Розуміючи, що після модернізації у дуже короткий термін модернізована система буде прибутковою на достатньому рівні, перед руйнуванням системи ОПР отримала максимально можливий прибуток та знищила систему з отриманням максимального прибутку від реалізації її елементів. По–друге, ОПР не врахувала усіх складових початкового завдання на модернізацію та ризику своїх дій. Якщо маємо перший варіант, то дії ОПР були повністю виправданими і привели до бажаного результату, тобто модернізована система знищується і надалі не підлягає розгляду. Якщо сценарій розвивався за іншим варіантом, то потрібно нове модернізування системи, або її переформатування,

вже зі значно більшим ризиком та зі значно більшими витратами, як це показано на рис. 6.5.

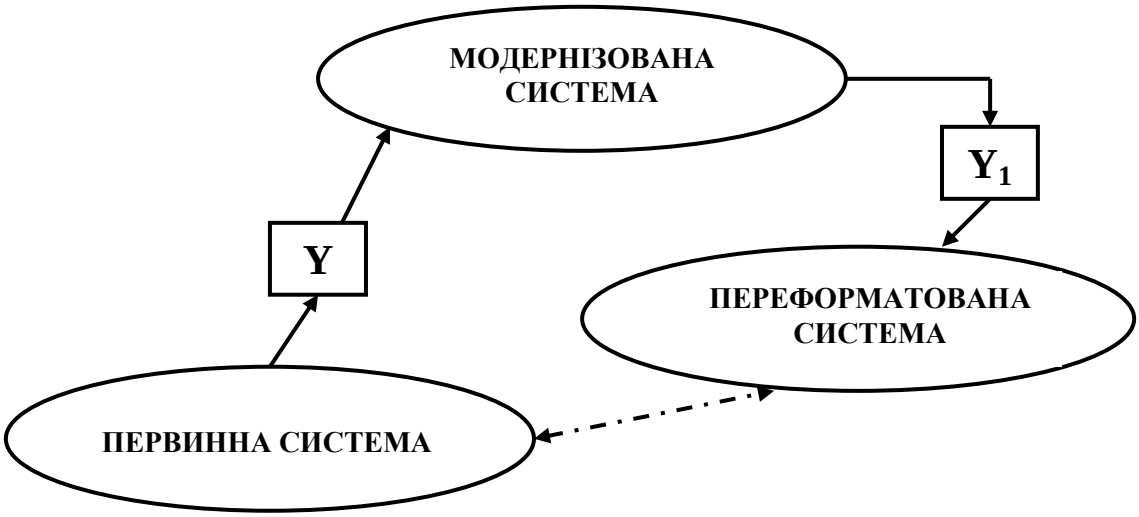

Рисунок 6.5 – Схема вторинної модернізації або переформатування системи

Потрібно відзначити, що основним розрахунком ризику у цьому випадку буде ризик перевищення витрат на вторинну модернізацію, що знов таки не буде компенсовано штатною роботою вторинної модернізованої системи. Як наслідок призведе до неможливості її поточного фінансового, технічного та кадрового утримання і знову ж – до руйнування.

Наведені приклади свідчать про те, що ефективною з точки зору глобальної модернізації системи буде тільки комплексна системна оцінка ризиків за всіма параметрами з отриманням загального ризику при визначенні факторних ризиків, тобто

$$R_{\text{ЗС}} = F\left(R_{1\Phi}, R_{2\Phi}, \ldots\right), \qquad (6.17)$$

де $R_{\text{ЗС}}$ – загальносистемний ризик; $R_{1\Phi}$, $R_{2\Phi}$, … – ризики за окремими факторами.

Формування функціональної залежності F та розв’язання рівняння (6.17) потребує первинних досліджень за вагомістю кожного з факторів ризику для особи, яка приймає рішення. Для цього пропонується двохетапний метод визначення оцінки глобального ризику відмови системи після модернізації

внаслідок помилки у початковому завданні. Серед багатьох методів визначення вагових коефіцієнтів ризиків за окремими факторами в умовах модернізації існуючої системи найбільш прийнятним є метод багатофакторного аналізу для визначення множини значущих факторів. При його застосуванні потрібно виконати таку послідовність дій:

1) визначити допустимий рівень значущості окремих факторів ризику – α;

2) визначити факторну структуру;

3) визначити максимальну кількість факторів ризику, що аналізуються, за допомогою критерію Кеттела;

4) виконати факторизацію матриці сумісних кореляцій та формування матриці факторних навантажень, визначених до процесу обертання;

5) здійснити процес прямокутного варімакс–обертання (varimax normalized) та проведення попередньої ідентифікації;

6) поліпшити якість факторної структури за принципом Терстоуна;

7) розрахувати умовне навантаження та факторні коефіцієнти.

Отримані в результаті наведеного алгоритму факторні коефіцієнти k_n є незалежними та відображають структуру як структуру взаємозв'язків окремих факторів, а також як вплив кожного із факторів на функціонування системи. Використовуючи *t*– критерій Стьюдента, можна визначити ті фактори ризику, для яких вплив на функціонування системи перевищує зазначений рівень значущості, тобто визначимо відповідну множину факторів ризику так:

$$\Re = \left\{ R_{n\Phi} \middle| \, t\left(R_{n\Phi}\right) \le t_{\alpha} \right\}, \quad \text{card}\, \Re = N\,. \qquad (6.18)$$

Множина (6.18) дозволяє визначити вагові коефіцієнти всіх її елементів:

$$\beta_n = \frac{k_n}{\sum\limits_{i=1}^{N} k_i} \quad \forall n \in \overline{1,N}; \quad \sum_{n=1}^{N} \beta_n = 1. \qquad (6.19)$$

Для вибору критерію ефективності при застосуванні комплексної системної оцінки ризиків застосуємо ризик–орієнтований підхід із інструментарієм ймовірнісного аналізу безпеки. Для кожного окремого фактора ризику з тих, що аналізуються, визначимо нормований показник безпеки

$$P_n = \sum_{k=1}^{\theta_n} \lambda_n \left(1 - \prod_{j=1}^{M_{kn}} \prod_{i=1}^{N_{knj}} \left(1 - p_{knji} \right) \right), \qquad (6.20)$$

де λ_n – частота впливу даного фактору; θ_n – кількість дерев подій, для котрих визначається відповідний показник безпеки; M_{kn} – кількість послідовностей у k–му дереві подій, що призводять до руйнування системи; N_{knj} – кількість мінімальних зрізів j–ої послідовності в k–му дереві подій для n–го фактору ризику; p_{knji} – ймовірність виникнення i–го мінімального зрізу у j–й послідовності в k–му дереві подій для n–го фактора ризику.

В свою чергу, ймовірність реалізації мінімального зрізу в загальному випадку залежить як від ймовірностей відмов підсистем або елементів, так і від похибок в обслуговуванні:

$$p_{knji} = \prod_{\xi_1 \in \Xi_{1n}} p_{n\xi_1} \cdot \prod_{\xi_2 \in \Xi_{2n}} p_{n\xi_2} \cdot \prod_{\xi_\zeta \in \Xi_{\zeta n}} p_{n\xi_\zeta}, \qquad (6.21)$$

де для i–го мінімального зрізу у j–й послідовності в k–му дереві подій для n–го фактору ризику визначені: $p_{n\xi_1}$ – ймовірність відмови окремих базових подій (переважно визначається надійністю підсистем або елементів) із множини Ξ_{1n}, які в результаті оцінки відповідного дерева відмов методом мінімальних зрізів були визначені; $p_{n\xi_2}$ – ймовірність похибок в обслуговуванні при управлінні підсистемами або елементами із множини Ξ_{2n}, $p_{n\xi_\zeta}$ – ймовірність інших похибок та неопрацьованих подій, виявлених методом мінімальних зрізів.

Тоді прогнозована зміна нормованого показника безпеки за n–м фактором ризику після завершення процесу модернізації системи розраховується як

$$\Delta P_n = \frac{P_n^{(m)}}{P_n^{(b)}}, \qquad (6.22)$$

де індекси (m) та (b) відповідають показникам безпеки модернізованої та базової систем.

Використовуючи (6.18) – (6.22) та враховуючи для кожного окремого фактора ризику ваговий коефіцієнт із (6.17), визначимо оцінку глобального ризику відмови системи після модернізації так:

$$P_{ЗС} = \sum_{n=1}^{N} \beta_n \Delta P_n. \qquad (6.23)$$

6.4. Надійність оператора

Надійність оператора визначається як імовірність якісного виконання роботи або поставленого завдання протягом установленого терміну при заданих умовах.

Надійність діяльності людини у СЛТС визначається надійністю її організму: надійністю виконання людиною функцій з керування технічними засобами і їх обслуговування. Тому надійність оператора зазвичай подають у вигляді структурної і функціональної надійності. *Структурну надійність* розуміють як властивість людини зберігати працездатність протягом визначеного часу у певних умовах.

Функціональна надійність визначається як властивість людини виконувати визначені функції відповідно до завдання у той самий термін і за тих самих умов.

Таким чином, у загальному вигляді надійність оператора як імовірність безвідмовної роботи за термін t дорівнює

$$P_{оп}(t) = K_{оп}\, P_{ф}(t) P_{Ψ}(t), \qquad (6.24)$$

де $K_{оп}$ – коефіцієнт готовності оператора, що дорівнює імовірності сприймання інформації за час t; $P_ф$ – структурна надійність; $P_Ψ$ – функціональна надійність.

На безпечність функціонування СЛТС найбільше впливає функціональна надійність (далі надійність). Тому надійність оператора характеризується показниками *безпомилковості*, *готовності*, *відновлюваності*, *своєчасності*.

Як і для технічних засобів, основним показником безпомилковості роботи є імовірність безпомилкової роботи. Ця імовірність розраховується як на рівні окремої операції, так і рівні всього завдання (алгоритму) в цілому. На рівні окремої операції основними критеріями є вірогідність безпомилкового виконання операції, а для типових операцій, що найчастіше повторюються, – *інтенсивність помилок* (відмов).

Помилку оператора розуміють як неправильне виконання або невиконання оператором відповідних дій. Це може бути причиною пошкодження обладнання чи порушення нормального перебігу запланованої операції. Всі помилки оператора поділяють на *закономірні і випадкові*. До закономірних належать ті помилки, причини яких можуть бути виявлені, проаналізовані і ліквідовані. Причини випадкових помилок невідомі, вони мають стохастичний характер.

За природою виникнення розрізняють три види помилок оператора:

- *сенсорні,* пов’язані із сприйняттям інформації;
- *логічні*, пов’язані із прийняттям рішення;
- *моторні*, пов’язані з виконанням керуючих дій.

Отже, оператор є джерелом суттєвої небезпеки у СЛТС, оскільки виконує в ній основну функцію. Статистика вказує, що приблизно 20 – 30% відмов обладнання пов’язані з помилками людини. При керуванні літаком їх ціна підвищується. Так, за даними американського психолога П. Фіттса, до 70 % льотних подій відбувається з вини людини. За даними Р. Дженсена, найбільша кількість подій зі смертельним наслідком відбувалася з причини сенсомоторних помилок – 51,6 % (табл. 6. 2).

Таблиця 6.2 – Статистика помилок пілотів

Форми льотної роботи	Події зі смертельним наслідком		Події без смертельного наслідку	
	Частка,%	Абсолютна кількість	Частка, %	Абсолютна кількість
Процедури керування двигуном, автопілотом, ведення радіозв'язку тощо	4,6	264	8,6	2 230
Сенсомоторні акти (пілотування літаком, контроль швидкості, географічне орієнтування тощо)	43,8	2 496	56,3	14 561
Приймання рішень (оцінка наземних і бортових систем, оцінка небезпечних подій)	51,6	2 940	35,1	9 118
Усього випадків		5 700		25 978

Помилки оператора є імовірними подіями, але у їх підґрунті є причини як об'єктивного, так і суб'єктивного характеру. Вплив цих факторів на виникнення небезпек показаний на рис. 6.6.

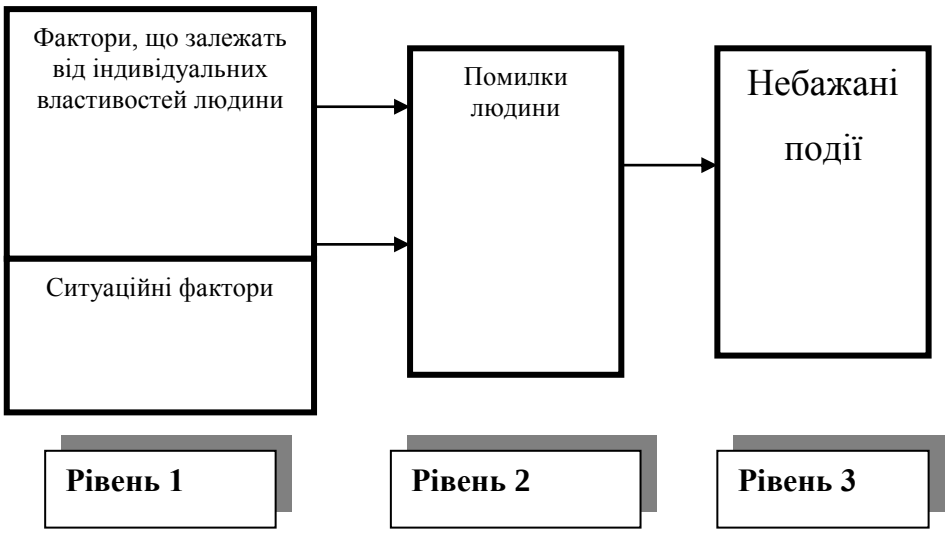

Рисунок 6.6 – Рівні виникнення небезпечних подій

Помилки, що робить оператор, можуть мати різні наслідки для людини, техніки й системи в цілому. Класифікація помилок за їх наслідками наведена на рис. 6.7.

Рисунок 6.7 – Класифікація помилок за їх наслідками

Помилки з вини оператора можуть виникати у таких випадках:

– оператор прагне досягнення помилкової мети;
– поставлена мета не може бути досягнена через неправильні дії програми;
– оператор нічого не робить або робить зайве у той момент, коли його участь необхідна.

За кількістю безпомилкових операцій W визначається ефективність оператора як ланки СЛТС

$$W = K_a\, W_0\, R'\, R'', \qquad (6.25)$$

де K_a – коефіцієнт творчої активності; W_0 – ідеальна ефективність, кількість операцій за одиницю часу; R' – імовірність працездатного стану оператора перед початком роботи; R'' – імовірність збереження працездатності оператора і безпомилкова реалізація завдання.

Основним показником безпомилковості є імовірність безпомилкової роботи. Ця імовірність може розраховуватися як на рівні окремої операції, так і на рівні алгоритму в цілому. За статистичними даними цей показник розраховується за формулою

$$P_J = N_J - n_J/N_J, \qquad (6.26)$$

де P_J – імовірність безпомилкової роботи; N_J , n_J – загальна кількість операцій J – го виду, що виконуються і кількість допущених помилок.

Для типових операцій, що повторюються досить часто, показником безпомилковості може бути *інтенсивність помилок* λ

$$\lambda_J = n_J / N_J T_J, \qquad (6.27)$$

де T_J – середній час виконання операції $_J$ – го виду.

Безпомилковість оператора $P_{оп}$ під час виконання усього завдання дорівнює

$$P_{оп} = \ell^{-\sum_{i=1}^{r} \lambda_j \tau_j k_j} \qquad (6.28)$$

де k_J – кількість виконаних операцій $_J$ – го виду; r – кількість різних операторів.

Коефіцієнт готовності $K_{оп}$ характеризує включення оператора в роботу у будь-який час

$$K_{оп} = 1 - T_0 / T, \qquad (6.29)$$

де T_0 – час відсутності оператора на робочому місці, або час неможливості сприйняття інформації; T – загальний час роботи.

Відновлюваність $P_{від}$ оцінює імовірність виправлення зробленої помилки

$$P_{від} = P_к \cdot P_п \cdot P_{випр}, \qquad (6.30)$$

де $P_{від}$ – імовірність сигналу контролю; $P_п$ – імовірність виявлення помилкових дій; $P_{випр}$ – імовірність виправлення помилкових дій.

Основним критерієм своєчасності $P_{св}$ є імовірність виконання завдання за час $t_л$

$$P_{св} = P\{\tau \le t_л\} = \int_0^{t_л} f(\tau) d\tau \qquad (6.31)$$

де $f(\tau)$ – функція щільності розподілу.

Ця імовірність може бути визначена і за статистичними даними

$$P_{св} = 1 - N_{нс} / N, \qquad (6.32)$$

де $N_{нс}$ – кількість несвоєчасного виконання завдань; N – загальна кількість виконаних завдань.

6.5. Фактори надійності оператора

Надійність оператора залежить від багатьох факторів об'єктивного і суб'єктивного характеру (рис. 6.8).

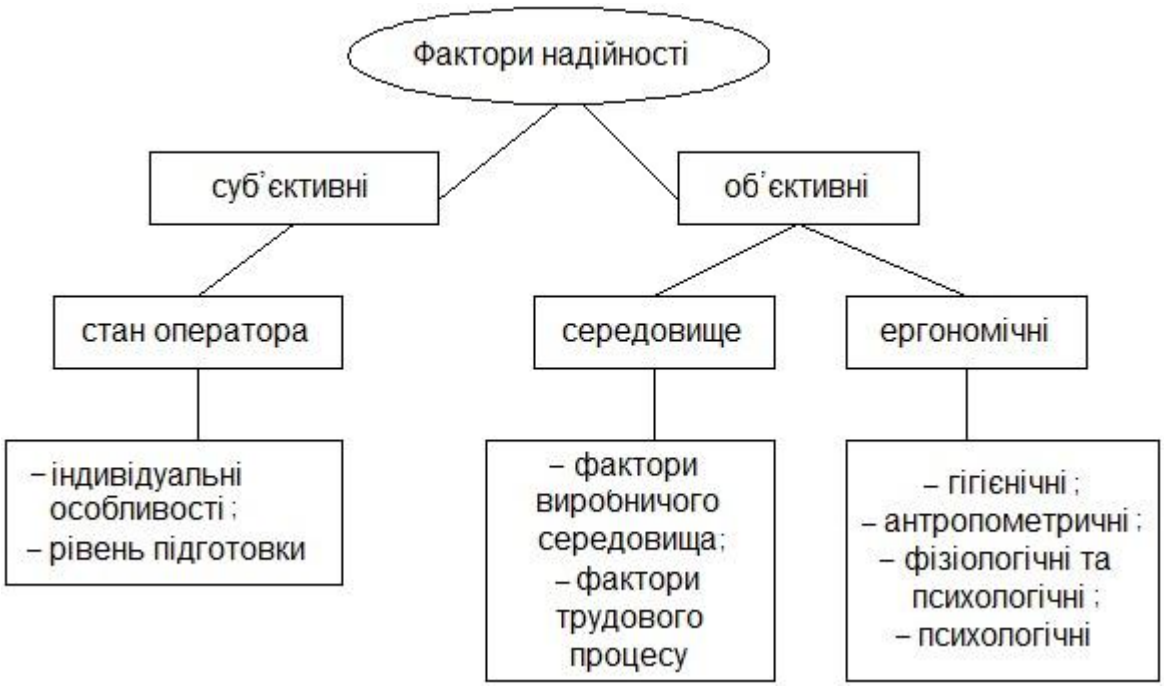

Рисунок 6.8 – Класифікація факторів, що впливають на надійність роботи оператора

Суб'єктивні фактори залежать від стану оператора, його індивідуальних властивостей, морально–психологічних якостей, медико–біологічних показників, а також рівня підготовки до цього виду діяльності. Вони мають враховуватися під час організації діяльності оператора, що забезпечить безпеку функціонування СЛТС.

Серед суб'єктивних факторів, що впливають на надійність оператора, важливе значення має функціональний стан оператора. Розрізняють – *нормальний, граничний* і *патологічний* стани. Кожний стан має свої ознаки, які

можуть бути визначені на основі медико-фізіологічних та виробничих показників.

Для оцінки функціонального стану організму використовують показники поточних змін фізіологічних функцій (сили і витривалості м'язових груп, серцево-судинної і нервової систем та ін.), що характеризують рівень працездатності і втоми під час праці, показники більш віддалених наслідків роботи. Якщо рівень більшості функцій центральної нервової системи, аналізаторів, периферійних систем і органів після роботи вищий, ніж до роботи, то функціональний стан організму нормальний.

Граничний функціональний стан проявляється у сповільненні (погіршення) деяких функцій, які входять до складу робочого акту, що призводить до неточних, зайвих рухів і зниження якості роботи.

Патологічний стан характеризується функціональною недостатністю деяких важливих підсистем організму. Позитивні сигнали людина може не сприймати, а негативні, навпаки, можуть викликати дії, що призводять до помилок, а отже, сприяють виникненню небезпечних ситуацій. Згідно з цими станами, які формуються в організмі людини під впливом трудових навантажень і умов праці, визначають ступінь важкості праці.

Індивідуальні особливості оператора визначаються загальним станом його здоров'я, станом нервової системи, психофізіологічними властивостями. Від індивідуальних особливостей людини залежить здатність людини до навчання й тренування. Вони є підґрунтям професійного відбору.

Індивідуальні особливості оператора визначають на підставі:

–безпомилковості;

–працездатності;

–витривалості й готовності до екстреної роботи;

–стійкості до перешкод;

–емоційної стійкості;

–відновлення працездатності під час відпочинку;

–багатоваріантності способів і прийомів роботи;

–гнучкості й здатності своєчасно змінювати стратегію дій;

–швидкості прийняття і виконання рішення та ін.

Суттєвим при визначенні індивідуальних особливостей оператора є властивості нервової системи: сила, динамічність, лабільність і рухомість нервових процесів.

Сила нервових процесів характеризується витривалістю нервових клітин, тобто їх здатністю витримувати тривалу і дуже сильну напругу, без переходу у позамежне гальмування. Динамічність нервової системи розуміють як швидкість умовних рефлексів, тобто здатність до навчання. Лабільність – властивість нервової системи, пов'язана із швидкістю виникнення, перебігу і припинення нервового процесу. Рухомість нервової системи характеризується швидкістю їх протікання. Вона визначає здатність до швидкої зміни одного нервового процесу іншим. Рухомість визначає швидкість обробки інформації мозком і швидкісні параметри процесу прийняття рішення оператором.

Значне місце серед психічних процесів, що впливають на якість роботи оператора, займає увага. Вона характеризується появою вибіркової готовності мозку до відповідних реакцій на певні сигнали. При цьому відбувається підвищення чутливості аналізаторів та зменшення латентного періоду до очікуваних сигналів, підвищення готовності виконавчого апарату для цих сигналів. Від уваги залежить рівень налаштованості людини до сприймання і переробки інформації. Надійність оператора залежить від фактора розподілу і переведення уваги.

Об'єктивні фактори поділяють на дві групи: *ергономічні та середовища*. До факторів середовища належать фактори умов праці й фактори трудового процесу.

6.6. Фактори середовища

До факторів середовища належать фактори умов праці і фактори трудового процесу. Умови праці – це сукупність факторів виробничого

середовища, що впливають на здоров’я і працездатність людини. Виробниче середовище – це середовище, де людина здійснює свою трудову діяльність.

Фактори виробничого середовища включають певну сукупність санітарно–гігієнічних, психологічних та естетичних елементів виробничого середовища, які діють на людину на її робочому місці. Вони суттєво впливають на функціональний стан і працездатність операторів (рис. 6.9).

У нормативному документі «Гігієнічна класифікація умов праці за показниками шкідливості і небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу» до фізичних факторів виробничого середовища належать :

– вібрація (загальна і локальна);

– шум;

– інфразвук;

– ультразвук;

– неіонізуючі випромінювання (радіочастотного діапазону, діапазону промислової частоти, оптичного діапазону (лазерне випромінювання);

– мікроклімат у приміщенні (температура повітря, швидкість руху повітря, відносна вологість повітря, інфрачервоне випромінювання);

– температура зовнішнього повітря (при роботі на відкритому повітрі) узимку й улітку;

– атмосферний тиск (підвищений і понижений);

до хімічних факторів належать:

– шкідливі хімічні речовини 1– 4 класів небезпеки;

– пил переважно фіброгенної дії;

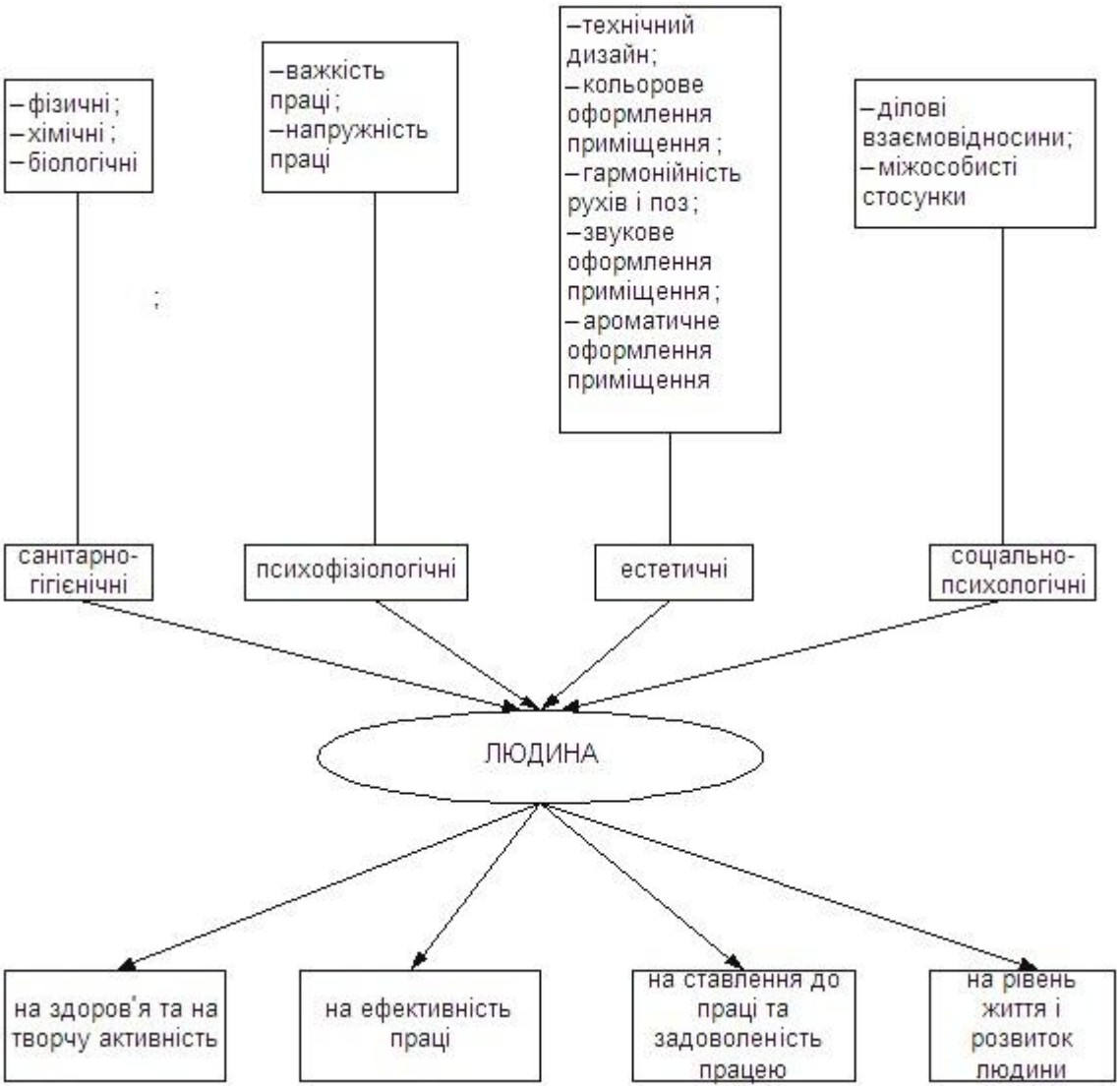

Рисунок 6.9 – Фактори виробничого середовища і їх вплив на оператора

до біологічних факторів належать:

– мікроорганізми 1–4 класу небезпеки;

– білкові препарати 1–4 класу небезпеки;

– природні компоненти організму (амінокислоти, вітаміни тощо) 1–4 класу небезпеки.

Регламентують умови праці санітарні норми. Виділяють таку класифікацію санітарних норм:

– за призначенням (проектування промислових підприємств, санітарний стан підприємств, техніки безпеки та виробничої санітарії, норми для окремих видів виробничих шкідливостей тощо);

– за обов’язковістю застосування (обов’язкові та рекомендовані);

– залежно від впливу умов праці на організм людини (оптимальні та допустимі);

– залежно від сфери застосування (загальні та галузеві);

– залежно від терміну дії (постійні та тимчасові).

При визначенні характеру впливу на людину факторів умов праці виходять із таких установлених гігієнічних нормативів :

– гранично допустимі рівні виробничого фактора (ГДР) – рівень виробничого фактора, дія якого при роботі встановленої тривалості за час всього трудового стажу працівника не призводить до травм, захворювання чи відхилення у стані здоров’я в процесі роботи, або у віддалені періоди життя теперішнього і наступного поколінь. Цей норматив застосовується для оцінки дії на людину фізичних факторів);

– гранично допустима концентрація (ГДК) – концентрація, яка при щоденній (крім вихідних днів) роботі протягом 8 годин або іншої тривалості, але не більше 41 год. за тиждень, за час усього стажу роботи не може викликати захворювань або відхилень у стані здоров’я.

Цей норматив застосовується для оцінки дії на людину переважно хімічних факторів середовища.

Значення гігієнічних нормативів регламентовані нормативно–технічними документами і стандартами з безпеки праці. Для додержання цих нормативів застосовують заходи і засоби захисту працюючих.

Вивченням факторів виробничого середовища, організаційно–технічних і санітарно–гігієнічних умов, у яких відбувається трудова діяльність людини, а також системи правових заходів з виконання правил безпеки та виробничої санітарії є предметом навчальних дисциплін «Основи охорони праці» та «Охорона праці в галузі».

На діяльність операторів СЛТС найбільше впливають: мікроклімат, шум та рівень освітленості виробничих поверхонь.

Вплив цих факторів на працездатність оператора відбиває функція відкликання, що має вигляд

$$Z(x,t) = a_0 + a_1 t + a_2 t^2 + \sum_{i=1}^{m} (в_1 + в_i t) x_i + \sum_{i=1}^{m} в_i x_i x_J + \sum_{i=1}^{m} c_1 x_1^2, \qquad (6.33)$$

де $a_0, a_1, a_2, в_i, c_i$ – постійні коефіцієнти функціонального ряду при перемінних t, x_i, x_J, що відображають поточний час роботи, температуру зовнішнього середовища, освітленість робочого місця і виробничий шум.

Психофізіологічні фактори визначають особливості трудового процесу у СЛТС. Вони представлені такими показниками, як важкість і напруженість праці. Важкість праці є кількісною характеристикою фізичної праці. Напруженість – кількісна характеристика розумової праці.

Важкість праці розуміють як ступінь навантаження на м'язову систему та фізіологічні витрати внаслідок цього навантаження. Напруженість праці характеризує навантаження на організм, що виникають унаслідок інтенсивної роботи мозку при отриманні і переробці інформації.

Важкість праці оцінюється за показником статичного і динамічного навантажень. Статичне навантаження визначають як добуток зусилля і часу його підтримання при виконанні конкретної роботи. Потім усі величини за окремі відрізки часу підсумовують і отримують статичне навантаження за весь термін роботи. Обсяг динамічного навантаження за кожний окремий відрізок часу вираховують за формулою

$$W = [PH + (PL/9) + (PH_1/2)]\, K, \qquad (6.34)$$

де W – робота (кгс · м); P – маса вантажу (кгс); H – висота, на яку піднімається вантаж з вихідного положення; L – відстань, на яку переміщується вантаж (м); H_1 – відстань, на яку опускається вантаж (м); K – коефіцієнт, що дорівнює 6.

Потім підсумовують показники динамічної роботи за всі відрізки робочого часу. При розумовій праці основною є аналітико-синтетична функція

центральної нервової системи, значущими факторами – кількість одночасно перероблюваної інформації, її новизна, складність переробки і необхідність запам'ятовування, емоційне напруження.

Напруженість праці оцінюється за показниками, що характеризують інтелектуальні властивості: *сенсорні, емоційні навантаження, монотонність* та *режим праці*.

Для операторів СЛТС ключовою є функція аналізаторів, а значущими елементами напруженості праці – сила сигналів, ступінь їх розпізнавання і щільність, складність інформації, емоційне напруження та ін. Ці фактори суттєво впливають на надійність оператора СЛТС. Перевантаження інформацією може призвести до її пропусків, помилок в обробці, затримки відповіді тощо. Підвищенню надійності сприяє самоконтроль, який дозволяє своєчасно попередити або знайти помилки, допущені під час роботи.

За рівнем напруження розрізняють:

– помірне, або нормальний робочий стан, який виникає під впливом праці. Воно супроводжується помірними зрушеннями фізіологічних функцій та виявляється в доброму самопочутті, стабільному виконанні роботи;

– підвищене, що виникає в екстремальних умовах роботи і виявляється в зміні показників роботи вегетативних органів, опорно–рухового апарату, біохімічних реакцій. Під час такого стану порушуються силові рефлекси на подразники. Це може бути причиною виникнення небезпеки у СЛТС.

Емоційне напруження оператора після виконання особливо відповідальної роботи супроводжується психічним виснаженням (функціональною астенією). Відзначається слабкість процесів збудження (недостатня рухливість, пасивність, сповільнене мислення, або гальмування, (помірно виражена рухова метушливість, неглибокий аналіз і оцінка подій). Такий стан може тривати протягом 1–3 години (рідше добу), після чого з'являються головний біль, стомленість, апатія, неглибокий сон. Відмічається погіршення пам'яті, сприймання. Тривалі і сильні емоційні напруження оператора негативно впливають на його діяльність, а отже, є небезпечними для

нього, оскільки призводять до нервово–емоційних зривів і погіршення стану здоров'я.

Основними напрямами забезпечення безпеки діяльності оператора, відповідно й усієї СЛТС, є зменшення емоційного напруження і підвищення надійності його роботи, врахування та погодження конструкційних рішень технічної ланки системи із можливостями людини під час проектування та експлуатації цих систем.

Психофізіологічне вивчення діяльності оператора дозволило виділити *мінімальний, оптимальний та екстремальний* режими роботи, у яких надійність оператора суттєво відрізняється.

Мінімальний режим роботи характеризується недовантаженістю інформацією, монотонність призводить до втрати пильності, гіпнотичних станів оператора. Це може бути причиною несвоєчасних дій на аварійні сигнали, виникнення аварій, катастроф.

Оптимальний режим роботи характеризується комфортними умовами. Робота виконується без значних нервово–психічних навантажень.

Екстремальний режим роботи визначається різко підвищеними вимогами до інтелектуальних та емоціональних властивостей людини.

Оцінка праці за факторами трудового процесу проводиться згідно з гігієнічною класифікацією. Найважливіші фактори трудового процесу наведено в табл. 6.3.

За нормативним документом «Гігієнічна класифікація умов праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу» умови праці поділяються на 4 класи: I клас – оптимальні умови праці, II клас – допустимі умови праці, III клас – шкідливі умови праці, IV клас – небезпечні (екстремальні) умови праці.

Таблиця 6.3. Фактори трудового процесу

Фактор	Трудовий процес	Фактор	Трудовий процес
I. Важкість праці	1) динамічна робота (потужність зовнішньої роботи; маса вантажу, що піднімається і переміщується; дрібні стереотипні рухи кистей і пальців рук); 2) статичне навантаження (величина навантаження за зміну при утриманні вантажу руками; за участю м'язів тулуба	II. Напруженість праці	1) увага (тривалість зосередження, щільність сигналів у середньому за годину); 2) напруженість аналізаторних функцій (зору, слуху); 3) емоційна та інтелектуальна напруженість; 4) одноманітність (кількість елементів у багаторазово повторюваних операціях; тривалість виконання повторюваних операцій; час спостереження за перебігом виробничого процесу без активних дій).

До соціально-психологічних факторів виробничого середовища відносять:

– ділові взаємовідносини;

– міжособистісні стосунки.

Ділові взаємовідносини визначаються змістом завдання, що вирішується, штатним розписом, службовими інструкціями тощо. За своїм характером вони можуть бути як безпосередні (міжособистісне спілкування), так і опосередковані за допомогою інших людей або технічних засобів.

Міжособистісні стосунки виникають на основі суб'єктивних відносин між працівниками і будуються на принципах моральних групових норм поведінки, суб'єктивних установок і стереотипів, почуттів симпатії або антипатії, довіри або недовіри, притягування або відштовхування, вдячності або негативізму.

Ефективність діяльності виробничого колективу може бути описана як функція з чотирьох компонентів:

$$E = K_1(K_2E_{пс} + K_3E_к + K_4E_{пр} + K_5E_{ос}); \qquad (6.35)$$

де $E_{пс}$ – психосоціальна ефективність; $E_к$ – ефективність комунікацій; $E_{пр}$ – професійна ефективність; $E_{ос}$ – складова ефективності за рахунок сприяння психологічного клімату; K_1, K_2, K_3, K_4, K_5 – відповідно константи повної ефективності, психосоціальної ефективності, ефективності комунікацій, професійної ефективності і сприятливості психологічного клімату.

Ефективність роботи оператора повною мірою залежить від психологічного клімату, що створюється на виробництві. Складові ефективності за рахунок психологічного клімату ($E_{ос}$) визначаються при невеликій напруженості ($0 \le S \le 10$) за рівнянням:

$$E_{ос} = 0{,}5833\ (C_1 + C_2)/2; \qquad (6.36)$$

де C_1 і C_2 показники спрацьованості групи.

Психологічний клімат визначається через задоволеність міжособистісними відносинами по вертикалі (керівник – підлеглі) й

горизонталі (виконавці), а також через задоволеність змістом діяльності, що полягає у сумісності й спрацьованості.

Сумісність – це ефект взаємодії людей, який означає максимальне суб'єктивне задоволення партнерів один одним. Суб'єктивна задоволеність, задоволеність спілкуванням – основні ознаки сумісності.

Спрацьованість – це результат взаємодії конкретних учасників діяльності. Вона характеризується продуктивністю, емоційно–енергетичними витратами та задоволеністю собою, партнерами, змістом роботи.

Взаємовідносини та взаємодія колективу у процесі діяльності значною мірою залежить від узгодженості думок членів групи відносно напряму пошуку можливих рішень і оцінки наслідків їх прийняття у будь–яких ситуаціях, психічної привабливості один для одного.

6.7. Ергономічні фактори

Ергономічні фактори надійності оператора включають гігієнічні, антропометричні, фізіологічні, психофізіологічні, психологічні фактори.

Гігієнічні фактори визначають умови життєдіяльності і працездатності людини в процесі взаємодії з технікою і середовищем. Показниками є рівень освітлення, температура, вологість, шум, вібрація, токсичність, загазованість тощо.

Антропометричні фактори визначають відповідність конструкцій техніки антропометричним характеристикам людини (зріст, розміри тіла і окремі рухові ланки). Показниками є раціональна робоча поза, оптимальні зони досягнення, раціональні трудові рухи).

Фізіологічні та психофізіологічні фактори визначають відповідність техніки і середовища функціональним можливостям працівника (силовим, швидкісним, енергетичним, зоровим, слуховим). Показниками є темп робочих рухів, обсяг інформації, навантаження на м'язову та нервову системи.

Психологічні фактори визначають відповідність техніки і середовища можливостям працівника щодо сприймання, переробки інформації, прийняття і реалізації рішень.

Дослідження впливу цих факторів на СЛТС із метою створення для працівника досконалих знарядь і оптимальних умов праці є об'єктом науки *ергономіки*. На підставі цих досліджень відбувається проектування, яке передбачає аналіз характеристик об'єкта керування, розподіл функцій між людиною та машиною, узгодженості діяльності оператора і технічних засобів, оцінку системи в цілому.

Необхідність врахування людського фактора при проектуванні СЛТС потребує погодження предметного середовища з можливостями людини. Погодження характеристик людини і предметного середовища здійснюється в просторовому, часовому, інформаційному, енергетичному напрямах.

Просторове погодження передбачає організацію робочого місця працівника, робочу позу, визначення зон досягання, траєкторії рухів, доступність органів керування тощо.

Часове погодження враховує динаміку працездатності з виконанням роботи, її темпу, інтенсивності, зміною діяльності і відпочинком.

Інформаційне погодження пов'язане з оцінкою потоків інформації та пропускною здатністю аналізаторних функцій щодо сприйняття і переробки інформації, врахуванням перешкод.

Енергетичне погодження враховує вплив трудових навантажень на м'язову, серцево–судинну системи на основі встановлення оптимального обсягу рухової діяльності, величини м'язових зусиль залежно від умов праці.

Організація робочого місця передбачає вирішення таких основних завдань:

– правильне розміщення робочого місця у виробничому приміщенні;
– вибір раціональної робочої пози;
– раціональне розміщення індикаторів і органів керування згідно з їх важливістю і частотою користування в межах поля зору і зон досягання;
– забезпечення оптимального огляду робочого місця;

– відповідність конструкції технічних пристроїв і робочих меблів антропометричним, фізіологічним і психологічним характеристикам людини;

– організація пересування людини;

– відповідність інформаційних потоків можливостям людини щодо сприймання і переробки інформації;

– забезпечення сприятливих санітарно–гігієнічних умов праці.

Діяльність людини у СЛТС пов’язана із сприйняттям від засобів відображення інформації різних сигналів. Вони є технічною основою для побудови інформаційної моделі оператора і тому суттєво впливають на безпеку функціонування системи.

Основними ергономічними вимогами до інформаційної моделі СЛТС є:

1) обсяг, структура й форма подання інформації повинні відповідати розв’язуваним завданням, що вирішуються, і психофізіологічним можливостям оператора, адекватно відображати об’єкт керування і навколишнє середовище;

2) за кількістю інформації бути лаконічною, запобігати як недовантаженню, так і перевантаженню оператора;

3) форма подання інформації не повинна вимагати від оператора її додаткового перекодування.

4) інформація має відображатися з таким ступенем точності, який потрібний для вирішення оператором покладених на нього завдань;

5) розміщення інформаційної моделі має відповідати найімовірнішій послідовності їх обслуговування оператором;

6) інформаційна модель має давати змогу оператору прогнозувати характер розвитку ситуацій;

7) характеристики сигналів, що подаються оператору, мають забезпечувати необхідний рівень їх диференційного сприймання;

8) для більшої рівномірності завантаження аналізаторів оператора основна інформація має оптимально поділятися між ними.

Виходячи з цих вимог, основні принципи компонування засобів відображення інформації такі:

•*лаконічність* – засіб відображення інформації має містити лише ті елементи, які необхідні для забезпечення оператора інформацією про стан об’єкта керування і засоби впливу на нього;

•*важливість* – най важливіші інформаційні пристрої і органи керування розміщуються в найбільш зручних для керування місцях;

•*черговість* – інформаційні пристрої та органи керування розміщуються в тій послідовності, в якій вони використовуються;

•*частота використання* – інформаційні пристрої та органи керування розміщуються у центральному полі зору;

•*функціональний взаємозв’язок* – інформаційні прилади або органи керування, пов’язані однією функцією, повинні бути згруповані разом.

Ергономічні вимоги до конструкцій робочих місць стосуються:

- конструктивного виконання робочих місць та елементів їх розміщення елементів на робочому столі;
- ергономічної організації пульта управління.

Конструкція робочого місця має забезпечувати оператору можливість швидко зайняти його, змінити положення тулуба і кінцівок, прийняти зручну позу для відпочинку та ін.

Вибір органів керування визначається властивостями параметрів об’єкта або системи керування, й залежить від типу впливу оператора на систему. Незалежно від типу органів керування вони мають бути логічно згруповані, їхнє просторове розміщення має відповідати розміщенню пов’язаних із ними груп індикаторів. Спрямованість рухів органів керування має враховувати сформовані сенсорно-моторні навички людини.

Запитання для самоконтролю

1. З чого складається системний аналіз, що використовується для оцінки системи «людина – техніка – середовище» (СЛТС)?

2. Які три види подій розрізняють при побудові дерев у графоаналітичних

методах аналізу?

3. Від яких складових залежить надійність виробництва?

4. Що розуміють як надійність системи?

5. Як визначається імовірність безвідмовної роботи засобу та людини?

6. Що характеризує інтенсивність відмов технічних засобів?

7. Наведіть загальний закон надійності технічного засобу.

8. У чому полягає підхід визначення надійності за наслідками?

9. Як надійність системи після модернізації впливає на безпеку?

10. Як визначається надійність оператора у системі СЛТС?

11. Що означає функціональна надійність оператора?

12. Які показники характеризують функціональну надійність оператора?

13. Які види помилок характеризують роботу оператора?

14. На які види помилок за природою походження поділяються помилки оператора?

15. В яких випадках частіше за все виникають помилки оператора?

16. Які фактори характеризують надійність оператора?

17. Яке місце серед психічних процесів на роботу оператора займає увага?

18. Що таке виробниче середовище та з яких факторів воно складається?

19. За якими показниками оцінюють важкість праці?

20. З яких факторів складаються ергономічні показники?

21. Що визначають антропометричні фактори праці?

22. Які завдання необхідно вирішувати при організації робочого місця?

23. Із чого складається інформаційна модель СЛТС?

Тема 7. АНАЛІЗ АВАРІЙНОГО РИЗИКУ. ПЛАН ЛІКВІДАЦІЇ АВАРІЙНИХ СИТУАЦІЙ.

7.1. Види техногенних небезпек.

7.2. Етапи аналізу аварійного ризику.

7.3. Попередній аналіз небезпек (ПАН).

7.4. План ліквідації аварійних ситуацій (ПЛАС).

7.1. Види техногенних небезпек

Загальновідомо, що науково–технічний прогрес надає не тільки блага, але і все наростаючі загрози для життя і здоров'я людей, для всього навколишнього середовища. Техногенні аварії, що відбулися наприкінці 20–го століття, чітко показали, що існуюча раніш «концепція техніки безпеки» в промисловій сфері, яка спиралась на принцип «реагувати і виправляти», повністю себе викорінила. На зміну їй у вісімдесяті роки минулого століття була висунута нова «концепція прийнятного техногенного ризику», в основі якої був покладений принцип «передбачати і упереджувати»[27,28,]. Стало ясно, що забезпечити абсолютну безпеку об'єктів техносфери неможливо. Необхідно досягати їх відносної безпеки, доводячи аварійний ризик, пов'язаний із ними, до прийнятного, допустимого ризику.

До основних видів техногенних небезпек належать: хімічна, радіаційна та бактеріологічна небезпеки. Хімічна небезпека проявляється в аварійному або систематичному токсичному ураженні людей та забрудненні навколишнього природного середовища (НПВ), у пожежах і вибухах.

26.«Анализ риска – основа для решения проблем безопасности населения и окружающей среды» [Електроний ресурс]. Режим доступу: http://www.admhmao.ru/committe/upr_prst/Sayt/ht01.htm.

27. Легасов В.А. Из сегодня – в завтра. Мысли вслух. /В.А.Легасов. - М. – 1996, – 226 с.

Небезпеку, що призводить до ураження людей і забруднення навколишнього природного середовища токсичними речовинами, правомірніше було б називати токсичною небезпекою, виділяючи її з інших видів хімічної небезпеки.

Хімічно небезпечним об'єктом (ХНО) прийнято називати об'єкт техносфери, при аварії на якому або руйнуванні якого може відбутися масове отруєння людей, сільськогосподарських тварин і рослин або хімічне зараження навколишнього природного середовища хімічними речовинами в кількостях, що перевищують природний рівень їх вмісту в середовищі.

Серед ХНО виділяють хіміко–технологічні об'єкти (ХТО), в яких відбувається переробка хімічної субстанції. Типовий ХТО зазвичай розчленовують на складові частини (ділянки) різного призначення: основні технологічні ділянки, допоміжні ділянки та функціональні частки загального призначення.

Життєдіяльність, тобто життєвий цикл практично будь-якого промислового об'єкта, включаючи і ХТО, може бути поділений на ряд етапів: передпроектне опрацювання, розробку технічного проекту, розробку робочого проекту, будівництво, здавання об'єктів в експлуатацію (пусконалагоджувальні роботи), планову експлуатацію. Після припинення експлуатації – розбирання обладнання, демонтаж, утилізація. Етап експлуатації здатний викликати найбільші небезпеки.

Система забезпечення безпеки ХТО повинна бути комплексною і містити в своєму складі підсистеми:

– науково–технічного,

– інформаційного,

– матеріально–технічного,

– кадрового,

– організаційного забезпечення.

Розглянемо систему науково-технічного забезпечення безпеки хіміко-технологічного об'єкта (СБ ХТО) на рис. 7.1.

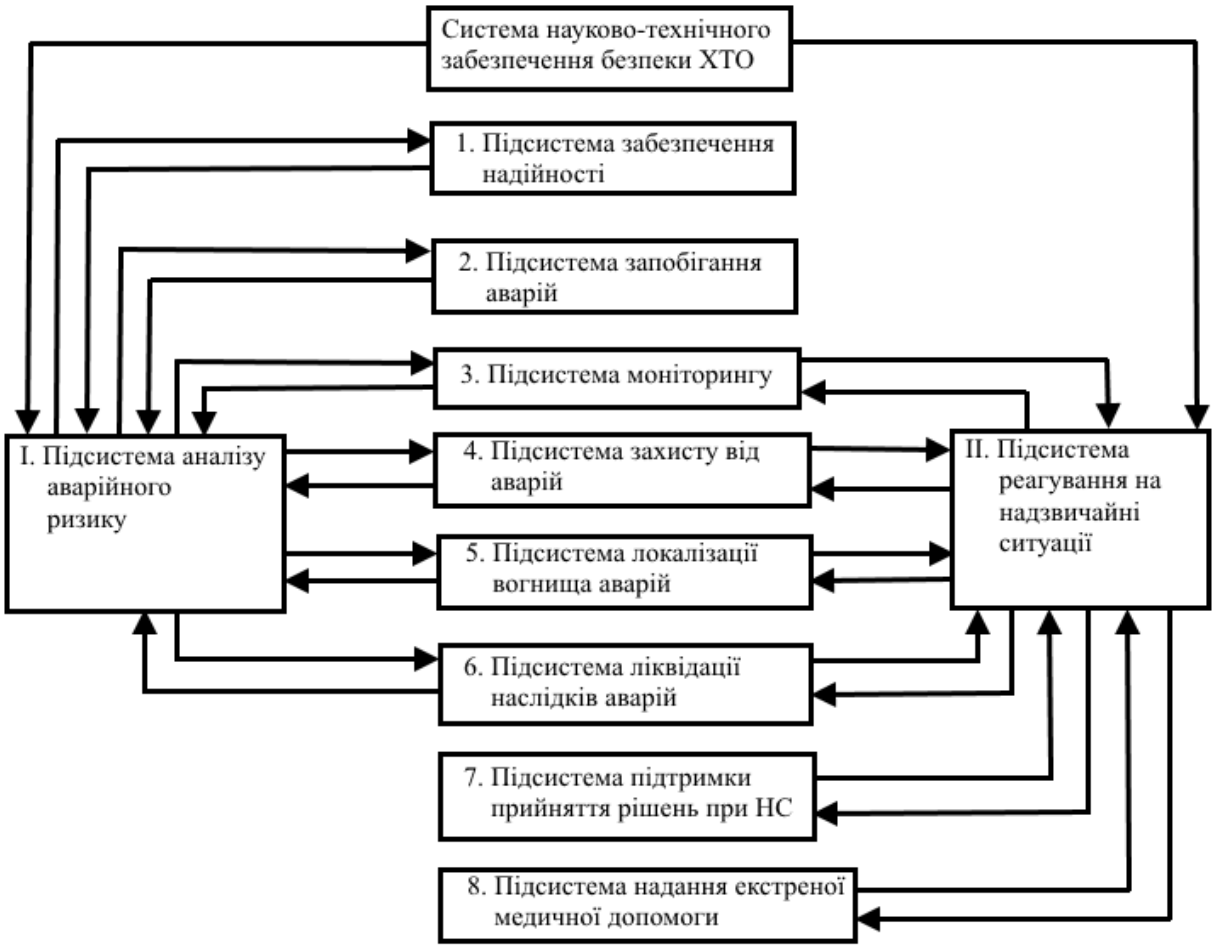

Рисунок 7.1. – Блок-схема системи науково–технічного забезпечення безпеки ХТО

При цьому мова буде йти про заходи та дії, спрямовані на прогнозування аварійного ризику і дій в умовах НС. Науково–технічні аспекти, пов’язані з систематичним ризиком, що спричинений ХТО при «нормальних» безаварійних умовах експлуатації, тут не розглядаються. Система безпеки ХТО може бути подана у вигляді 10-ти взаємопов’язаних підсистем[28], які зображені на рис. 7.1. Таке розбиття певною мірою є умовним; окремі функції підсистем можуть перекриватися.

28. Горский В.Г. и др. Научно–методические аспекты анализа аварийного риска./ В.Г. Горский и др. – М.: Экономика и информатика, 2001. – 320 с.

Як особливі виділено 2 підсистеми: аналізу аварійного ризику і реагування на надзвичайні ситуації. З позиції сучасної концепції забезпечення безпеки перша підсистема I* виконує функцію координатора підсистем 1–6. Підсистема II* реагування на надзвичайні ситуації (НС) координує та керує підсистемами 3–8. Призначення підсистем 1–8 випливає з їхніх назв.

Підсистема I* аналізу аварійного ризику призначена концентрувати інформацію про об'єкт в цілому, про систему його безпеки і про навколишнє оточення й прогнозувати можливі аварії та їхні наслідки. Але основна її активна функція – розробка рекомендацій з коригуючих дій на об'єкту в цілому, на інші підсистеми СБ ХТО для того, щоб забезпечити зниження величини ризику, і підтримати його на прийнятному рівні. На рис.7.1 зв'язок підсистеми аналізу аварійного ризику з рештою підсистем СБ ХТО (1–6) відбитий подвійними стрілками, щоб підкреслити їх взаємодію.

Підсистема II* реагування на надзвичайні ситуації, що виникають на об'єкті при аваріях, є координатором зазначених вище підсистем 3–6, а також підсистем 7, 8. Подвійними стрілками відображена взаємодія між підсистемами II* і 3–8.

Наведене розбиття СБ ХТО на підсистеми є суб'єктивним. Одні й ті самі технічні засоби, методи і заходи можуть використовуватися в різних підсистемах. Це належить, наприклад, до засобів оповіщення. Наведені підсистеми повинні підключатися до роботи як послідовно, так і паралельно.

Підсистеми 1,2 націлені, переважно, на забезпечення безаварійної роботи хімічного об'єкта або, якщо іти за термінологією, прийнятою в сфері цивільної оборони, можна сказати, що ці підсистеми призначені для запобігання надзвичайних ситуацій.

Підсистеми 3–8 мають на меті забезпечити безпеку людей або необхідні дії в надзвичайних ситуаціях на об'єкті. Реалізація заходів, передбачених підсистемами 3–8, проводиться відповідно до плану заходів і дій у НС.

7.2. Етапи аналізу аварійного ризику

Відповідно до сучасних уявлень важливою частиною системи науково–технічного забезпечення безпеки ХТО є підсистема аналізу аварійного ризику. Аналіз аварійного ризику – це складна комплексна процедура, що включає цілий ряд етапів. Залежно від того, про який період життєвого циклу об’єкта йде мова, ступінь глибини і деталізації аварійного ризику буде різний.

Найбільш повна блок–схема аналізу аварійного ризику, що включає всі основні процедури аналізу ризику, наведена на рис. 7.2.

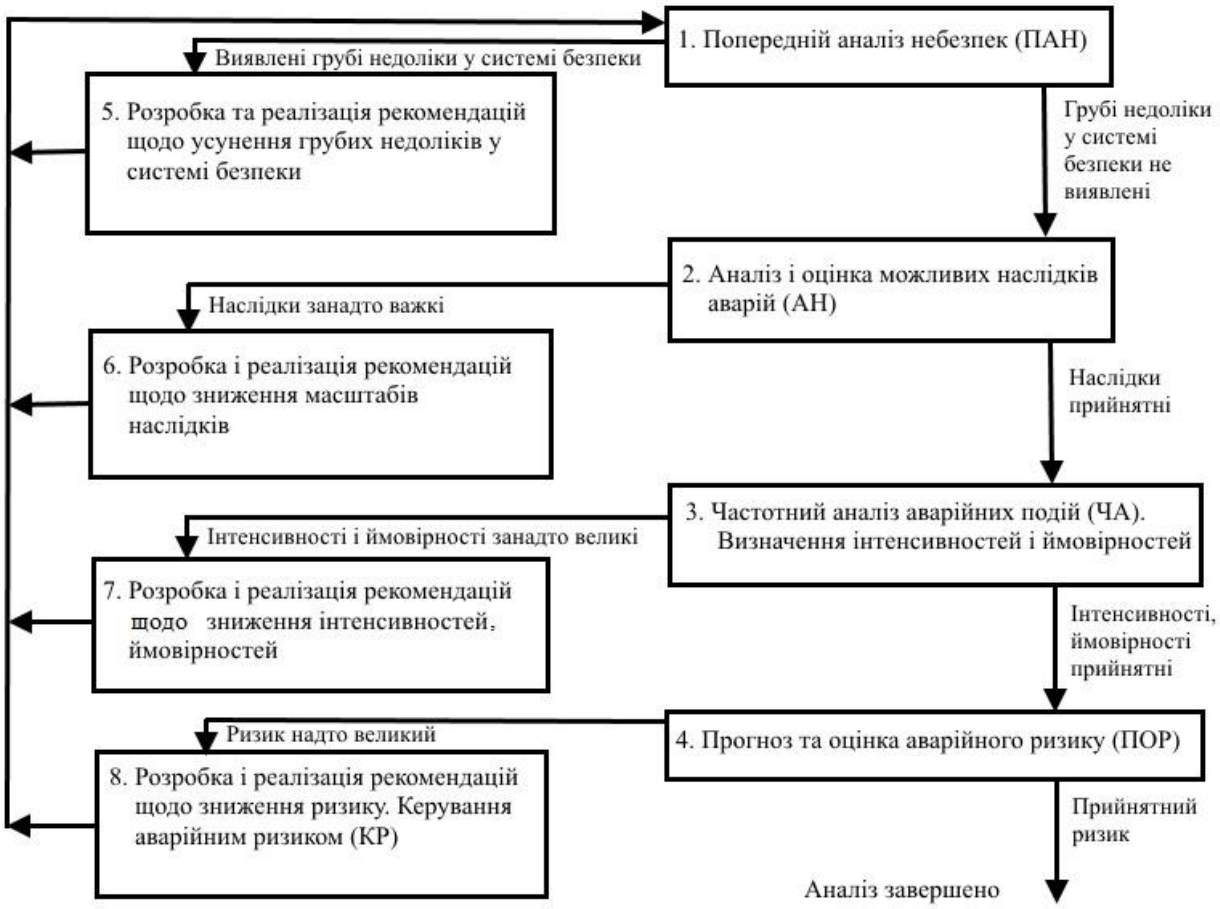

Рисунок 7.2 – Блок-схема аналізу аварійного ризику

Подібна процедура застосовується найчастіше на етапі експлуатації об’єкта.

До початку проведення аналізу мають бути визначені:

1) об’єкт дослідження;

2) мета;

3) ступінь глибини аналізу;

4) вид прогнозованого аварійного ризику;

5) обмеження на аналіз.

Вся процедура аналізу аварійного ризику може бути поділена на ряд порівняно самостійних, але взаємопов'язаних етапів. Перший етап (блок 1) призначений для виявлення основних небезпек, прихованих у цьому об'єкті. На другому етапі (блок 2) проводиться аналіз і кількісна оцінка можливих наслідків від прогнозованих аварій. Третій етап (блок 3) є частиною аналізу аварійних подій; він полягає у визначенні інтенсивності (частот) і ймовірностей аварійних подій. На четвертому етапі (блок 4) дані про збитки що очікуємо і втрати від окремих аварій комбінуються з даними щодо можливих інтенсивностей і ймовірностями аварійних подій, та знаходиться величина прогнозованого аварійного ризику.

Після кожного з перерахованих вище етапів проводиться аналіз отриманих даних. Якщо на етапі ПАН виявлено грубі недоліки системи безпеки, на етапі АН – занадто важкі наслідки можливих аварій, на етапі ЧА – занадто великі значення прогнозованих інтенсівностей і ймовірностей та на етапі ПОР – занадто велике значення прогнозованого ризику, то розраховуються і реалізуються необхідні корегувальні впливи на об'єкт, щоб знизити рівень його небезпеки (блоки 5–8). Таким чином, керування аварійним ризиком має перманентний характер. Після здійснення зазначених впливів знову реалізуються блоки 1–4 і так доки не буде досягнуте прийнятне значення прогнозованого ризику.

7.3. Попередній аналіз небезпек (ПАН)

Основне призначення аналізу полягає в такому: виявити, з яких причин можуть виникати аварії, ідентифікувати носії аварійної небезпеки; визначити, за якими сценаріями можуть розвиватися аварії; відібрати з них найбільш

небезпечні. Попередній аналіз небезпек складається з ряду етапів, поданих на рис. 7.3.

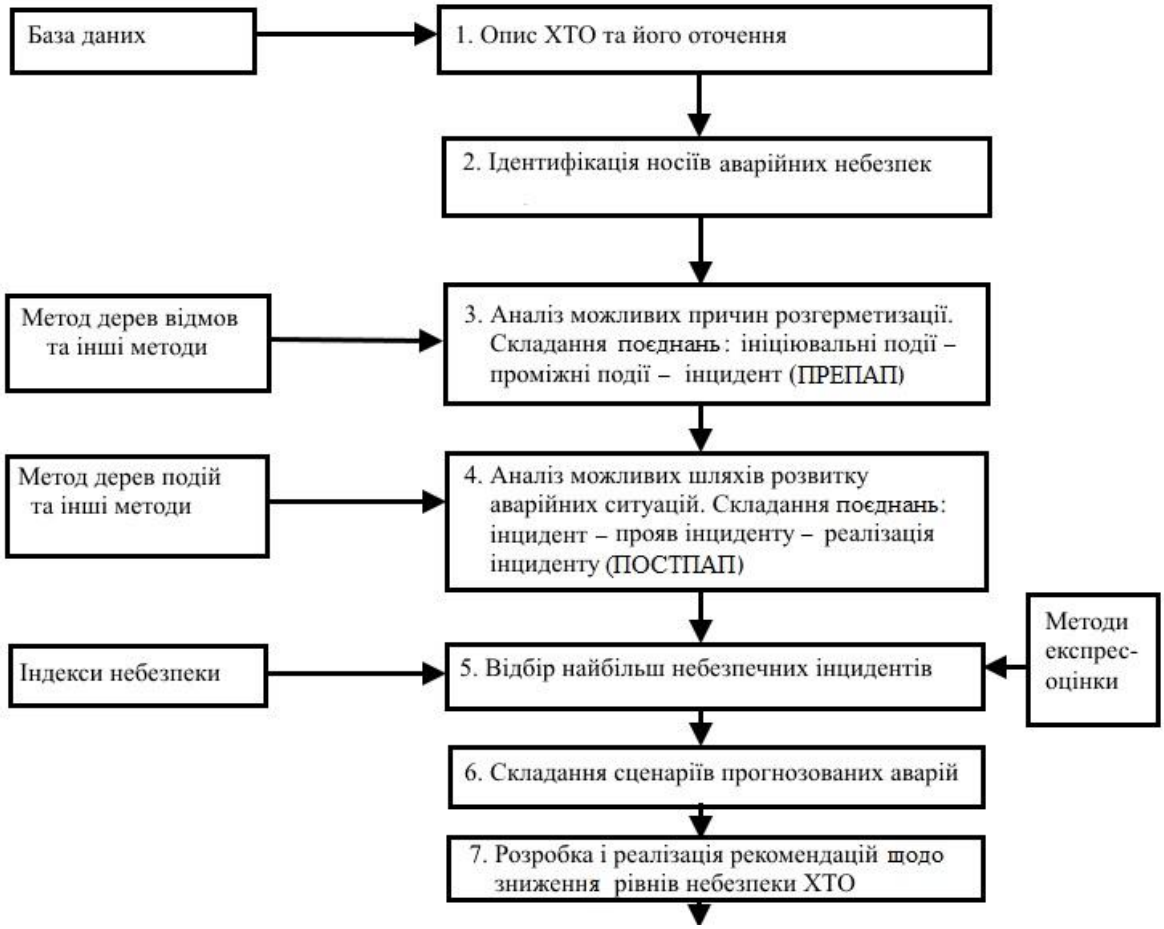

Рисунок 7.3 – Блок-схема попереднього аналізу небезпек.

Перший етап ПАТ (блок 1) полягає в описі ХТО і його оточення. Безглуздо братися за аналіз небезпек, прихованих в об’єкті, не знаючи досконально сам об’єкт. Дослідник повинен ретельно ознайомитися з усіма сторонами життєдіяльності ХТО. Разом з тим рівень небезпечності ХТО залежить і від його оточення, яке теж має бути розглянуто. На цьому етапі повинна бути зібрана і вивчена така інформація: структура об’єкта; просторове розміщення його елементів; основні операції, що виконуються на об’єкті; технологічна схема; обладнання, що використовується; речовини і матеріали, що застосовуються на об’єкті; відмови устаткування, що мали місце; надійність

використовуваного обладнання; можливі помилкові дії персоналу; природні явища катастрофічного характеру, можливі у певній місцевості; розміщення населення в районі розташування об’єкта; місцеві метеорологічні, географічні та топографічні характеристики. Блок 2 ПАТ містить опис таксономії носіїв небезпеки та їх класифікацію. На цьому етапі важливо виділити носії, що відзначаються найбільшим токсичним та/або енергетичним потенціалом. Третій блок ПАТ (блок 3) призначений для виявлення можливих інцидентів. Аналіз полягає у побудові преінцидентних поєднаннь аварійних подій (ПРЕПАП): ініціюють умови – проміжні події – інцидент, (несанкціоноване вивільнення токсичного та/або енергетичного потенціалу), які сстановлять фази ініціювання аварій. Відстежуються різні, можливі ініціюючі події, такі, як відмови устаткування, відхилення від технологічних режимів, помилки персоналу та надзвичайні зовнішні події. На цьому етапі найчастіше використовують метод дерев відмов (ДВ) у припущенні, що верхня небажана подія є інцидентом. Блок 4 присвячений аналізу постінцідентних поєднань аварійних подій, процесів і явищ (ПОСТПАП), які можуть відбуватися після інциденту, тобто розгерметизації, порушень ізоляції обладнання та інших явищ, що супроводжуються вивільненням токсичного та/або енергетичного потенціалу. Ці події, процеси і явища становлять фазу розвитку аварії. Тут розглядаються різні види витоків небезпечних речовин у навколишній простір. Детально розбираються можливі наслідки токсичних аварій, пожеж і вибухів. На цьому етапі може бути з успіхом використано метод дерева подій (ДП), за умови, що вихідною випадковою подією є інцидент. Блок 5 включає відбір найбільш небезпечних інцидентів і формування остаточного списку інцидентів. При складанні такого списку використовують методи, що дозволяють ранжирувати інциденти і відібрати серед них найбільш небезпечні. Серед таких є методи, що спираються на індекси небезпеки й експертні методи експрес–оцінювання небезпек. У блоці 6 передбачається складання сценаріїв аварій на основі підсумкового списку інцидентів.

Заключний блок ПАТ містить розробку рекомендацій щодо зниження рівня небезпеки ХТО.

Методи попереднього аналізу небезпек, прихованих у ХТО, важко формалізувати, здебільшого вони мають якісний характер. При проведенні ПАТ широко використовуються експертні оцінки.

У Західних країнах виключно велика увага приділяється проблемі забезпечення безпеки хіміко-технологічних та інших небезпечних об'єктів. Так, у 1977 р. Т. Клетц, спеціаліст з питань промислової безпеки, засвідчив нові принципи забезпечення технічної безпеки, названі принципами «природної» безпеки[29].

Суть цих принципів проста – при створенні перед усім хімічно небезпечних об'єктів необхідно:

– мінімізувати маси використовуваних небезпечних речовин;

– замінювати матеріали і речовини менш небезпечними;

– реалізовувати менш небезпечні умови ведення процесів з менш небезпечними формами існування матеріалів або створювати виробництва, які характеризуються більш низьким рівнем впливу витоків небезпечних речовин або енергії;

– спрощувати проектовані промислові об'єкти, виключаючи невиправдані ускладнення, які менш чутливі до помилок. при виборі та функціонуванні обладнання, до помилок керування і помилок персоналу.

7.4. План ліквідації аварійних ситуацій (ПЛАС)

План ліквідації аварійних ситуацій (ПЛАС) складають відповідно до Положення[30].

29. Kletz T.A. What You Don't Have, Can't Leak / T. A. Kletz // Chemistry and Industry. – 1978. – 6 May. – P. 287–292.

30. «Положення щодо розробки планів локалізації та ліквідації аварійних ситуацій і аварій», затверджено наказом Комітету з нагляду за охороною праці України 17.06.99 № 112, зареєстровано в Міністерстві юстиції України 30 червня 1999 р. за № 424/3717.

У тексті Положення слово "Держнаглядохоронпраці" замінено словом "Держгірпромнагляд" у відповідному відмінку згідно з Наказом Державного комітету України з промислової безпеки, охорони праці та гірничого нагляду N 224 (z1176–07) від 01.10.2007. Нормативний акт поширюється на потенційно небезпечні підприємства (далі – підприємства), потенційно небезпечні об'єкти (далі – об'єкти), на яких можливі аварії із залповими викидами вибухонебезпечних і токсичних продуктів, вибухами й загораннями (пожежами) в апаратурі, виробничих приміщеннях і зовнішніх спорудах, які можуть призвести до зруйнування будинків, споруд, технологічного устаткування, ураження людей, негативного впливу на довкілля. Нормативний акт встановлює порядок розробки планів локалізації та ліквідації аварійних ситуацій і аварій (далі – ПЛАС), вимоги до їх складу, змісту та форми, процедуру затвердження й перегляду ПЛАС.

Вимоги цього нормативного акта обов'язкові для всіх міністерств, відомств, підприємств, організацій, юридичних і фізичних осіб незалежно від їхньої галузевої та/або відомчої належності й форми власності.

Вимоги даного нормативного акта не поширюються на:

- ядерні установки та підприємства з переробки радіоактивних речовин, за винятком тих об'єктів на цих підприємствах, де є оборот нерадіоактивних речовин;
- військові об'єкти;
- підприємства гірничодобувної промисловості (шахти);
- на всі види транспорту, крім трубопровідного.

Терміни та визначення, які застосовують у ПЛАСі

Аварійна ситуація – стан потенційно небезпечного об'єкта, що характеризується порушенням меж та/або умов безпечної експлуатації, але не перейшов в аварію, при якому всі несприятливі впливи джерел небезпеки на персонал, населення та навколишнє середовище утримуються у

прийнятних межах за допомогою відповідних технічних засобів, передбачених проектом.

Аварія – раптова подія, така як потужний викид небезпечних речовин, пожежа або вибух внаслідок порушення експлуатації підприємства (об'єкта), що призводить до негайної та/або подальшої загрози для життя та здоров'я людей, довкілля, матеріальних цінностей на території підприємства та/або за його межами.

Блок технологічний – апарат (устаткування) або група (з мінімальною кількістю) апаратів (устаткування), які в заданий час можна відключити (ізолювати) від технологічної системи без небезпечних змін режиму, що можуть призвести до розвитку аварії в суміжній апаратурі.

Відділення – структурний підрозділ підприємства або цеху, що містить декілька виробничих дільниць, займає відокремлену територію та здійснює частку виробничого процесу з перероблення предмета праці.

Дільниця виробнича – структурний підрозділ підприємства або цеху, що об'єднує групу робочих місць, організованих за предметним, технологічним чи предметно–технологічним принципом спеціалізації.

Критичні значення параметрів – граничні значення одного або кількох взаємопов'язаних параметрів (щодо складу матеріального середовища, тиску, температури, швидкості руху, часу перебування в зоні із заданим режимом, співвідношення компонентів, що змішуються, роз'єднання суміші та ін.), при яких можливе виникнення вибуху в технологічній системі або розгерметизація технологічної апаратури та викиди горючої або токсичної речовини в атмосферу.

Ліквідація наслідків аварії – режим функціонування, під час якого підприємство (об'єкт) після аварії переводиться в режим нормальної експлуатації або перетворюється на екологічно безпечну природно–технологічну систему.

Небезпечні режими роботи устаткування – режими, що характеризуються такими відхиленнями технологічних параметрів від

регламентних значень, при яких може виникнути аварійна ситуація та/або статися зруйнування обладнання, будинків, споруд.

Об'єкт потенційно небезпечний – будь–яке джерело потенційної шкоди життєво важливим інтересам людини.

Підприємство потенційно небезпечне – промислове підприємство, що використовує в своїй діяльності або має на своїй території потенційно небезпечні об'єкти.

Підприємство (промислове) – статутний суб'єкт, який має право юридичної особи та здійснює виробництво і реалізацію продукції певних видів із метою одержання відповідного прибутку.

Підрозділ структурний – ланка організації (підприємства), що включає колектив виконавців або/і робітників має відокремлені, чітко визначені функції в процесі керівництва або виробничому процесі, які відрізняються від функцій інших ланок, і через це входить як організаційно відокремлена від інших підрозділів частка організації (підприємства) в його структуру або в структуру підрозділів організації (підприємства). Наприклад: виробництво, цех, відділення, виробнича дільниця.

Складовою частиною виробництва можуть бути цехи, відділення, виробничі дільниці. Складовою частиною цеху можуть бути відділення і виробничі дільниці. Складовою частиною відділення є виробничі дільниці.

Процес технологічний – сукупність фізико–хімічних перетворень речовин і змін значень параметрів матеріального середовища, які проводяться з певною метою в апараті (системі взаємопов'язаних апаратів, агрегаті, машині і т. ін.).

Спеціалізовані підрозділи – гірничо–газорятувальні і пожежні частини, медична служба, підрозділи формувань органів Міністерства з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи.

Уражаючі чинники аварії – фактори, що виникають під час аварії, які здатні у разі досягнення певних значень завдати збитків здоров'ю людей,

довкіллю, матеріальним цінностям (надлишковий тиск на фронті ударної (вибухової) хвилі, теплове навантаження від полум'я, концентрація небезпечних речовин в атмосфері, воді, ґрунті тощо).

Установка – сукупність устаткування (апаратів), що виконує певну функцію в технологічному процесі.

Цех – організаційно та/або технологічно відокремлений структурний підрозділ, що прямо чи опосередковано бере участь у переробленні предмета праці на готову продукцію та складається із сукупності виробничих дільниць.

Метою плану локалізації і ліквідації аварійних ситуацій та аварій є планування дій (взаємодії) персоналу підприємства, спецпідрозділів, населення, центральних і місцевих органів виконавчої влади та органів місцевого самоврядування щодо локалізації і ліквідації аварій та пом'якшення їх наслідків.

Перелік виробництв (цехів, відділень, виробничих дільниць) і окремих об'єктів, для яких розроблюється ПЛАС, визначається і затверджується власником (керівником) підприємства за узгодженням із територіальними управліннями Держгірпромнагляду, територіальними органами Міністерства з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи (далі – МНС).

Аварії залежно від їх масштабу можуть бути трьох рівнів: **А, Б** і **В.**

На рівні **А** аварія характеризується розвитком в межах одного виробництва (цеху, відділення, виробничої дільниці), яке є структурним підрозділом підприємства.

На рівні **Б** аварія характеризується переходом за межі структурного підрозділу і розвитком її в межах підприємства.

На рівні **В** аварія характеризується розвитком і переходом за межі території підприємства, можливістю впливу уражаючих чинників аварії на

населення та інші підприємства (об'єкти), розташовані поблизу населених районів, а також на довкілля.

ПЛАС повинен охоплювати всі рівні розвитку аварії, встановлені в процесі аналізу небезпек. Дозволяється не включати в оперативну частину ПЛАС дії персоналу під час аварійних ситуацій, які регламентуються проектно–технологічною документацією (технологічний регламент, інструкція з експлуатації, інші). У такому випадку в ПЛАС мають бути посилання на документи, в яких ці дії регламентовані.

ПЛАС розробляється з урахуванням усіх станів підприємства (об'єкта): пуском, роботою, зупинкою і ремонтом.

ПЛАС повинен бути узгоджений із територіальними управліннями Держгірпромнагляду та з територіальними органами МНС, територіальними установами державної санепідслужби та, за потреби, з органами місцевого самоврядування. Відмова в узгодженні має бути мотивованою і надаватись у письмовому вигляді.

ПЛАС затверджується власником (керівником) підприємства. Оперативна частина ПЛАС для аварій рівня В затверджується органами місцевого самоврядування. Обов'язки щодо розробки і впровадження ПЛАС та відповідальність за його якість покладаються на власника (керівника) підприємства (об'єкта).

Розробка ПЛАС може виконуватися власником самостійно або із залученням спеціалізованих організацій за умови, що вони мають дозвіл на виконання такої роботи, отриманий в установленому порядку.

Територіальні управління Держгірпромнагляду й територіальні органи МНС контролюють розробку та впровадження ПЛАС на підприємстві (об'єкті).

ПЛАС ґрунтується:

– на прогнозуванні сценаріїв виникнення аварій;

– на поетапному аналізі сценаріїв розвитку аварій і масштабів їх наслідків;

– на оцінці достатності існуючих заходів, що перешкоджають виникненню і розвитку аварії, а також технічних засобів локалізації аварій;

– на аналізі дій виробничого персоналу та спеціальних підрозділів щодо локалізації аварійних ситуацій (аварій) на відповідних стадіях їх розвитку.

При розробці ПЛАС потрібно враховувати реальні можливості і ресурси підприємства, накопичений персоналом підприємства і спецпідрозділів досвід дій під час аварійних ситуацій та аварій, для забезпечення уяви щодо потрібних додаткових навичок та ресурсів.

Посадові особи, на яких цим Положенням та іншими чинними нормативно–правовими актами покладаються обов'язки щодо розробки та впровадження ПЛАС, несуть відповідальність згідно з чинним законодавством України.

ПЛАС повинен містити: титульний лист; аналітичну частину, в якій міститься аналіз небезпек можливих аварій та їх наслідків; оперативну частину, що регламентує порядок взаємодії та дій персоналу, спецпідрозділів і населення (за потреби) в умовах аварії (зміст оперативної частини змінюється залежно від рівня аварії, на який вона поширюється); додатки.

Для забезпечення ефективної боротьби з аварією на всіх рівнях її розвитку наказом створюється штаб, функціями якого є: збір і реєстрація інформації про хід розвитку аварії та вжиті заходи щодо боротьби з нею; поточна оцінка інформації і прийняття рішень щодо оперативних дій в зоні аварії та поза її межами; координація дій персоналу підприємства і всіх залучених підрозділів і служб, які беруть участь у ліквідації аварії.

Загальне керівництво роботою штабу здійснює відповідальний керівник робіт щодо локалізації та ліквідації аварій (далі – ВК).

У ПЛАС має бути визначене: місце розташування штабу, в т.ч. резервне; посадові особи, які виконують функції ВК. До ПЛАС мають бути додані копії наказу по підприємству (об'єкту) про призначення посадової

особи (осіб), які виконують функції ВК при аваріях на рівнях А і Б , та рішення органів місцевого самоврядування про призначення посадової особи (осіб), які виконують функції ВК при аваріях на рівні В .

ПЛАС має бути пронумерований, зброшурований, затверджений і узгоджений відповідними організаціями, а також скріплений печатками підприємств і організацій, які узгодили його. ПЛАС у повному обсязі повинен знаходитись у керівника й диспетчера підприємства (об'єкта), в територіальному управлінні Держгірпромнагляду, а також у територіальному органі МНС. Витяги з ПЛАС в обсязі, який є достатнім для якісного виконання відповідних дій, мають знаходитись у керівників (начальників) виробництв (цехів, відділень, виробничих дільниць), на пункті зв'язку районної (об'єктової) пожежної частини, начальника (інструктора) воєнізованої газорятувальної служби, а також на робочих місцях.

Терміни приведення у відповідність із цим Положенням тих виробництв, які проектуються, реконструюються, розпочаті будівництвом і діють, визначаються власником (керівником) підприємства за узгодженням з територіальним управлінням Держгірпромнагляду й територіальним органом МНС.

ПЛАС підлягає перегляду через кожні 5 років.

Позачерговий перегляд ПЛАС здійснюється за розпорядженням (приписом) органів Держгірпромнагляду, а також при змінах у технології, апаратурному оформленні, метрологічному забезпеченні технологічних процесів, змінах в організації виробництва, за наявності даних про аварії на аналогічних підприємствах (об'єктах). У таких випадках, залежно від конкретних обставин, ПЛАС переглядають повністю або до нього вносять зміни і доповнення. В останньому випадку узгодженню і затвердженню підлягають тільки ці зміни і доповнення.

Терміни позачергового перегляду узгоджуються з територіальним управлінням Держгірпромнагляду.

ПЛАС має переглядатися і коректуватися з урахуванням змін житлового будівництва й розвитку в цьому районі, вдосконалення дій під час аварій і досвіду, накопиченого під час тренувань та перевірок.

Після аварії слід переглядати, а за потреби – вносити зміни в ПЛАС на основі одержаного досвіду.

З метою наступної оцінки і коректування ПЛАС, накопичення та вивчення досвіду потрібно проводити аналіз дій і рішень, які були прийняті під час аварії.

Аналіз небезпеки підприємства (об'єкта) проводиться на основі докладного розгляду його стану згідно з вимогами цього Положення, міжгалузевої і галузевої нормативної документації, рекомендацій довідкової і науково–технічної літератури, а також з урахуванням аварій та аварійних ситуацій, що відбувалися на ньому та аналогічних підприємствах (об'єктах).

Під час аналізу небезпеки підприємства (об'єкта) потрібно визначити всі можливі аварійні ситуації і аварії, в тому числі й малоймовірні, з катастрофічними наслідками, які можуть виникати на підприємстві, розглянути сценарії їхнього розвитку й оцінити наслідки. Виявлення можливостей та умов виникнення аварій має виконуватись на основі аналізу особливостей роботи як окремого обладнання (апаратів, машин тощо), так і їх групи (технологічних блоків), а також з урахуванням небезпечних властивостей речовин і матеріалів, що використовуються у виробництві.

Виявлення можливих аварій потрібно проводити в такій послідовності.

1. Визначити наявність на підприємстві небезпечних речовин, небезпечних режимів роботи обладнання та об'єктів. До небезпечних речовин належать: вибухопожежонебезпечні речовини; шкідливі речовини. Небезпечні режими характеризуються такими технологічними параметрами, як тиск, вакуум, температура, напруга, склад технологічного середовища тощо.

2. Виявити потенційні види небезпеки для кожної одиниці обладнання (апарата, машини) і процесу, що проходить у ньому. До видів небезпеки, що

розглядаються, належать: пожежа; вибух (усередині обладнання, у будівлях або навколишньому середовищі); розрив або зруйнування обладнання; викид шкідливих речовин; поєднання перелічених видів небезпеки.

3. Для виявлених потенційно небезпечних об'єктів потрібно спрогнозувати сценарії виникнення і розвитку можливих аварій, що призводять до реалізації потенційних небезпек. Сценарій має починатися з події (стадії), що утворює безпосередню загрозу виходу технологічного процесу з–під контролю й виникнення аварії.

При цьому слід враховувати параметри стану речовин (температура, тиск, агрегатний стан тощо) і стан обладнання, що відповідають як нормальному технологічному режиму, а також і режимам, можливим при настанні й розвитку аварії.

На кожній стадії розвитку аварії потрібно:

- оцінити кількість небезпечних речовин, яка може взяти участь в аварії, що прогнозується;
- встановити уражаючі чинники, які притаманні виду небезпеки, який реалізується під час аварії;
- оцінити наслідки впливу уражаючих чинників аварії на сусідні об'єкти й людей з урахуванням властивостей цих об'єктів і їх взаєморозташування: визначаються масштаби зон руйнування, ураження людей і зараження місцевості;
- визначити безпечні зони й місця можливих сховищ, шляхи евакуації, що не потрапляють під вплив уражаючих чинників аварії.

За результатами аналізу виникнення й розвитку аварій та оцінки їх наслідків потрібно встановити можливість переходу аварії на рівні Б і В. Для кожної стадії сценарію розвитку аварії надається код.

Оцінка наслідків аварії та її окремих стадій виконується за допомогою методик, наведених у нормативно–технічній документації і довідковій

літературі. Аналіз небезпеки надається у вигляді звіту або пояснювальної записки, який повинен містити:

- використану вихідну інформацію або посилання на документи, в яких вона міститься;
- опис використаних методів аналізу й методик оцінки або відповідні посилання на них;
- результати розрахунків і оцінок.

Результати аналізу надаються:

- для устаткування (апаратів, машин тощо) – у вигляді картки небезпеки;
- для технологічного блоку (стадії технологічного процесу) – у вигляді стислої характеристики небезпеки блоку;
- для підприємства – у вигляді плану підприємства;
- для регіону – у вигляді ситуаційного плану.

Результати виконаного аналізу мають пройти незалежну експертизу.

Вимоги до складання оперативної частини ПЛАС для аварій на рівнях А і Б

Оперативна частина ПЛАС розроблюється для керівництва діями персоналу підприємства, добровільних і спеціалізованих підрозділів з метою запобігання аварійним ситуаціям та аваріям на відповідних стадіях їхнього розвитку або локалізації їх з метою зведення до мінімуму наслідків аварії для людей, матеріальних цінностей і довкілля, запобігання її розповсюдженню на інші виробництва (цехи, відділення, виробничі дільниці) підприємства й за його межі, рятування і виведення людей із зони ураження та потенційно небезпечних зон.

При розробці оперативної частини потрібно: забезпечити узгодженість дій персоналу підприємства й спецпідрозділів; запровадити перелік посадових осіб, відповідальних за виконання конкретних дій; запровадити порядок здійснення зв’язку зі спецпідрозділами, органами державного нагляду й органами місцевого самоврядування; викласти дії

персоналу підприємства й спецпідрозділів щодо локалізації і ліквідації аварій на відповідних стадіях їхнього розвитку. В тих випадках, коли у спецпідрозділах є свої плани дій, замість опису може бути дано посилання на ці плани; надати розпізнавальні ознаки рівней аварії і їх значення, за якими керівництво роботами щодо локалізації і ліквідації аварії переходить на рівні Б і В.

Оперативна частина ПЛАС для аварій на рівні А повинна містити:

- блок–схему виробництва (цеху, відділення, виробничої дільниці);
- план виробництва (цеху, відділення, виробничої дільниці);
- блок–карти об'єктів (цехів, відділень, виробничих дільниць), які входять до складу виробництва;
- опис дій персоналу;
- список і схему оповіщення посадових осіб, які мають бути терміново сповіщені про аварійну ситуацію (аварію);
- список робітників, що залучаються до локалізації аварії, осіб, що дублюють їхні дії за відсутності перших з будь–яких причин, із зазначенням місць їх постійної роботи, проживання й номерів телефонів;
- перелік інструментів, матеріалів, засобів індивідуального захисту, які мають бути використані при локалізації аварії, із зазначенням місць їх зберігання (аварійних шаф);
- обов'язки відповідального керівника робіт, виконавців і інших посадових осіб щодо локалізації аварії;
- інструкцію щодо аварійної зупинки виробництва (цеху, відділення, виробничої дільниці).

У блок–схемі виробництва (цеху, відділення, виробничої дільниці) визначаються його складові частини без деталізації їх. На блок–схемі визначаються прямі та зворотні міжцехові потоки, їх характеристики й параметри, відповідна, в тому числі і гранична для виробництва (цеху, відділення, виробничої дільниці) відсічна арматура, які мають безпосереднє

значення для локалізації (ліквідації) аварії. Кожний елемент блок–схеми повинен мати буквене або цифрове позначення, яке відповідає номеру позиції або умовному позначенню, нанесене на місці та/або визначене технологічним регламентом.

На плані виробництва (цеху, відділення, виробничої дільниці) має бути вказано місце розташування:

- основного технологічного обладнання і комунікацій;
- відсічної запірної арматури, що має безпосереднє відношення до локалізації (ліквідації) аварії;
- засобів протиаварійного захисту, зв'язку й оповіщення;
- евакуаційних виходів і маршрутів евакуації;
- шляхів під'їзду, ділянок для встановлення і маневрування спецтехніки;
- сховищ і місць укриття.

На плані можуть бути додатково нанесені місця найбільш імовірного виникнення аварійних ситуацій, розміри й межі потенційно небезпечних зон та інші характеристики потенційно можливих аварій.

Додатково можуть зазначатися кількісні показники, що характеризують потенційну небезпеку блоків, показники тяжкості наслідків можливих аварій, основні дестабілізуючі фактори і критичні значення параметрів процесу.

Блок-карту належить складати для кожного об'єкта, який входить до складу виробництва (цеху, відділення, виробничої дільниці), що розглядається. Блок-карта повинна містити:

- принципову технологічну схему об'єкта;
- план розташування устаткування об'єкта;
- стислу характеристику небезпеки технологічних блоків, що входять до складу об'єкта.

Кожний елемент блок-карти повинен мати буквене або цифрове позначення, що відповідає номеру позиції або умовному позначенню, що нанесене на місці та/або визначене технологічним регламентом.

На принциповій технологічній схемі та на плані розташування устаткування повинні бути визначені межі технологічних блоків. Межами технологічних блоків можуть бути, як правило, автоматичні відсікачі, запірна арматура з дистанційним керуванням, ручна запірна арматура (за умови можливості практичного користування в аварійній ситуації), яка встановлена на трубопроводах або устаткуванні як по прямому, так і по зворотному потоку матеріального середовища.

У разі обігу в технологічній системі пилостворювальних дисперсних продуктів межами блока можуть бути шнекові живильники, секторні затвори та інші пристрої, що забезпечують щільність (герметичність) системи при підвищеному тиску в умовах внутрішнього вибуху.

На принциповій технологічній схемі потрібно відобразити технологічні параметри й основні технічні характеристики устаткування, прямі та зворотні технологічні потоки (із зазначенням їх умовного перетину, продуктивності й параметрів), регулювальну й запірну арматуру (умовне позначення, тип виконання, швидкість дії), прилади, засоби й системи контролю і регулювання, системи протиаварійного захисту (із зазначенням їх основних характеристик), які мають безпосереднє відношення до локалізації (ліквідації) аварії.

Забороняється перевантажувати схему елементами, що не мають прямого відношення до ліквідації аварійної ситуації (аварії).

На плані розташування обладнання позначають місця розміщення устаткування об’єкта із зазначенням технологічних потоків, відсічної запірної арматури, систем протиаварійного призначення, пультів (пристроїв) керування, автоматичних сповіщувачів і засобів зв’язку, які мають безпосереднє відношення до локалізації (ліквідації) аварії. У разі потреби план складається для кожної відмітки.

У стислій характеристиці небезпеки технологічного блока має бути зазначено:

- основні небезпеки блока і їх характеристики (наприклад, кількість шкідливих речовин, енергетичний потенціал вибухонебезпеки та ін.);
- можливі аварії і зони ураження;
- інші потрібні відомості.

Розділ «Опис дій персоналу» потрібно оформляти у вигляді таблиці, яка містить три графи:

графа 1 – «Найменування і код аварії (стадії)». У цій графі зазначаються найменування стадії розвитку аварії за прийнятими сценаріями із зазначенням коду й місця;

графа 2 – «Розпізнавальні ознаки». У цій графі зазначаються розпізнавальні ознаки із зазначенням засобів контролю, їх позицій і показань, а також зовнішніх ефектів та інших критеріїв, за якими може бути ідентифікована та чи інша стадія розвитку аварії;

графа 3 – «Перелік виконавців, порядок їх дій».

Порядок дій виконавців має передбачати:

- виявлення й оцінку аварії або загрози її виникнення за розпізнавальними ознаками;
- оповіщення персоналу виробництва (цеху, відділення, виробничої дільниці) й диспетчера підприємства (об’єкта) про аварію або загрозу її виникнення;
- увімкнення протиаварійних систем;
- вимкнення пошкодженої дільниці, повну або часткову зупинку виробництва (цеху, відділення, виробничої дільниці);
- виведення з небезпечної зони персоналу із зазначенням порядку забезпечення його засобами індивідуального захисту;
- інші заходи, що запобігають розвитку аварії, з урахуванням специфіки виробництва.

Описуючи дії персоналу, необхідно особливо підкреслити ті з них, які не допускають зволікань і потребують негайного виконання. Описуючи дії спецпідрозділів, потрібно зазначити орієнтовний час їх прибуття і розгортання.

В інструкції щодо аварійної зупинки виробництва (підприємства), яка є складовою оперативної частини ПЛАС, для кожної аварії повинні бути визначені послідовність уведення в дію систем протиаварійного захисту, вимкнення апаратів і механізмів, вимкнення електроенергії та інших енергоносіїв, режим роботи вентиляції і систем очищення повітря, порядок використання засобів рятування людей і ліквідації аварії.

При цьому має бути врахований вплив виконуваних переключень і вимкненнь на роботу систем протиаварійного захисту, життєзабезпечення та інших систем, які є суттєвими під час ліквідації аварії.

Оперативна частина ПЛАС для аварій на рівні Б містить додатково: блок–схему підприємства; план підприємства.

У блок–схемі підприємства потрібно позначити виробництва без поділу їх на окремі цехи, відділення або виробничі дільниці (за аналогією з блок–схемою виробництва), прямі та зворотні міжвиробничі потоки, їх характеристики й параметри, міжвиробничу й граничну для підприємства відсічну арматуру, її тип і основні технічні характеристики (умовне позначення, тип виконання, швидкодія), які мають безпосереднє відношення до локалізації (ліквідації) аварії.

Кожний елемент блок–схеми повинен мати буквене або цифрове позначення, що відповідає номеру позиції або умовному позначенню, що нанесені на місці та/або прийняті технологічним регламентом.

На плані підприємства потрібно визначити:

- місця розташування виробництв;
- місця скупчення небезпечних продуктів із зазначенням найменування й маси продукту;

- прямі та зворотні міжвиробничі потоки, їхні характеристики й параметри;
- міжвиробничу відсічну арматуру, її тип і основні технічні характеристики;
- засоби протиаварійного захисту;
- засоби зв'язку й оповіщення;
- евакуаційні виходи і маршрути евакуації;
- сховища й місця укриття;
- шляхи під'їзду, місця встановлення й маневрування спецтехніки;
- місця найбільш імовірного виникнення аварійних ситуацій (аварій);
- зони можливого ураження обслуговуючого персоналу підприємства з урахуванням розповсюдження вибухових і ударних хвиль, напрямку руху вибухонебезпечних і токсичних хмар.

Як план підприємства може бути використаний генплан із необхідними додатками.

Вимоги до складання оперативної частини ПЛАС для аварій на рівні В

Оперативна частина розроблюється для керівництва діями відповідних служб і підрозділів із метою запобігання розвитку аварії і розповсюдженню її на інші підприємства (об'єкти), для рятування та виведення людей із зони ураження й потенційно небезпечних зон.

При розробці оперативної частини слід визначити всіх учасників протиаварійних дій. Крім того, потрібно реально з'ясувати їхні функції, ресурси, обов'язки й ступінь участі. До складу учасників протиаварійних дій повинні входити:

- органи Держгірпромнагляду;
- спеціальні формування – районна (об'єктна) пожежна частина, воєнізована газорятувальна служба та інші;

- міліція, медична (у тому числі лікарні), транспортна служби та служба соціального забезпечення;
- органи з керівництва аварією та/або територіальні органи МНС;
- комунальні служби району (міста);
- керівництво підприємства;
- органи масової інформації і зв'язку;
- органи охорони здоров'я і навколишнього середовища.

При розробці оперативної частини потрібно:

- передбачити процедуру залучення населення до робіт щодо локалізації і ліквідації аварії;
- передбачити узгоджені дії виробничого персоналу, усіх залучених підрозділів і служб, а також населення;
- забезпечити спільні дії персоналу розташованих поруч підприємств (об'єктів) і органів місцевого самоврядування сусідніх районів.

Оперативна частина повинна містити:

- титульний лист;
- ситуаційний план із додатками;
- обов'язки ВК, виконавців і інших посадових осіб щодо локалізації аварії.

Ситуаційний план розроблюється для здійснення керівництва й координації дій персоналу підприємства (об'єкта), спецпідрозділів, формувань МНС, інших організацій, що залучаються для локалізації аварії, організації великомасштабних рятувальних робіт і евакуації людей з небезпечних зон.

На ситуаційному плані позначаються промисловий майданчик підприємства (об'єкта) на місцевості, а також житлові райони, населені пункти, інші підприємства й організації, що розташовані поруч із ним і на які може поширюватися дія уражаючих чинників аварії. Розмір території, яка охоплюється ситуаційним планом, визначається масштабом зон ураження (зараження).

На ситуаційний план наносять:

- зони можливого ураження за різними сценаріями розвитку аварій;
- чисельність людей у цих зонах і час досягнення їх уражаючими чинниками аварії з урахуванням швидкості й напрямку вітру, погодних умов, рельєфу місцевості;
- можливі шляхи евакуації населення і безпечні зони, сховища, укриття;
- місця розташування засобів протиаварійного захисту, джерел аварійного енерго– і водопостачання, а також наявність і місцезнаходження запасів засобів пожежогасіння: води, піноутворювача, вогнегасильного порошку, засобів захисту органів дихання;
- місця розташування аварійно–рятувальних підрозділів, пожежних частин та ін., можливі місця їх розгортання і маневрування;
- місця скупчення небезпечних продуктів поза територією підприємства із зазначенням найменування й маси продукту.

До ситуаційного плану додають:

- план підприємства (об’єкта) ;
- схему зв’язку, порядок оповіщення і взаємодії органів керівництва комісії з надзвичайних ситуацій з організаціями й формуваннями МНС, що залучаються при цьому, як у даному, так і в сусідніх регіонах (у разі потреби);
- відомості щодо наявності частин МНС, радіаційного й хімічного захисту, пожежних і газорятувальних частин, медичних служб, їх чисельності, оснащеності, часу розгортання;
- відомості щодо невоєнізованих формувань підприємства (об’єкта);
- відомості щодо наявності засобів гасіння пожежі й нейтралізації викидів на підприємстві (об’єкті) і в спецслужбах;
- заходи щодо евакуації і рятування людей із зазначенням переліку, місця розташування й порядку залучення захисних споруд, медичних служб і засобів, технічних і транспортних засобів, засобів індивідуального захисту

людей, у тому числі із зазначенням кількості технічних та інших засобів, які потрібні для цього;

- склад штабу (оперативної групи для ліквідації аварії) і порядок оповіщення його членів;
- порядок оповіщення робітників підприємства (об'єкта) і населення, що мешкає поблизу підприємства (об'єкта), про аварію;
- порядок постійної інформації щодо ходу розвитку аварії, перебігу робіт із її локалізації (ліквідації), щодо належної поведінки й заходів безпеки на цей момент;
- порядок організації розвідки пожежі;
- порядок організації розвідки й спостереження осередку хімічного ураження, зони можливого зараження шкідливими речовинами;
- організацію медичного забезпечення, життєзабезпечення евакуйованих у місцях їх збору;
- порядок проведення заходів щодо зниження запасу шкідливих речовин і безаварійної зупинки виробництва;
- порядок взаємодій між спецпідрозділами і залученими організаціями.

Повноваження та обов'язки відповідального керівника робіт

Керівництво роботами з ліквідації аварії, рятування людей та зниження впливу небезпечних чинників аварії на майно (власність), людей та на довкілля здійснює **ВК** – *відповідальний керівник* робіт.

З метою полегшення виявлення ВК серед осіб, які знаходяться в місці розташування органу керівництва локалізацією аварії, він повинен мати одяг (каску, куртку та інше) яскравого оранжевого кольору. Забороняється іншим особам, крім ВК, носити одяг, який пофарбовано аналогічним кольором.

Забороняється втручатися в дії ВК. При явно невірних діях відповідального керівника робіт вища керівна особа має право звільнити його й

прийняти на себе керівництво ліквідацією аварії або призначити для цього іншу відповідальну особу.

Обов'язки ВК виконують:

- на рівні розвитку аварії «А» – начальник виробництва (цеху, відділення, виробничої дільниці). До його прибуття на місце аварії обов'язки ВК виконує його заступник або спеціально призначена особа, яка повинна бути зазначена в ПЛАС;
- на рівні розвитку аварії «Б» – керівник підприємства. До його прибуття на місце аварії обов'язки ВК виконує його заступник або спеціально призначена особа, яка повинна бути зазначена в ПЛАС;
- на рівні розвитку аварії «В» – посадова особа, призначена рішенням органу місцевого самоврядування. До її прибуття на місце обов'язки ВК виконує керівник підприємства.

При виникненні під час аварії пожежі відповідальним керівником її гасіння є старша посадова особа МНС.

ВК зобов'язаний на рівні розвитку аварії «А»:

– оцінити умови, виявити кількість і місцезнаходження людей, захоплених аварією, вжити заходів щодо оповіщення робітників підприємства та населення (за потреби) про аварію;

– вжити заходів щодо оточення району аварії і небезпечної зони;

– вжити негайних заходів щодо рятування людей, локалізації та ліквідації аварії;

– забезпечити виведення з небезпечної зони людей, які не беруть безпосередньої участі в ліквідації аварії;

– обмежити допуск людей та транспортних засобів до небезпечної зони;

– контролювати правильність дій персоналу, а в разі потреби – дії газорятувальних, пожежних, медичних підрозділів щодо рятування людей, локалізації і ліквідації аварії на виробництві, та виконання своїх розпоряджень;

– інформувати безпосереднє керівництво, органи Держгірпромнагляду, а за потреби – територіальні органи МНС, органи місцевого самоврядування і засоби масової інформації про перебіг і характер аварії, про потерпілих під час рятувальних робіт;

– уточнювати та прогнозувати перебіг розвитку аварії, за потреби вносити корективи в оперативну частину плану;

на рівні розвитку аварії «Б» додатково :

– сповістити про місце розташування органу управління роботами щодо локалізації аварії;

– уточнити з територіальним органом МНС, організаціями охорони здоров'я та іншими організаціями порядок евакуації потерпілих, персоналу підприємства, а в разі потреби – й місцевого населення;

– управляти діями персоналу підприємства, газорятувальних, пожежних, медичних підрозділів щодо рятування людей, локалізації і ліквідації аварії на підприємстві та контролювати виконання своїх розпоряджень;

на рівні розвитку аварії «В» додатково:

– уточнити з територіальним органом МНС, організаціями охорони здоров'я та іншими організаціями порядок евакуації потерпілих, персоналу сусідніх підприємств і організацій, а в разі потреби – й місцевого населення;

– визначити коло і порядок залучення організацій, технічних і транспортних засобів; наявність і потребу в медикаментах, засобах гасіння пожежі, засобах індивідуального захисту та ін., спосіб їх постачання, місце розташування потерпілих та евакуйованих людей;

– організувати надання медичної допомоги потерпілим;

– організувати харчування та відпочинок осіб, які беруть участь у ліквідації аварії.

Обов'язки власника (керівника) підприємства (об'єкта)

Власник (керівник) підприємства (об'єкта) зобов'язаний:

- розробити спеціальні програми (з визначенням пріоритету щодо реалізації), які передбачають дооснащення засобами контролю, автоматичного

регулювання, обладнанням вибухопопередження та вибухозахисту, швидкодіючими відсікачами, системами безпечної аварійної зупинки підприємства (об'єкта), оповіщення, захисту та рятування людей, створення запасів дегазувальних реагентів, вдосконалення систем уловлювання та дегазації шкідливих викидів, влаштування систем локалізації, що перешкоджають розповсюдженню неорганізованих викидів на території підприємства та за його межами, та інше, якщо під час розробки ПЛАС виявляється недостатня готовність підприємства (об'єкта) до протиаварійного захисту;

- передбачити у разі потреби установлення резервних систем життєзабезпечення, сигналізації і протиаварійного захисту. Наприклад, повинні існувати резервні мережі зв'язку, має бути призначені дублери для провідних фахівців, повинен бути визначений альтернативний центр керівництва, якщо порушено функціонування основного центру, повинні бути продубльовані життєво важливі вузли на об'єктах підвищеної небезпеки;
- забезпечити оперативність виявлення, ефективність локалізації та ліквідації аварії за рахунок застосування технічних засобів із належною надійністю та швидкодією;
- забезпечити відповідність оперативності дій персоналу підприємства динаміці розвитку можливих аварій: шляхом забезпечення розподілу обов'язків між виробничим персоналом, використання надійних засобів оповіщення та зв'язку й раціонального розташування пультів (пристроїв) керування протиаварійними системами;
- при визначенні обов'язків персоналу в разі аварії потрібно враховувати можливість відсутності окремих робітників внаслідок хвороби, відпустки, свят;
- Оперативно повідомляти органи, що відповідають за дії з локалізації аварії, про всі випадки, які пов'язані з небезпечними речовинами і можуть завдати шкоди здоров'ю людини та навколишньому середовищу.

Повідомлення повинна здійснювати посадова особа, яка має на це право і може надати якомога оперативніше інформацію про характер випадку, небезпечні речовини, задіяні в ньому, потенційну складність випадку, можливість виявлення дії уражаючих чинників аварії за межами території підприємства;

- передбачати забезпечення сучасними антидотами та іншими фармацевтичними препаратами, в тому числі киснем, якщо на підприємстві є шкідливі речовини, а також забезпечити наявність постійно оновлюваного запасу відповідних медичних препаратів, які необхідні при аварії, дезактиваційного обладнання для застосування на майданчику та в лікарнях, а також, за можливості, засобів захисту для персоналу медичних бригад невідкладної допомоги;
- передати органам місцевого самоврядування результати виконаного аналізу небезпеки підприємства (об'єкта), а також інші матеріали, потрібні для розробки ПЛАС;
- надати засобам масової інформації дані про всі небезпеки, які були встановлені в процесі аналізу;
- співробітничати з центральними та місцевими органами виконавчої влади та органами місцевого самоврядування при розробці оперативної частини ПЛАС для аварій рівня «В».

Впровадження ПЛАС. ПЛАС і зміни до нього (в потрібному для якісного виконання своїх обов'язків обсязі) повинні бути вивчені персоналом організацій, що беруть участь у ліквідації аварії, та відповідними спецслужбами. Допуск до роботи осіб, які у встановленому порядку не пройшли навчання, інструктаж і перевірку знань ПЛАС, забороняється. Персонал усіх організацій, які беруть участь у ліквідації аварії, повинен проходити навчання і практичну підготовку з метою підтримки постійної готовності. На великих підприємствах для персоналу може бути організовано спеціальне курсове навчання з ПЛАС на навчально-

тренувальних полігонах з використанням комп'ютерних тренажерів і інших сучасних технічних засобів навчання. Протягом року з імовірних аварійних ситуацій, що передбачені ПЛАС, повинні проводитись навчально–тренувальні заняття і навчальні тривоги.

Графік проведення навчально-тренувальних занять і навчальних тривог затверджується керівником підприємства (об'єкта) або органом місцевого самоврядування, залежно від рівня аварії, та узгоджується з територіальним управлінням Держгірпромнагляду й територіальним управлінням МНС. Навчальні тривоги проводяться під керівництвом ВК за участі всіх організацій, участь яких передбачається оперативною частиною ПЛАС. При незадовільних результатах навчальної тривоги вона має бути проведена вдруге протягом 10 днів, після детального вивчення допущених помилок.

При проведенні тренувань слід практикувати участь незалежних спостерігачів, оскільки це забезпечує об'єктивну оцінку недоліків або помилок ПЛАС. Необхідно також проводити тренування в екстремальних умовах (наприклад, під час перезміни, вночі, в холодну погоду, та ін.). Персонал сторонніх організацій і особи, що відвідують підприємство (об'єкт), повинні бути проінструктовані про свої дії у випадку виникнення аварії. Необхідно підтримувати постійну готовність обладнання й засобів інформації, які можуть знадобитися для отримання необхідних даних у випадку аварії. Сюди можна віднести, наприклад, аналітичні методи і засоби для виявлення небезпечних речовин, а також заходи, що впроваджуються при пошкодженні захисної оболонки небезпечної речовини. Необхідно повідомити населення щодо систем оповіщення про аварійну ситуацію (аварію), які використовуються. Ці системи потрібно періодично перевіряти.

ДОДАТОК

Таблиця Д.1. - Огляд можливих пов’язаних з професійною діяльністю інфекційних захворювань, що уражають серцево–судинну систему

Захворю-вання	Ураження серця	Випадки / Частота ураження серця у разі захворювання	Професійні групи ризику
1	2	3	4
СНІД / ВІЛ	Міокардит, Ендокардит, Перикардит	42 % (Blanc та ін. 1990); умо-вно–патогенна інфекція, а також саме безпосередньо ВІЛ, що спричиняє лімфоцитарний міокардит (Beschorner та ін. 1990)	Персонал медичних і соціальних служб
Аспергільоз	Ендокардит	Рідко; переважно в осіб з приг ніченою імунною системою	Фермери
Бруцельоз	Ендокардит, Міокардит	Рідко (Gross, Jahn і Schulmerich, 1970; Schulz і Stobbe, 1981)	Робітники - паку-вальники м’яса, зайняті розведенням тварин, фермери, ветеринари
Хвороба Чагаса	Міокардит	Дані варіюють: 20 % в Арген-тині (Acha і Szyfres 1980); 69 % в Чилі (Arribada та ін., 1990); 67 % (Higuchi та ін., 1990); хронічна форма хвороби Чагаса завжди з міокардитом (Gross, Jahn і Schulmerich, 1970)	Виїжджають в біз-нес-поїздки в Центральну і Пів-денну Америку

Продовження табл.Д.1.

1	2	3	4
Коксакі вірус	Міокардит, Перикардит	Від 5 % до 15 % збудник – Коксакі вірус типу В (Reindell і Roskamm, 1977)	Персонал медичних і соціальних служб, робітники, які обслуговують каналізаційні системи
Цитомегаловірус	Міокардит, Перикардит	Надзвичайно рідко, зазвичай серед осіб з пригніченою імунною системою	Персонал, що працює з дітьми (особливо з маленькими дітьми), у відділеннях діалізу та трансплантації
Дифтерія	Міокардит, Ендокардит	Локалізована форма 10 – 20 %, більш поширене прогресуюче Д. (Gross, Jahn і Schulmerich 1970), особливо токсична форма	Персонал, що працює з дітьми і в медичних установах
Ехінококоз	Міокардит	Рідко (Riecker, 1988)	Робітники лісової промисловості
Інфекція, що спричиняється вірусом Епштейна – Барра	Міокардит, Перикардит	Рідко; зазвичай серед осіб з недостатністю імунної системи	Персонал медичних і соціальних служб

Продовження табл. Д.1.

1	2	3	4
Еризипелоїд	Ендокардит	Дані варіюють від рідкісних випадків (Gross, Jahn і Schulmerich, 1970; Riecker, 1988) до 30 % (Azofra та ін. 1991)	Робітники з упакування м'яса, переробці риби, рибалки, ветеринари
Філяріоз	Міокардит	Рідко (Riecker, 1988)	Виїжджаючі у ділові поїздки в ендемічні райони
Тиф серед інших рикетсіозів (спричиняючи Ку-гарячку)	Міокардити, Васкуліти дрібних судин	Дані варіюють; пряма дія збудника захворювання, токсичне ураження або зниження опірності в процесі лікування гарячки	Виїжджаючі у ділові поїздки в ендемічні райони
Весняний менінго–енцефаліт	Міокардит	Рідко (Sundermann, 1987)	Робітники лісової промисловості, садівничих господарств

Продовження табл. Д.1.

1	2	3	4
Жовта гарячка	Токсичне ураження судин (Gross, Jahn і Schulmerich, 1970), Міокардит	Рідко; відомі важкі випадки	Виїжджаючі у ділові поїздки в ендемічні райони
Геморагічна гарячка (Ебола, Марбург, Ласса, Денге та ін.)	Міокардит і ендокардіальні крововиливи на фоні загальної кровотечі, недостатність серцево-судинної системи	Інформації немає	Співробітники медичних служб заражених районів і спеціальних лабораторій, робітники, що займаються розведенням тварин
Грип	Міокардит, Крововиливи	Дані варіюють від рідкісних випадків до частих (Schulz і Stobbe, 1981)	Співробітники медичних установ

Продовження табл. Д.1.

1	2	3	4
Гепатит	Міокардит (Gross, Willensand Zeldis, 1981; Schulz і Stobbe, 1981)	Рідко (Schulz і Stobbe, 1981)	Співробітники медичних і соціальних служб, робітники, які обслуговують каналізації та системи стічних вод
Легіонельоз	Перикардит, Міокардит, Ендокардит	Якщо трапляється, то дуже рідко (Gross, Willens і Zeldis, 1981)	Обслуговуючий персонал систем кондиціонування повітря, зволоження, водопостачання, персонал з догляду (Maintenance personnel in air conditioning, humidifiers, whirlpools, nursing staff)
Лейшманіоз	Міокардит (Reindell і Roskamm, 1977)	У поєднанні з вісцеральним лейшманіозом	Виїжджаючі у ділові поїздки в ендемічні райони

Продовження табл. Д.1.

1	2	3	4
Лептоспіроз (жовтянична форма)	Міокардит	Токсичне або пряме ураження збудником захворювання (Schulz і Stobbe, 1981)	Робітники каналізації і систем стічних вод, боєнь
Лістерел-леза	Ендокардит	Дуже рідко (переважає шкірний лістеріоз як профзахворювання)	Фермери, ветеринари, робітники, зайняті в м'ясопереробних галузях
Хвороба Лайма	На 2–й стадії: Міокардит, Панкардит. На 3–й стадії Хронічний кардит	8 % (Mrowietz, 1991) або 13 % (Shadick та ін., 1994)	Робітники лісової промисловості
Малярія	Міокардит	Відносно часто у випадку тропічної малярії (Sundermann, 1987); пряме інфекційне ураження капілярів	Виїжджаючі у ділові поїздки в ендемічні райони
Кір	Міокардит, Перикардит	Рідко	Персонал медичних установ і працюючі з дітьми

Продовження табл. Д.1.

1	2	3	4
Ящур	Міокардит	Дуже рідко	Фермери, робітники, зайняті розведенням тварин (особливо з парнокопитних тварин)
Свинка (Епідемічний паротит)	Міокардит	Рідко – менше 0.2 – 0.4 % (Hofmann, 1993)	Персонал медичних установ і працюючі з дітьми
Інфекція, що спричиняється видом мікоплазми Mycoplasma pneumonia	Міокардит, Перикардит	Рідко	Працівники медичних і соціальних служб
Орнітоз / Пситтакоз	Міокардит, Ендокардит	Рідко (Kaufmann і Potter), 1986; Schulz і Stobbe, 1981)	Особи, які займаються розведенням декоративної і свійської птиці, працівники зоомагазинів, ветеринари

Продовження табл. Д.1.

1	2	3	4
Паратиф	Інтерстиціалний міокардит	Особливо серед літніх і тяжко хворіючих як токсичне ураження	Працівники програм розвитку та допомоги в тропіках і субтропіках
Поліомієліт	Міокардит	Поширена у важких випадках протягом першого та другого тижня	Працівники медичних установ
Ку-гарячка	Міокардит, Ендокардит, Перикардит	Можливо у людей віком до 20 років після гострого захворювання (Behymer і Riemann 1989); дані варіюють від рідкісних випадків (Schulz і Stobbe, 1981; Sundermann, 1987) до 7.2 % (Conolly та ін., 1990); більш часто (68 %) у разі хронічної Ку–гарячка в осіб з ослабленою імунною системою або з раніше існуючим захворюванням серця (Brouqui та ін., 1993)	Робітники, що займаються розведенням тварин, ветеринари, фермери, можливо також робітники боєнь та птахоферм
Кірева краснуха	Міокардит, Перикардит	Рідко	Працівники медичних і дитячих установ

Продовження табл. Д.1.

1	2	3	4
Зворотна гарячка	Міокардит	Інформації немає	Виїжджаючі у ділові поїздки і медичні працівники в тропіках і субтропіках
"Червона гарячка" та інші стрептококові інфекції	Міокардит, Ендокардит	Від 1 до 2,5 % випадків ревматичної гарячки зустрічається як ускладнення (Dukert, 1981), далі від 30 до 80 % випадків кардита (Sundermann, 1987); від 43 до 91 % (al-Eissa, 1991)	Персонал медичних установ і працюючі з дітьми
Сонна хвороба	Міокардит	Рідко	Виїжджаючі в ділові поїздки в африканські регіони, розташовані між 20° південної та північної паралелі
Токсоплазмоз	Міокардит	Рідко, зазвичай серед осіб з ослабленою імунною системою	Люди, що мають професійний контакті з тваринами

Продовження табл. Д.1.

1	2	3	4
Туберкульоз	Міокардит, Перикардит	Міокардит, особливо в поєднанні з міліарним туберкульозом, перикардит при значному поширенні туберкульозу до 25 %, в іншому випадку 7 % (Sundermann 1987)	Співробітники медичних установ
Черевний тиф	Міокардит	Токсичне ураження – 8 % (Bavdekar і інш. 1991)	Співробітники програм допомоги і розвитку, персонал мікробіологічних лабораторій (особливо роблять аналіз калу),
Вітрянка Герпес (Herpes zoster)	Міокардит	Рідко	Персонал медичних установ і працюючі з дітьми

Список джерел інформації

1. Березуцкий В.В. Теоретические основы безопасности жизнедеятельности : Монография / В.В. Березуцкий. – Х.: ХГПУ.– 1999.– 170 с.

2. Березуцкий В.В. Разработка универсального показателя опасности оборудования и производства/ В.В. Березуцкий, А.Н. Древаль // Охрана труда. – 1997. – №5. – С. 34 – 37.

3. Березуцкий В. В., Виртуальный производственный участок, интегрированный по вредным и опасным факторам / В.В. Березуцкий, А.Б. Радван// Восточно–Европейский журнал передовых технологий. – 2011. – № 5/2(53).— С. 52 – 57.

4. IEC 61882 Hazard and operability studies (HAZOP studies) – Application guide ISO 22000 Food safety management systems – Requirements for any organization in the food chain

5. ISO/IEC Safety aspects – Guidelines for their inclusion in standards Guide 51 IEC 60300–3–11 Dependability management – Part 3 – 11: Application guide – Reliability centred maintenance

6. IEC 61078 Analysis techniques for dependability – Reliability block diagram and Boolean methods

7. IEC 61165 Application of Markov techniques

8. ИСО/МЭК (all parts) Software and systems engineering – High–level Petri nets 15909

9. IEC 60812 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

10. IEC 61025 Fault tree analysis (FTA)

11. ISO/IEC Uncertainty of measurement – Part 3: Guide to the expression of uncertainty in measurement

12. Guide 98–3:2008 (GUM:1995)

Навчальне видання

БЕРЕЗУЦЬКИЙ Вячеслав Володимирович

АДАМЕНКО Микола Ігорович

НЕБЕЗПЕЧНІ ВИРОБНИЧІ РИЗИКИ ТА НАДІЙНІСТЬ

Навчальний посібник

(для студентів за напрямком підготовки «Цивільна безпека»,
спеціальність «Цивільна безпека», спеціалізація «Охорона праці»)

Відповідальний за випуск *В.В.Березуцький*

Роботу до видання рекомендував *М.А.Погрібний*

Редактор *О.В.Козюк*

План 2016 р.,поз. 200

Підп. до друку 04.08.2016 р. Формат 60 х 84 1/16. Папір офсетний.

Друк цифровий. Гарнітура Таймс. Ум. друк. арк. 14,4 Наклад 50 прим.

Зам. №8. Ціна договірна.

Видавець: ФОП Панов А. М.

Свідоцтво серії ДК №4847 від 06.02.2015 р.

Надруковано в поліграфцентрі «Влавке»

м. Харків, вул. Жон Мироносиць (Раднаркомівська),10, оф. 6

тел.+38 (057)714-06-74, +38(050) 976 -32-87

copy@vlavke.com.ua, http://vlavke.com.ua