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.

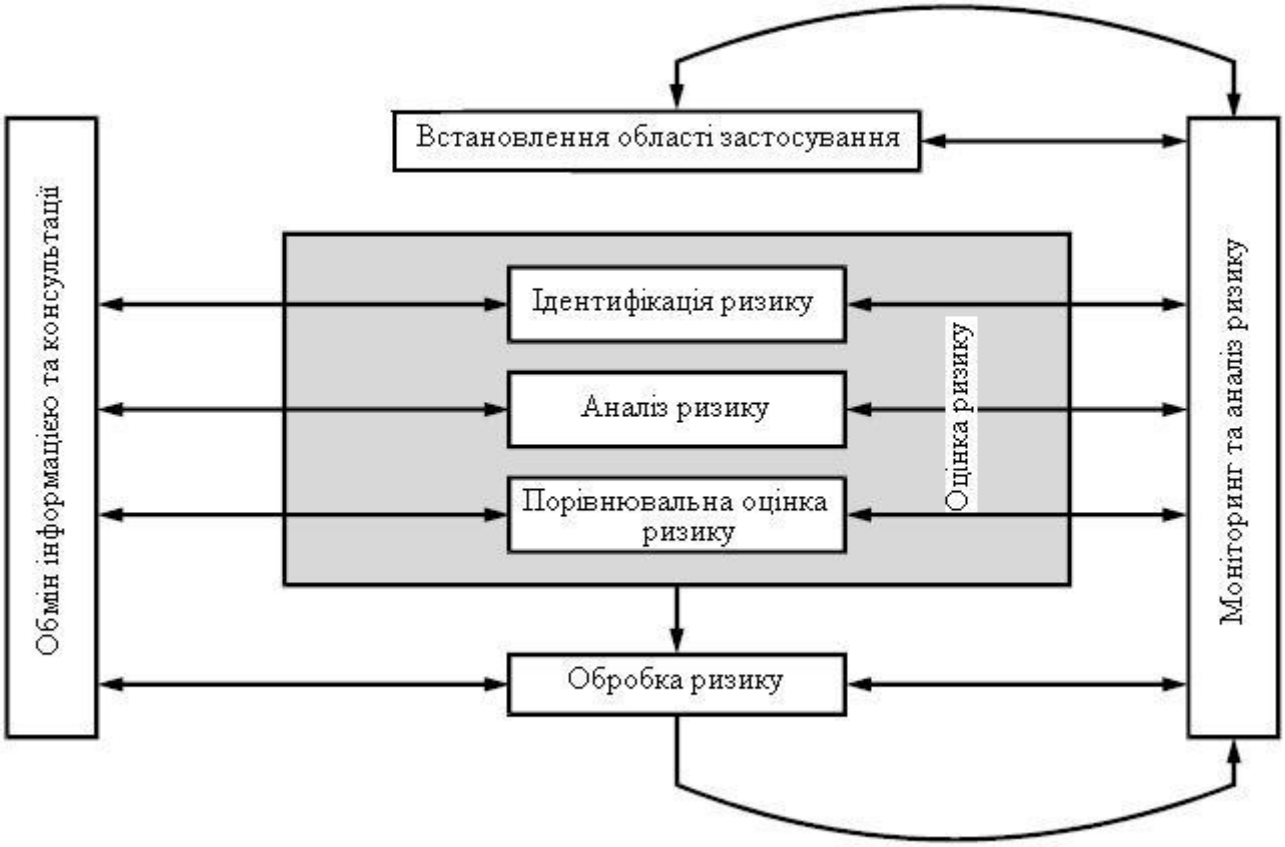

Рисунок 4.1 – Вхідні дані процесу загальної оцінки ризику

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?