Лекція 2.
Розділ 1. Безпека життєдіяльності.
Тема 1.2. Ризик як кількісна оцінка небезпек.

Ризик, як кількісна оцінка небезпек. Індивідуальний та груповий ризик. Класифікація (ідентифікація) ризиків. Загальний аналіз ризику і проблем безпеки складних систем, які охоплюють людину (керівник, оператор, персонал, населення). Методичні підходи до визначення ризику. Можливості управління ризиком. Концепція прийнятного ризику.

Література: Л1.2; Л1.10; Л1-19; Л2.1-Л2.3; Л2.6-Л2.8; Л2.20.

Кількісна оцінка небезпек

На попередній лекції ми розглядали питання виникнення, видів, характеру проявів та дії на людей небезпек природного, техногенного та соціально-політичного характеру. Зазначалося, що наслідком прояву цих небезпек стають нещасні випадки та професійні захворювання, аварії, катастрофи, які супроводжуються смертельними випадками, скороченням тривалості життя, шкодою здоров'ю, шкодою природному чи техногенному середовищу, дезорганізуючим впливом на суспільство або життєдіяльність окремих людей.

Яким же чином можна порівняти небезпеки, що мають не тільки різне походження, а і різний характер та ступінь впливу на людей, об'єкти господарювання, природне середовище? Ще більш складне питання, але й більш актуальне, це як оцінити можливу шкоду від небезпеки, яка ще не проявилась, але існує ймовірність того, що вона може проявиться і таким чином завдати певної шкоди? І найскладніше питання, які кошти необхідно вкласти для того, щоб уникнути, а якщо це неможливо, то як захиститись від існуючих небезпек?

Квантифікація небезпеки, тобто кількісна оцінка збитків, заподіяних нею, залежить від багатьох чинників — кількості людей, що знаходились у небезпечній зоні, кількості та якості матеріальних (в тому числі і природних) цінностей, що перебували там, природних ресурсів, перспективності зони тощо.

З метою уніфікації будь-які наслідки небезпеки визначають як шкоду. Кожен окремий вид шкоди має своє кількісне вираження, наприклад, кількість загиблих, поранених чи хворих, площа зараженої чи затопленої території, площа лісу, що вигоріла, вартість зруйнованих споруд тощо. Отже всі небезпеки різняться за цим показником. Найбільш універсальний кількісний спосіб визначення шкоди — це вартісний, тобто визначення шкоди ***(E)*** у грошовому еквіваленті**.**

Другою, не менш важливою характеристикою небезпеки, є частотна ймовірність прояву небезпеки ***(p)*.**

Частотна ймовірність прояву небезпеки /в подальшому просто частота прояву небезпеки/ ***(p),*** визначається як відношення кількості подій з певними наслідками ***(n)*** до максимально можливої їх кількості ***(N)*** за конкретний період часу:

$$p = n/N.$$

Комплексною оцінкою небезпеки є ризик (R), який визначається як добуток частоти прояву небезпеки на шкоду, яку вона завдає.

$$R = p \cdot E$$

Оскільки ймовірність – це величина безрозмірна, то виходить, що одиниці вимірювання ризику і потенційної шкоди повинні бути однакові. Якщо ми

говоримо про визначення шкоди ***(E)*** у грошовому еквіваленті, то це безумовно буде грошова одиниця, якщо про небезпеку іонізуючого опромінення, то ризик буде визначатися в одиницях виміру поглинутої дози, якщо про небезпеку повені, то в одиницях виміру площини залитої водою території і т.ін.

Також для кількісної оцінки небезпеки допускається можливість умовного прийняття ***E=1*** і використання так званого коефіцієнту індивідуального ризику.

Необхідно зазначити, що наведена формула дозволяє розрахувати величину як **загального**, так і **групового** та **індивідуального ризику**. При оцінці загального ризику величина ***N*** визначає максимальну кількість усіх подій, а при оцінці групового та індивідуального ризику – відповідно максимальну кількість подій у конкретній групі, що вибрана із загальної кількості за певною ознакою, або максимальну кількість подій для одного індивіда.

В групу можуть входити люди, що належать до однієї професії, віку, статі; групу можуть складати також транспортні засоби одного типу; один клас суб'єктів господарської діяльності тощо.

З метою можливості порівняння небезпек різного походження для них використовується наступна упорядкована шкала ризиків смертності (таблиця 2.1).

Таблиця 2.1. Упорядкована шкала ризиків смертності

Низький рівень ризику смертності			Середній рівень ризику смертності		Високий рівень ризику смертності			
$<1*10^{-8}$	$1*10^{-8}$	$1*10^{-7}$	$1*10^{-6}$	$1*10^{-5}$	$1*10^{-4}$	$1*10^{-3}$	$1*10^{-2}$	$>1*10^{-2}$
Знехту-ваний	Низький	Відносно низький	Середній	Відносно середній	Високий	Дуже високий	Екстремальний	

Максимально прийнятним рівнем індивідуального ризику загибелі людини, як правило, вважається ризик, який дорівнює 10^{-6} на рік. Малим вважається індивідуальний ризик загибелі людини, що дорівнює 10^{-8} на рік (див. табл. 2.4).

Нижче у таблиці 2.2 наведені значення ризику загибелі 1-ї людини впродовж року в залежності від виду професійної діяльності.

Таблиця 2.2. Класифікатор безпеки професійної діяльності

Категорія безпеки	Умови професійної діяльності	Ризик загибелі 1-ї людини на рік
1	Безпечні (працівники швейної, взуттєвої, текстильної, паперової, типографської, харчової та лісової промисловості)	<0,0001 ($R<1*10^{-4}$)
2	Відносно безпечні (працівники металургійної, суднобудівної, вуглевидобувної промисловості, чавунно-ливарного, гончарного та керамічного виробництв, працівники промисловості загалом, а також працівники цивільної авіації)	0,0001…0,0010 ($1*10^{-4}<R<1*10^{-3}$)
3	Небезпечні (зайняті у вуглекоксівному та вулканізаційному виробництві, члени екіпажів риболовецьких траулерів, будівельні робітники, верхолази, трактористи)	0,0010…0,0100 ($1*10^{-3}<R<1*10^{-2}$)
4	Особливо небезпечні (льотчики-випробувачі, члени екіпажів військових вертольотів, водолази)	>0,0100 ($R>1*10^{-2}$)

Класифікація (ідентифікація) ризиків

Враховуючі наявність в сучасній літературі достатньо значної кількості визначень та трактувань щодо ризиків і пов'язаних з ними понять, розглянемо лише основні, найбільш поширені види існуючих на даний час види класифікацій (ідентифікацій) ризиків.

За джерелом ризику:

- техногенний ризик;
- природний ризик.

За видом джерела ризику:

- внутрішній ризик, пов'язаний із функціонуванням організації;
- зовнішній ризик, пов'язаний із функціонуванням організації;
- зовнішній ризик пов'язаний із зовнішнім середовищем і не залежний від функціонування організації;
- ризик, пов'язаний з помилками людини (так званий людський фактор).

За характером нанесеного збитку:

- економічний;
- екологічний;
- соціальний.

За розміром нанесеного збитку:

- припустимий;
- граничний (критичний);
- катастрофічний.

За рівнем небезпеки:

- безумовно прийнятний;
- прийнятний;
- неприйнятний.

За часом впливу:

- короткостроковий;
- середньостроковий;
- Довгостроковий.

За частотою впливу:

- разовий;
- періодичний;
- постійний.

За рівнем впливу:

- локальний;
- глобальний.

За масштабом впливу:

- індивідуальний;
- колективний.

За сприйняттям людей:

- добровільний;
- примусовий.

Методи визначення ризику на якісному рівні

Як правило, аналіз небезпек починають з попереднього дослідження, яке дозволяє в основному ідентифікувати джерела небезпек. Потім, при необхідності, дослідження можуть бути поглиблені і може бути виконаний детальний якісний аналіз. Методи цих аналізів та прийоми, які використовуються при їх виконанні, відомі під різними назвами. Нижче наведені основні з цих загальних інструментів.

Методи аналізу:

- попередній аналіз небезпек (ПАН)
- системний аналіз небезпек (САН)
- підсистемний аналіз небезпек (ПСАН)
- аналіз небезпеки робіт та обслуговування (АНРО).

Методи та прийоми, що використовуються при аналізах:

- аналіз пошкоджень та викликаного ними ефекту (АПВЕ)
- аналіз дерева відмов (АДВ)
- аналіз ризику помилок (АРП)
- прорахунки менеджменту та дерево ризику (ПМДР)
- аналіз потоків та перешкод енергії (АППЕ)
- аналіз поетапного наближення (АПН)
- програмний аналіз небезпек (ПрАН)
- аналіз загальних причин поломки (АЗПП)
- причинно-наслідковий аналіз (ПНА)
- аналіз дерева подій (АДП).

Ознайомимось з основами двох з наведених вище методик, а саме: з попереднім аналізом небезпек (ПАН) та аналізом дерева відмов (АДВ).

Попередній аналіз небезпек — це аналіз загальних груп небезпек, присутніх в системі, їх розвитку та рекомендації щодо контролю. ПАН є першою спробою в процесі безпеки систем визначити та класифікувати небезпеки, які мають місце в системі.

Як правило, ПАН виконується у наступному порядку:

- вивчають технічні характеристики об'єкта, системи чи процесу, а також джерела енергії, що використовуються, робоче середовище, матеріали, встановлюють їхні небезпечні та шкідливі властивості;

- визначають закони, стандарти, правила, дія яких поширюється на даний об'єкт, систему чи процес;

- перевіряють технічну документацію на відповідність її законам, правилам, принципам і нормам безпеки;

- складають перелік небезпек, в якому зазначають ідентифіковані джерела небезпек (системи, підсистеми, компоненти), чинники, що викликають шкоду, потенційні небезпечні ситуації, виявлені недоліки.

При проведенні ПАН особливу увагу приділяють наявності вибухо- та пожежонебезпечних і токсичних речовин.

Після того, як виявлені крупні системи об'єкта, які є джерелами небезпеки, їх можна розглядати окремо і досліджувати більш детально за допомогою інших методів аналізу, перелік яких було наведено вище.

Існують базові запитання, на які обов'язково необхідно відповісти, коли проводять ПАН, незважаючи на те що деякі з них можуть здаватися занадто простими. Якщо ці запитання не розглянути, то існує ризик неповного аналізу безпеки системи. Вся простота чи очевидність має схильність приховувати деякий рівень прихованої небезпеки. Базові запитання, які мають бути вирішені в першу чергу, це наступні:

- який процес/система аналізуються?
- чи залучені до цієї системи люди?
- що система повинна зазвичай робити?
- чого система не повинна робити ніколи?
- чи існують стандарти, правила, норми, які мають відношення до системи?
- чи використовувалась система раніше?
- що система виробляє?
- які елементи включено в систему?
- які елементи вилучено із системи?
- що може спричинити появу небезпеки?
- як оцінюється ця поява?
- що і де є джерелами та перешкодами енергії?
- чи існує критичний час для безпечності операцій?
- які загальні небезпеки притаманні системі?
- як може бути покращений контроль?
- чи сприйме керівництво цей контроль?

Аналіз дерева відмов (АДВ) вважається одним з найбільш корисних аналітичних інструментів в сфері системної безпеки, особливо при проведені оцінки складних систем. Дедуктивно-логічний метод (тобто поступовий рух від загального до часткового), який при цьому використовується, є особливо корисним при дослідженні можливих умов, які можуть призвести до небажаних наслідків або яким-небудь чином вплинути на ці наслідки. Небажані події рідко відбуваються під впливом тільки одного чинника. Через це при побудові дерева відмов небажану подію відносять до кінцевої події і починають ідентифікувати ті окремі події, які сприяли виникненню кінцевої події. Розташовуючи кожний фактор у відповідному місці дерева, дослідник може точно визначити, де відбулись ті чи інші пошкодження в системі, який зв'язок існує між ними і яки події відбулись, або не відбулись, або можуть відбутись.

Якісна оцінка ризику небезпеки

Одразу визначимо термін «**оцінка**». **Оцінка** має на меті одержання інформації, що є основою для ухвалення рішення у відношенні того, наскільки задовільним є те, що розглядається. При цьому, як інструменти можуть бути використанні різні види аналізу. Отже, оцінка може включати цілий ряд аналізів і вона є підсумковим результатом дослідження.

Якщо поширити вимоги стандарту ГОСТ 27.310-95 «Надійність в техніці. Аналіз видів, наслідків та критичності відмов» на сферу безпеки життєдіяльності, то при відповідних допущеннях, серйозність /тяжкість/ ймовірних наслідків небезпечних умов можна умовно класифікувати за чотирма видами або чотирма

категоріями (I – незначна; II – гранична; III – критична; IV – катастрофічна), що представлені у таблиці 2.3. Існуючі види та категорії серйозності небезпеки встановлюють кількісне значення відносної серйозності ймовірних наслідків небезпечних умов в залежності від характеру наслідків цієї небезпеки. Їх використання є ефективним інструментом для визначення необхідних заходів та засобів щодо забезпечення необхідного рівня безпеки життєдіяльності. Безумовно, що ситуації, які належать до категорії IV (катастрофічні небезпеки), потребують більшої уваги, ніж віднесені до категорій I - III.

Таблиця 2.3. Вид та категорія серйозності небезпеки

Вид	**Категорія**	**Опис нещасного випадку**
Незначна	I	Небезпека, при реалізації якої настають менш значні, ніж у категорії II, травми, захворювання
Гранична	II	Небезпека, реалізація якої може спричинити затримку виконання завдання підприємством, привести до зниження працездатності людей, а при тривалому впливі - до захворювань
Критична	III	Небезпека, реалізація якої може швидко та з високою ймовірністю спричинити значний збиток для підприємства та/або навколишнього середовища і важкі травми та стійкі захворювання людей
Катастрофічна	IV	Небезпека, реалізація якої може швидко та з високою ймовірністю спричинити значний збиток для підприємства та/або навколишнього середовища, а також загибель людей

Можливі види та рівні ймовірності небезпеки, що представлені у наступній таблиці (табл. 2.4), є якісним відображенням відносної ймовірності того, що відбудеться небажана подія, яка є наслідком не усунутої або непідконтрольної небезпеки.

Використовуючи відповідні методики щодо визначення існуючих видів, категорій серйозності та рівнів ймовірності небезпеки, можна оцінити потенційні ризики з урахуванням серйозності цієї небезпеки, її потенційно ймовірних наслідків та ймовірності того, що такі наслідки будуть мати місце.

Таблиця 2.4. Вид та рівень ймовірності небезпеки

Вид (по частоті виникнення)	Рівень	Опис наслідків
Часта	A	Небезпека спостерігається постійно
Ймовірна	B	Ймовірно часте виникнення небезпеки, може трапитися кілька разів за життєвий цикл
Можлива	C	Небезпека спостерігається кілька разів за період роботи
Рідка	D	Малоймовірно, але можливе виникнення небезпеки хоча б раз впродовж життєвого циклу системи
Практично неймовірна	E	Виникнення небезпеки настільки малоймовірне, що можна припустити, що вона ніколи не відбудеться

Якщо порівняти таблиці 2.3 та 2.4, то легко помітити, що навіть серйозна небезпека може бути припустимою у разі, якщо буде доведено, що її ймовірність занадто низька. Так само може бути припустимою і дуже ймовірна подія, якщо буде доведено, що наслідки її менш ніж незначні. Таким чином, можна допустити, що ймовірність припустимого ризику повинна бути зворотно пропорційною його серйозності і, навпаки – серйозність припустимого ризику повинна бути зворотно пропорційною його ймовірності. Табл. 2.5 демонструє приклад матриці ризиків небезпеки, що включає у себе як елементи таблиці 2.3, так і елементи таблиці 2.4, що дає змогу забезпечити новий ефективний інструмент для оцінки припустимого та неприпустимого рівнів або ступенів ризику.

Таблиця 2.5. Матриця оцінки ризику

Частота, з якою відбувається подія (небезпека)	Категорія небезпеки			
	IV Катастрофічна	III Критична	II Гранична	I Незначна
(A) Часто	4A	3A	2A	1A
(B) Імовірно	4B	3B	2B	1B
(C) Можливо	4C	3C	2C	1C
(D) Рідко	4D	3D	2D	1D
(E) Практично неможливо	4E	3E	2E	1E
Індекс ризику небезпеки				
Класифікація ризику 4A,4B,4C,3A,3B,2A 4D,3C,3D,2B,2C 4E,3E,2D,2E,1A,1B 1C,1D,1E	Критерії ризику Неприпустимий (надмірний) Небажаний (гранично допустимий) Припустимий з перевіркою (прийнятний) Припустимий без перевірки (знехтуваний)			

Завдяки застосованій цифро-буквеній системі класифікації ризиків для кожної з категорій серйозності та кожного рівня ймовірності, стає можливим оцінювати ризик за ступенем припустимості (індексом ризику). Безумовно, що використання такої матриці значно спрощує оцінку ризику.

Концепція прийнятного (припустимого) ризику

Як було показано в таблиці 2.5, за ступенем припустимості ризик може бути знехтуваний, прийнятний, гранично допустимий та надмірний.

Знехтуваний ризик має настільки малий рівень, що він перебуває в межах допустимих відхилень природного (фонового) рівня.

Прийнятним вважається такий рівень ризику, який суспільство може прийняти (дозволити), враховуючи техніко-економічні та соціальні можливості на даному етапі свого розвитку.

Гранично допустимий ризик — це максимальний ризик, який не повинен перевищуватись, незважаючи на очікуваний результат.

Надмірний ризик характеризується виключно високим рівнем, який у переважній більшості випадків призводить до негативних наслідків.

На практиці досягти нульового рівня ризику, тобто абсолютної безпеки, неможливо. Через це вимога щодо забезпечення абсолютної безпеки, яка приваблює більшість людей своєю гуманністю, може обернутися для останніх значною трагедією. Знехтуваний ризик на даний час також майже неможливо забезпечити з огляду на відсутність необхідних технічних та економічних передумов для цього. Саме тому сучасна концепція безпеки життєдіяльності базується на досягненні саме прийнятного (припустимого) ризику.

Сутність концепції прийнятного (припустимого) ризику полягає у прагненні суспільства забезпечити такий рівень безпеки, який воно здатне сприймати на даний час, виходячи з існуючого рівня життя, соціально-політичного та економічного становища, розвитку науки та техніки.

Рівень прийнятного (припустимого) ризику визначається сукупністю технічних, економічних, соціальних та політичних аспектів та проблем і є певним компромісом між бажаним рівнем безпеки й можливостями щодо його досягнення.

Розподіл витрат суспільства на досягнення заданого рівня безпеки у природній, техногенній та соціальній сферах необхідно здійснювати лише при оптимальному співвідношенні витрат у зазначених сферах, оскільки порушення балансу на користь однієї з них може спричинити різке збільшення ризику і його рівень вийде за межі прийнятних значень.

Як приклад, на рис. 2.1 наведено алгоритм оптимізації витрат на забезпечення мінімально можливого в умовах обмеженості коштів рівня прийнятного ризику.

Як бачимо, сумарний ризик має мінімум лише при певному співвідношенні інвестицій у технічну та соціальну сфери і це обов'язково потрібно враховувати при виборі рівня прийнятного (припустимого) ризику.

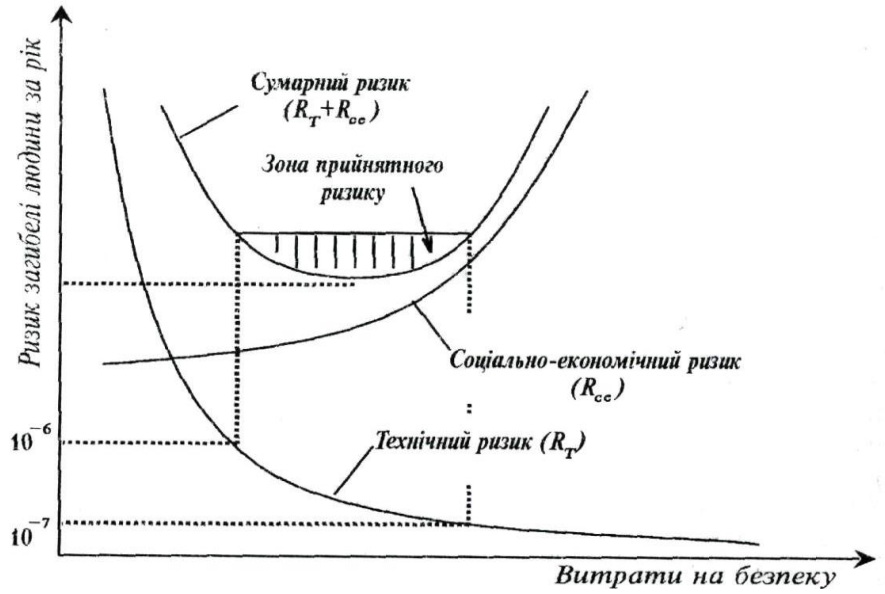

Рис. 2.1. Визначення прийнятного (припустимого) ризику

Концепція прийнятного (припустимого) ризику може бути ефективно застосована у будь-якій сфері діяльності та галузі виробництва.

Принцип АЛАРА, можливості управління ризиком

У світовій практиці при управлінні ризиком прийнято користуватися принципом АЛАРА (ALARA – as low as reasonably achievable (так низько, як це розумно).

«Будь-який ризик повинен бути знижений настільки, наскільки це є практично досяжним або ж до рівня, який є настільки низьким, наскільки це розумно досяжне».

Як вже було сказано раніше, основним питанням теорії і практики безпеки життєдіяльності, безумовно, є питання підвищення рівня безпеки. Таким чином, порядок пріоритетів при розробці будь-якого проекту вимагає, щоб вже на перших стадіях розробки будь-якого продукту чи системи у відповідний проект були обов'язково включені елементи, що виключають можливість виникнення небезпек. На жаль, це не завжди може бути реалізовано.

У разі, якщо виявлені небезпеки неможливо виключити повністю, то тоді необхідно знизити ймовірність їх ризиків до припустимих рівнів шляхом вибору відповідних рішень. Досягти цієї мети в будь-якій системі чи ситуації, як правило, можна кількома шляхами. Наприклад, це може бути:

- повна або часткова відмова від робіт, операцій та систем, які мають високий рівень небезпеки;
- заміна небезпечних операцій іншими – менш небезпечними;
- удосконалення технічних систем та об'єктів;
- розробка та використання спеціальних засобів захисту;
- заходи організаційно-управлінського характеру, в тому числі контроль за рівнем безпеки, навчання людей з питань безпеки, стимулювання безпечної роботи та поведінки.

Кожен із зазначених напрямів має свої переваги і недоліки, і тому часто заздалегідь важко сказати, який з них є кращим. Як правило, для підвищення рівня безпеки завжди використовується комплекс заходів та засобів.

Для того щоб надати перевагу конкретним заходам та засобам або певному їх комплексу, порівнюють витрати на ці заходи та засоби і рівень зменшення шкоди, який очікується в результаті їх запровадження.

Такий підхід до зменшення ризику небезпеки зветься управління ризиком.

Ризик орієнтований підхід в сфері безпеки

Процес формування сучасного фахівця практично будь-якої галузі вимагає глибоких знань сучасного інструментарію управління безпекою і, в першу чергу, методології аналізу ризику системи «людина – життєве середовище».

Людське суспільство наполегливо веде розробку нових методів аналізу і управління ризиком як техногенних, так і соціально-екологічних систем. Необхідність застосування ризик орієнтованого підходу (РОП) в питаннях безпеки розуміють вчені, інженери та фахівці різних галузей знань, виробництва, сфер діяльності.

Основними складовими ризик орієнтованого підходу в питаннях управління безпекою є процес порівняння існуючого ризику з припустимим (прийнятним), а також зроблені на підставі цього відповідні висновки та прийняті до виконання

рішення. В якості основної методології РОП використовується відповідний аналіз безпеки та можливих витрат і збитків.

Існує два шляхи встановлення гранично припустимого (прийнятного) ризику – це декларативний та обґрунтований. У разі декларативного підходу, значення припустимого (прийнятного) ризику встановлюється відповідно до нормативно-правових актів – законів, стандартів, правил, норм, якими визначені гранично допустимі (максимальні чи мінімальні) параметри певних шкідливих та небезпечних чинників. У разі обґрунтованого підходу, значення припустимого (прийнятного) ризику визначається шляхом порівняння окремих видів ризику з рівнями існуючих природних ризиків. Кінцеве значення оптимального гранично припустимого (прийнятного) ризику, як правило, корегується в процесі аналізу тих витрат, які необхідно нести для підтримання зазначеного рівня безпеки, а також в процесі порівняння цих витрат із можливими збитками із-за існуючих ризиків.

Найбільш детально та ґрунтовно проблеми ризику небезпек і існуючого людського чинника вирішуються в галузях з високою ціною помилки в разі надзвичайної ситуації, що, в першу чергу, характерно для енергетичної галузі і, особливо, для атомної енергетики, а також для авіації, космонавтики тощо. Ключовим моментом впровадження РОП в Україні стало прийняття в листопаді 2001 р. рішення колегії Держкоматомрегулювання України про планомірне впровадження РОП в практику експлуатації АЕС і регулюючу діяльність. На підставі цього рішення в 2002 р. була розроблена Програма впровадження ризик орієнтованих підходів, а у 2005 р. Державний комітет ядерного регулювання України підтвердив прихильність принципам РОП і визначив пріоритетним напрямом своєї діяльності виконання цієї програми.

Хоча в широку практику принципи РОП ще і не увійшли, але вони одержали відповідне визнання в усіх розвинених країнах при вирішенні проблем безпеки в суспільстві. В подальшому передбачається широке впровадження цієї теорії у різних сферах громадського життя, в тому числі і для оцінки шкоди від засух, повеней, ураганів, підтоплень, епідемій та інших небезпек.

Забезпечення безпеки шляхом використання ризик орієнтованого підходу передбачає превентивне втручання з урахуванням існуючих рівнів розвитку науки та технологій. Ризик орієнтований підхід в наш час – це основа організації безпеки складних технічних систем та систем їх управління і контролю, а також систем запобігання виникнення надзвичайних ситуацій тощо.

Особливості існуючої термінології для сфери охорони праці (ДСТУ OHSAS 18001:2010 «СИСТЕМИ УПРАВЛІННЯ ГІГІЄНОЮ ТА БЕЗПЕКОЮ ПРАЦІ. Вимоги»)

Небезпека

Потенційна дія небезпечних і шкідливих чинників на здоров'я та/чи життя людини

Небезпечний чинник; джерело небезпеки

Об'єкт підприємства, елемент його діяльності чи виробниче середовище, порядок і умови виконання робіт на підприємстві, що можуть завдати шкоди життю, здоров'ю чи майну людини, її правам і інтересам

Ідентифікація небезпеки

Процес розпізнавання наявності небезпеки та визначення її характеристик (ДСТУ OHSAS 18001:2010, 3.7)

Ризик

Поєднання ймовірності виникнення небезпечної події чи впливу(-ів) та істотності травми чи погіршення здоров'я, які може бути зумовлено такою подією чи впливом(-ами)

(ДСТУ OHSAS 18001:2010, 3.21)

Оцінювання ризику

Процес оцінювання ризику, що виникає від небезпеки, з урахуванням адекватності наявних заходів безпеки та прийняття рішення стосовно прийнятності чи неприйнятності ризику

(адаптовано з ДСТУ OHSAS 18001:2010, 3.22)

Прийнятний ризик

Ризик настільки низького рівня, що його може допустити підприємство, враховуючи свої правові зобов'язання, власну політику у сфері охорони праці та фінансові можливості

(адаптовано з ДСТУ OHSAS 18001:2010, 3.1)

Автор: доцент кафедри ОПЦБ ІЕЕ НТУУ «КПІ ім. Ігоря Сікорського»