Міністерство освіти і науки України
Національний університет водного господарства
та природокористування
Кафедра охорони праці та безпеки життєдіяльності

03-10-08

МЕТОДИЧНІ ВКАЗІВКИ

до виконання практичних занять
та самостійного вивчення навчальної дисципліни
«Ризики та моделювання в охороні праці»
для здобувачів вищої освіти другого (магістерського)
рівня за освітньо-професійною програмою
«Охорона праці» спеціальності № 263 «Цивільна безпека»
денної та заочної форм навчання

Рекомендовано науково-
методичною радою з
якості ННІБА
Протокол № 4
від 31.03.2020 р.

Рівне – 2020

Методичні вказівки до виконання практичних занять та самостійного вивчення навчальної дисципліни «Ризики та моделювання в охороні праці» для здобувачів вищої освіти другого (магістерського) рівня за освітньо-професійною програмою «Охорона праці» спеціальності № 263 «Цивільна безпека» денної та заочної форм навчання [Електронне видання] / Довбенко В. С. – Рівне : НУВГП, 2020. − 27 с.

Укладач: Довбенко В. С., кандидат технічних наук, додент, доцент кафедри охорони праці та безпеки життєдіяльності.

Відповідальний за випуск: Филипчук В. Л., доктор технічних наук, професор, завідувач кафедри охорони праці та безпеки життєдіяльності.

Керівник групи забезпечення
спеціальності Филипчук В. Л.

ЗМІСТ

ВСТУП

Методичні вказівки розроблено для вивчення навчальної дисципліни «Ризики та моделювання в охороні праці» здобувачами вищої освіти другого (магістерського) рівня за освітньо-професійною програмою «Охорона праці» спеціальності 263 «Цивільна безпека».

Предметом вивчення навчальної дисципліни «Ризики та моделювання в охороні праці» є формування теоретичних знань та практичних навичок щодо керування ризиком, індетифікацію небезпек та оцінкою процесів і явищ, які пов'язані діяльністю, функцією чи продукцією.

Вивченню навчальної дисципліни «Ризики та моделювання в охороні праці» передує отримання компетентностей з таких дисциплін як «Розслідування нещасних випадків на виробництві та професійних захворювань», «Виробнича санітарія та фізіологія праці», «Профілактика виробничого травматизму і професійних захворювань», «Організація служби охорони праці», «Державне соціальне страхування на виробництві» та інші.

Ключові слова: ризик, керування ризиком, ідентифікування ризику, моделювання, подія, небезпечний чинник, імовірність, наслідок

Практичне заняття № 1
ВИБІР МЕТОДІВ ЗАГАЛЬНОГО ОЦІНЮВАННЯ РИЗИКУ

Мета роботи: Ознайомитися із концепцією оцінки ризику та навчитися вибирати методи загального оцінювання ризику.

Загальне оцінювання ризику можна провадити зі зміненням глибини, детальності процесів і явищ, а також з використанням одного чи кількох методів - від найпростіших до найскладніших. Треба, щоб форма загального оцінювання ризику та його результат було узгоджено з критеріями ризику, розробленими під час оцінки. У табл. 1 показано концептуальний взаємозв'язок між основними категоріями методик загального оцінювання ризику та чинниками, пов'язаними з конкретною ситуацією ризику, а також наведено наочні приклади того, як організації можуть вибирати відповідні методи загального оцінювання ризику стосовно конкретної ситуації.

Взагальному необхідно щоб обраний метод відповідав таким критеріям:

- був обґрунтованим і доречним для розгляданих ситуації чи організації;
- міг забезпечувати отримання результатів у формі, яка дозволяє краще розуміння характер ризику та способи його оцінки;
- був таким, щоб його можна було простежити, відтворити чи перевірити.

Обґрунтовуючи вибір методів, треба враховувати їхню відповідність і придатність. У разі поєднання результатів різних досліджень треба, щоб застосовувані методи та отримані вихідні дані можна було порівняти.

Таблиця 1

Застосування методів аналізу для загального оцінювання ризику

Методи та засоби аналізу	Процес загального оцінювання ризику				
	Ідентифікація ризику	Наслідок	Імовірність	Рівень ризику	Оцінка ризику
1	2	3	4	5	6
«Мозкова атака»	ЗЗ[1)]	НЗ[2)]	НЗ	НЗ	НЗ
Структуроване чи напівструктуроване Опитування	ЗЗ	НЗ	НЗ	НЗ	НЗ
Метод Дельфі	ЗЗ	НЗ	НЗ	НЗ	НЗ
Переліки контрольних запитань	ЗЗ	НЗ	НЗ	НЗ	НЗ
Попередній аналіз небезпечних чинників (PHA)	ЗЗ	НЗ	НЗ	НЗ	НЗ
Дослідження небезпечних чинників і працездатності (HAZOP)	ЗЗ	ЗЗ	З[3)]	З	З
Аналіз небезпечних чинників і критичні точки контролю (HACCP)	ЗЗ	ЗЗ	НЗ	НЗ	НЗ
Загальне оцінювання екологічного ризику	ЗЗ	ЗЗ	ЗЗ	ЗЗ	ЗЗ
Структурований метод «що — якщо» (SWIFT)	ЗЗ	ЗЗ	ЗЗ	ЗЗ	ЗЗ
Аналіз сценаріїв	ЗЗ	ЗЗ	З	З	З
Аналіз впливу на діяльність	З	ЗЗ	З	З	З
Аналіз першопричини	НЗ	ЗЗ	ЗЗ	ЗЗ	ЗЗ
Аналіз видів і наслідків відмов	ЗЗ	ЗЗ	ЗЗ	ЗЗ	ЗЗ
Аналіз дерева відмов	З	НЗ	ЗЗ	З	З
Аналіз дерева подій	З	ЗЗ	З	З	НЗ
Аналіз причин і наслідків	З	ЗЗ	ЗЗ	З	З

1	2	3	4	5	6
Аналіз причинно-наслідкових зв'язків	ЗЗ	ЗЗ	НЗ	НЗ	НЗ
Аналіз рівнів захисту (LOPA)	З	ЗЗ	З	З	НЗ
Дерево рішень	НЗ	ЗЗ	ЗЗ	З	З
Загальне оцінювання надійності людини	ЗЗ	ЗЗ	ЗЗ	ЗЗ	З
Аналіз за схемою «краватка метелик»	НЗ	З	ЗЗ	ЗЗ	З
Технічне обслуговування, зорієнтоване на забезпечення безвідмовності	ЗЗ	ЗЗ	ЗЗ	ЗЗ	ЗЗ
Аналіз паразитних схем	З	НЗ	НЗ	НЗ	НЗ
Марковський аналіз	З	ЗЗ	НЗ	НЗ	НЗ
Імітаційне моделювання за методом Монте-Карло	НЗ	НЗ	НЗ	НЗ	ЗЗ
Байєсова статистика і мережі Байєса	НЗ	ЗЗ	НЗ	НЗ	ЗЗ
Криві FN	З	ЗЗ	ЗЗ	З	ЗЗ
Показники ризику	З	ЗЗ	ЗЗ	З	ЗЗ
Матриця «наслідок-імовірність»	ЗЗ	ЗЗ	ЗЗ	ЗЗ	З
Аналіз витрат і вигод	З	ЗЗ	З	З	З
Багатокритерійний аналіз рішень (MCPA)	З	ЗЗ	З	ЗЗ	З

[1)] Завжди застосовується
[2)] Незастосовується
[3)] Застосовується

Після того, як прийнято рішення про провадження загального оцінювання ризику і визначено цілі та сферу застосування, необхідно вибирати методи, зважаючи на такі чинники:

- цілі дослідження (цілі загального оцінювання ризику безпосередньо позначатимуться на виборі застосовуваних методів. Наприклад, якщо провадять порівняльне

дослідження різних варіантів, то прийнятним може бути використання менш докладних моделей наслідків для частин системи, на які не впливають відмінності);

- потреби осіб, хто приймає рішення (у деяких випадках потрібен високий рівень докладності для прийняття оптимального рішення, в інших випадках достатнім є загальне розуміння);

- тип і діапазон проаналізованих ризиків;

- потенційна величина наслідків - рішення щодо глибини загального оцінювання ризику має відображати первісне сприйняття наслідків (хоча може виявитися необхідним змінити його після завершення попереднього оцінювання);

- ступінь фахової компетентності, потреба в людських та інших ресурсах (простий, належно запроваджений метод, якщо він задовольняє цілі та сферу застосування загального оцінювання, може давати кращі результати, ніж складніша, але недостатньо опрацьована процедура. Зазвичай треба, щоб витрати на загальне оцінювання були сумірними з потенційним рівнем аналізованого ризику);

- наявність інформації та даних (для деяких методів потрібно більше інформації та даних, ніж для інших);

- потреба модифікувати чи актуалізувати загальне оцінювання ризику (надалі загальне оцінювання може бути потрібно модифікувати чи актуалізувати і у зв'язку з цим деякі методи більш придатні до вдосконалення ніж інші);

- будь-які регуляторні чи контрактні вимоги.

На вибирання підходу до загального оцінювання ризику впливають різномантні чинники, наприклад, наявність ресурсів, характер і ступінь невизначеності наявних даних та інформації, складність випадку застосування.

Ресурси та можливості, які можуть впливати на вибір методів загального оцінювання ризику охоплюють:

- компетентність, досвід, здібності та можливості групи загального оцінювання ризику;
- обмеження щодо часу та інших ресурсів організації;
- наявний бюджет у разі, якщо будуть потрібні зовнішні ресурси.

Методи загального оцінювання ризику можна класифікувати різними способами, щоб полегшити розуміння їхніх відносно сильних і слабких аспектів.

Література [1, 2, 6].

Практичне заняття № 2
ВИЗНАЧЕННЯ МЕТОДУ ІДЕНТИФІКАЦІЇ ХАРАКТЕРУ ВІДМОВ І ЧИННИКІВ (FMEA) ТА (FMECA)

Мета роботи: Навчитися працювати із методом аналіз видів і наслідків відмов (FMEA) та аналіз видів, наслідків і критичності відмов (FMECA).

Аналіз видів і наслідків відмов (FMEA) – це метод, що використовується для визначення елементів системи чи процесів, які можуть ставати непридатними до функціювання за проектною призначеністю.

FMEA дає змогу ідентифікувати:
- усі потенційні види відмов різних частин системи (вид відмови визначають, беручи до уваги спостережувані збої чи неналежне функціювання);
- впливи відмови, які можуть викликати несправність систем;
- чинники виникнення відмов;
- способи уникнення відмов і/або зменшування їхніх впливів на систему.

FMECA розширює FMEA, охоплюючи ранжування кожного ідентифікованого виду відмови відповідно до його важливості чи критичності. Аналіз критичності, зазвичай, якісна чи напівкількісна оцінка, але також дозволяє кількісне подання результату за умови використання даних щодо фактичної інтенсивності відмови.

Існує кілька сфер застосування FMEA:

- FMEA проекту (чи продукції), яке застосовують стосовно складників і продукції;
- FMEA системи, яке застосовують стосовно систем; FMEA процесу, яке застосовують стосовно виробничих і складальних процесів;
- FMEA послуги і FMEA програмного забезпечення.

FMEA і FMECA можна застосовувати під час проектування, вироблення чи функціювання технічної системи.

FMEA і FMECA можна також застосовувати до процесів і процедур, для підвищення надійності, проте, зміни легше вносити на стадії проектування. Наприклад, їх використовують, щоб ідентифікувати потенційну можливість медичної помилки в системах охорони здоров'я та відмов у процедурах технічного обслуговування.

FMEA і FMECA можна використовувати для:

- сприяння вибору альтернативних проектних рішень з високою надійністю;
- забезпечення розгляду всіх видів відмови систем і процесів, а також їхніх впливів на успішне функціювання;
- ідентифікація видів і наслідків помилок людини;
- забезпечення основи для планування випробування й технічного обслуговування технічних систем;
- поліпшення проектування процедур і процесів;

- отримання якісної та кількісної інформації для методів аналізу, наприклад, аналіз дерева відмов.

За допомогою FMEA і FMECA можна отримати вхідні дані для інших методів аналізу, наприклад, аналіз дерева відмов як на якісному, так і на кількісному рівні.

Для FMEA і FMECA потрібна досить докладна інформація про елементи системи, щоб дозволити змістовний аналіз способів, де кожний елемент може виходити з ладу. У разі докладного FMEA проекту елемент може перебувати на рівні докладності, що відповідає окремими складовим, тоді як у разі FMEA системи вищого рівня елементи можуть бути визначені на більш високому рівні узагальнення.

Інформація може охоплювати:

- кресленики чи блок-схему аналізованої системи та її складників або етапи функціювання процесу;
- основні відомості про функціювання кожного етапу процесу чи елемента системи;
- детальні відомості про параметри середовища та інші параметри, які можуть позначатися на функціюванні;
- основні відомості про результати конкретних відмов;
- хронологічні дані про відмови, зокрема дані щодо інтенсивності відмов, якщо вони наявні.

Процес FMEA полягає у:

1) визначенні сфери застосування та цілей дослідження;
2) формуванні групу;
3) з’ясуванні основних відомостей про систему чи процес, що досліджуватимуться FMECA;
4) розкладанні систем на елементи чи етапи функціювання;
5) визначенні функцій на кожному етапі чи кожному елементі;
6) визначенні відмов для кожного вибраного елементу чи етапу (як кожна частина може ймовірно вийти з ладу?; які чинники можуть зумовити ці види відмови?; якими можуть

бути наслідки в разі виникнення відмови?; чи є відмова нешкідливою чи руйнівною?; як виявляють відмову?)
7) ідентифікації потрібних для проекту заходів, щоб скомпенсувати відмову.

У разі FMECA дослідницька група має класифікувати кожний з ідентифікованих видів відмови відповідно до його критичності, це може бути здійснено кількома способами. Загальноприйняті методи враховують таке:
- показник критичності виду;
- рівень ризику;
- число пріоритетності ризику.

Критичність виду відмови - це міра імовірності того, що розглянутий вид зумовить відмову системи загалом; Визначають за формулою:

(Імовірність наслідку відмови) × (Інтенсивність виду відмови) × (Тривалість функціювання системи).

Дану модель найчастіше застосовують до відмов устаткування щодо яких кожний з цих елементів може бути визначено кількісно, і для всіх видів відмови буде такий самий наслідок.

Рівень ризику одержують, поєднуючи наслідки виду відмови та імовірність відмови. Його використовують, коли наслідки різних видів відмови різняться один від одного, а також може бути застосовано до пов'язаних з устаткованням систем або процесів. Рівень ризику може бути подано якісно, напівкількісно чи кількісно.

Число пріоритетності ризику (RPN) - це напівкількісна міра критичності, яку одержують множенням чисел ранжувальних шкал (зазвичай від 1 до 10), що відповідають наслідку відмови, на правдоподібність відмови і спроможність виявити проблему. (Якщо відмову важко виявити, то їй надають найвищий пріоритет). Цей метод використовують найчастіше в діяльності щодо забезпечення якості.

Після того як ідентифіковано види відмов і чинники їх виникнення, може бути визначено та виконано коригувальні дії щодо значних видів відмов.

FMEA наводять у звіті, який повинен містити:

- докладні відомості про систему, яку аналізували;
- спосіб, у який проведено аналіз системи;
- припущення, зроблені під час аналізу;
- джерела даних;
- результати, зокрема заповнені робочі аркуші;
- критичність (якщо розглядали) і методологію, використану для її визначення;
- будь-які рекомендації щодо подальшого поглибленого аналізу, змін у проекті чи функцій, які треба долучити до планів випробування тощо. Після виконання передбачених дій можна провести повторне загальне оцінювання системи, здійснивши ще один цикл FMEA.

Основні вихідні дані FMEA - це перелік видів відмов, чинників виникнення відмов і наслідків для кожного елементу чи етапу функціювання системи або процесу (до якого може бути внесено інформацію про правдоподібність відмови). Також подають інформацію про причини відмови та про її наслідки для системи загалом. Вихідні дані FMECA охоплюють оцінку важливості, яка базується на правдоподібності відмови системи, рівні ризику, що зумовлений видом відмови або комбінацією рівнів ризику та «можливості виявлення» виду відмови. Якщо використано придатні дані щодо інтенсивності відмови та кількісно поданих наслідків, FMECA дає змогу одержати кількісні вихідні дані.

Переваги FMEA/FMECA:

- широка придатність до видів відмов, пов’язаних з людиною, устаткованням та системами, а також до технічних засобів, програмних засобів і процедур;

- змога ідентифікувати види відмов елементів, їхні причини та наслідки для системи, а також подавати їх у зручному для сприйняття форматі;
- можливість уникати затратних змін експлуатованого устаткування завдяки ідентифікуванню проблем на ранній стадії у процесі проектування;
- змога ідентифікувати види локалізованої відмови та вимоги щодо систем з резервуванням або систем забезпечення;
- подання вхідних даних для розробляння програм моніторингу із зазначанням ключових функцій, що підлягають моніторингу.

Обмеження:
- можливість використання лише для ідентифікування окремих видів відмов, а не комбінацій видів відмов;
- дослідження можуть бути довгими за часом та витратами, якщо їх належно не контролювати та не спрямовувати, то можна отримати значну похибку.

Література [2, 3, 8].

Практичне заняття № 3
ДОСЛІДЖЕННЯ НЕБЕЗПЕЧНИХ ЧИННИКІВ І ПРАЦЕЗДАТНОСТІ (HAZOR)

Мета роботи: Ознайомитися із методом дослідження небезпечних чинників і працездатності (HAZard and OPerability study).

HAZOP – це акронім словосполучення «Дослідження небезпечних чинників і працездатності» (HAZard and OPerability study). Даний метод структурованого та систематизованого дослідження планованих або наявних продукції, процесів, процедур чи систем. Він дає змогу ідентифікувати ризики для персоналу, устаткування, довкілля та/або цілей організації, підприємства чи

установи. Від дослідницької групи очікують також вироблення, в усіх можливих випадках, рішення щодо обробляння конкретного ризику.

HAZOP – якісний метод, який базується на використанні керувальних слів, за допомогою яких формулюють питання, щоб визначити, якою мірою завдання на проектування чи умови функціювання можуть бути не досягнуті на кожному етапі проекту, процесу чи системи. Зазвичай дослідження здійснює багатодисциплінарна група під час кількох засідань.

Метод HAZOP подібний до методу FMEA в тому, що він дає змогу ідентифікувати види відмов процесу, системи чи процедури, їхні причини та наслідки. Відмінність полягає в тому, що група розглядає небажані результати та відхилення від передбачуваних результатів і станів, а потім діє у зворотному порядку, розглядаючи можливі причини та види відмов, тоді як FMEA починається з ідентифікування видів відмов.

Метод HAZOP було спочатку розроблено для аналізу систем хімічного виробництва, але потім його поширили на інші типи систем і складних процесів. До них належать, зокрема, механічні й електронні системи, процеси, системи програмного забезпечення, навіть, було застосовано до організаційних змін і юридичного опрацювання та критичного аналізу контрактів.

Процес HAZOP може стосуватися всіх видів відхилень від проектного задуму внаслідок недосконалості проекту, елементів, запланованих процесів і дій персоналу. Його широко використовують у межах критичного аналізу проекту програмного забезпечення. У разі застосування до контролю критичних для безпеки засобів і до комп’ютерних систем, він може бути відомий як CHAZOP (Control HAZards and OPerability Analysis — аналіз небезпечних чинників працездатності засобів керування чи

Computer HAZard and OPerability Analysis — аналіз небезпечних чинників і працездатності комп'ютерних систем).

Дослідження HAZOP зазвичай провадять на стадії докладного проектування, коли є повна схема передбачуваного процесу, але ще може бути внесено зміни до проекту. Однак, його можна провадитив в межах послідовного підходу із застосуванням керувальних слів на кожній стадії докладного проектування. Дослідження HAZOP можна також застосовувати на стадії функціювання, але на цій стадії внесення необхідних змін може бути пов'язане зі значними витратами.

Визначальні вхідні дані для дослідження HAZOP – це поточна інформація про систему, процес або явище, які підлягають критичному аналізу, а також цілям проекту та технічних характеристик об'єкта, що проектується. Вхідні дані можуть охоплювати: креслення, документи технічних вимог, технологічні карти, логічні діаграми та блок-схеми керування процесом, процеси фуцкціювання і технічного обслуговування, а також дії аварійного реагування. Якщо дослідження HAZOP не пов'язано з технічними засобами, вхідними даними можуть бути будь-які документи, які описують функції та елементи досліджуваних системи чи алгоритмів. Наприклад, вхідними даними можуть бути організаційні діаграми та посадові інструкці чи проект контракту.

Типові етапи дослідження HAZOP:

- призначення особи, наділеної необхідними повноваженнями для проведення дослідження HAZOP, що забезпечить належне виконання досліджень;
- визначення цілей і сфери дослідження;
- формування групи з HAZOP (група зазвичай є багатодисциплінарною, у складі групи мають бути проектанти та особи, що експлуатують з відповідною

технічною компетентністю, щоб оцінювати наслідки відхилень від задуманого чи фактичного проекту. До складу групи рекомендовано залучати осіб, які не пов'язані безпосередньо з проектом або системою, процесом чи дією, підданих критичному аналізу;
- збирання необхідної документації.

У межах технічного семінару дослідницька група виконує:
- розділення системи, процесу чи явища на дрібні елементи та підсистеми, підпроцеси чи піделементи, щоб забезпечити предметний критичний аналіз;
- погоджування проекту для кожної підсистеми, кожного підпроцесу чи піделемента, потім для кожного їхнього об’єкта, послідовно застосовуючи настановні слова, щоб теоретично припустити можливі відхилення, які матимуть небажані результати;
- погодження причин і наслідків у кожному випадку щодо якого ідентифіковано небажаний результат, і вироблення пропозицій щодо можливого способу їх оброблення, щоб запобігти виникненню чи зменшенню наслідків;
- документування обговорення та погодження конкретних дій з обробляння ідентифікованих ризиків.

Література [2, 7, 8].

Практичне заняття № 4
ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ МЕТОДОМ МОНТЕ-КАРЛО

Мета роботи: Ознайомитися із імітаційним моделюванням - методом Монте-Карло.

Багато систем є надто складними, щоб можна було аналітичними методами змоделювати впливи та невизначеності. Однак, їх можна оцінювати, розглядаючи вхідні дані як випадкові змінні та виконуючи певну

кількість N обчислень (так званих імітаційних моделювань) формуванням вибірок вхідних даних для одержання N можливих наслідків бажаного результату. Цей метод можна застосовувати до складних ситуацій, які може бути важко зрозуміти, застосовуючи аналітичні методи, а також щодо яких важко застосовувати аналітичні методи. Системи можна розробляти, використовуючи електронні таблиці та інші традиційні засоби, але вже є новітніші засоби, які задовольняють більш складні вимоги і багато з яких сьогодні відносно недорогі. Коли метод було вперше розроблено, кількість ітерацій, необхідних для імітаційних моделювань методом Монте-Карло, робило процес уповільненим та клопітким, але досягнення у сфері обчислювальної техніки та теоретичні розробки (наприклад, формування вибірок методом «латинського гіперкуба») значно скоротили тривалість опрацювання в багатьох застосуваннях.

Імітаційне моделювання методом Монте-Карло – це засіб оцінювання впливу невизначеності на системи в широкому спектрі ситуацій. Зазвичай, його застосовують, щоб оцінити діапазон можливих результатів і відносну частоту значень у цьому діапазоні для кількісних показників системи (наприклад, вартості, тривалості, продуктивності, попиту та інших подібних показників).

Імітаційне моделювання методом Монте-Карло можна застосовувати з двома різними цілями:

- поширення невизначеності на звичні аналітичні моделі;
- проведення імовірнісних обчислень у разі неможливості застосування аналітичних методів.

Вхідні дані імітаційного моделювання методом Монте-Карло – це детально пророблена модель системи та інформація про типи вхідних даних, джерел невизначеності. Вхідні дані, пов’язані з невизначеністю, зображають як випадкові змінні з більшим або меншим

розкидом їхніх розподілів відповідно до рівня невизначеності. Для цього, часто використовують рівномірний, трикутний, нормальний і логарифмічно-нормальний розподіли.

Процес імітаційного моделювання методом Монте-Карло такий:

1) визначають модель або алгоритм, які якомога точніше відображають поводження досліджуваної системи;

2) модель тестують кілька разів, використовуючи випадкові числа, щоб отримати вихідні дані моделі (імітування системи), коли застосування полягає в моделюванні впливів невизначеності, то модель подають у формі рівняння, яке відображає взаємозв'язок між вхідними параметрами та вихідними даними. Значення, які вибирають для вхідних даних, базуються на відповідних розподілах імовірності, які відображають характер невизначеності для цих параметрів;

3) в усіх випадках за допомогою комп'ютера модель застосовують багато разів (найчастіше до 10 000 разів) з різними вхідними даними та одержують численні вихідні дані. Використовуючи звичайні статистичні методи, ці результати може бути опрацьовано, щоб одержати таку інформацію, як наприклад, середні значення, стандартні відхилення, довірчі інтервали.

Вихідними даними можуть бути окремі значення, результат зазначено як імовірність чи розподіл частот або визначення основних функцій моделі, що найбільше впливає на вихідні дані.

Імітаційне моделювання методом Монте-Карло застосовують для загального оцінювання сукупного розподілу результатів, що можуть виникати або ключових показників, зумовлених розподілом, таких як:

- імовірність виникнення визначеного результату;

- значення результату щодо осіб, яких стосується проблема, мають певний рівень упевненості в тому, що його не буде перевищено, витрати, можливість перевищення яких становить менше ніж 10% або тривалість, упевненість у перевищенні якої становить 80%.

Аналізування зв’язків між вхідними та вихідними даними може сприяти виявленню відносної важливості задіяних чинників та ідентифікуванню цілей, на які корисно спрямовувати зусилля, щоб впливати на невизначеність результату.

Переваги імітаційного моделювання методом Монте-Карло:

- метод можна застосовувати за будь-якого розподілу вхідної змінної, охоплюючи емпіричні розподіли, виведені зі спостережень за суміжними системами;
- моделі відносно прості для розробляння, їх можна розширювати за потреби;
- дає змогу зображати всі впливи чи зв'язки, що виникають у реальності, зокрема ефекти, які важко виявити, наприклад, умовні залежності;
- для ідентифікування сильних і слабких впливів можна застосовувати аналізування чутливості;
- моделі легкі для розуміння, оскільки зв’язок між вхідними та вихідними даними є прозорим;
- є ефективні поведінкові моделі, наприклад, мережі Петрі, які виявляються дуже ефективними для цілей імітаційного моделювання методом Монте-Карло;
- забезпечує міру точності результату;
- програмне забезпечення доступне і відносно недороге.

Обмеження:

- точність рішень залежить від кількості імітаційних моделювань, які може бути виконано (ця обмеженість стає менш вагомою в разі збільшення швидкодії комп’ютера);

- спирається на спроможність зображати невизначеності параметрів переконливим розподілом;

- великорозмірні та складні моделі можуть завдавати труднощів спеціалісту з моделювання та утруднювати участь у процесі зацікавлених сторін;

- метод може неадекватно розрізняти важливі наслідки та малоймовірні події, тому не завжди спроможний відображати в аналізі готовність організації до ризику.

Література [2, 5, 9].

Практичне заняття № 5
ПРОЦЕС КЕРУВАННЯ РИЗИКОМ – МЕТОД ДЕЛЬФІ

Мета роботи: Ознайомитися із процесом керування ризику – методом Дельфі.

Метод Дельфі (або метод експертних оцінок) – це процес досягнення надійного консенсусу думок групи експертів. Хоча цей термін нині широко використовують на означення будь-якої форми мозкової атаки, істотна особливість методу Дельфі, згідно з його початковим формулюванням, полягала в тому щоб експерти висловлювали свої думки індивідуально та анонімно, маючи можливість ознайомлюватись з думкою своїх колег під час процесу.

Метод Дельфі можна застосовувати на будь-якій стадії процесу керування ризиком або на будь-якій стадії життєвого циклу системи кожного разу, коли потрібен консенсус думок експертів.

Групу експертів опитують за допомогою напівструктурованої анкети. Експерти не знають один одного, тому їхні думки незалежні.

Процедура така:

- формують команду, яка запроваджуватиме та відстежуватиме процес реалізовування методу Дельфі;
- добирають групи експертів (може бути одна чи кілька спеціалізованих груп експертів);
- розробляють анкети першого етапу;
- тестують анкети;
- надсилають анонімні анкети кожному члену групи;
- аналізують і об'єднують інформацію за першим етапом і розсилають її членам групи для обговорення;
- отримують відповіді членів групи та повторюють процес доти, доки не буде досягнено консенсусу.

Переваги:
- зважаючи на анонімність суджень, більш імовірним є висловлювання непопулярних думок;
- усі думки є рівноважними, що дає змогу уникати проблеми переважання думок окремих особистостей;
- дає право власності на результати;
- немає потреби збирати учасників одночасно в одному місці.

Обмеження:
- потребує багато часу та значних витрат праці;
- учасники мають бути здатні чітко письмово викладати свої думки.

Література [2, 4, 11].

Практичне заняття № 6
АНАЛІЗУВАННЯ РІВНІВ ЗАХИСТУ (LOPA)

Мета роботи: Ознайомитися із методом аналізу рівнів захисту (LOPA).

LOPA – це напівкількісний метод оцінювання ризиків, пов'язаних з небажаними подією чи сценарієм. Він дає

змогу аналізувати заходи контролювання чи зменшення ризику.

Вибирають пару причина-наслідок та ідентифікують рівні захисту, які запобігають впливу, що призводить до небажаного наслідку. Обчислюють порядок величини, щоб визначити адекватність захисту для зменшення ризику до прийнятного рівня.

LOPA можна застосовувати як якісний метод, тільки щоб критично проаналізувати рівні захисту між небезпечним чинником або причинною подією та результатом. Зазвичай, напівкількісний підхід застосовують для додання більшої строгості процесів відсортування (наприклад, після HAZOP або PHA).

LOPA – це основа для специфікування незалежних рівнів захисту (IPL) і рівнів цілісності безпеки (SIL) для контрольно-вимірювальних систем. Визначання вимог до рівнів цілісності безпеки (SIL) для контрольно-вимірювальних систем безпеки. LOPA можна застосовувати, щоб сприяти результативному розподіленню ресурсів зменшення ризику, аналізуючи зменшення ризику, що забезпечується кожним рівнем захисту.

Вхідні дані LOPA:

- основоположна інформація стосовно ризиків, зокрема небезпечних чинників, причин і наслідків (наприклад, одержувана за PHA);
- інформація стосовно засобів контролювання, запроваджених чи пропонованих;
- частота причинних подій, імовірності відмови рівнів захисту, величина наслідків і визначений допустимий ризик;
- частота першопочаткових причин, імовірності відмови рівнів захисту, величина наслідків і визначення допустимого ризику.

LOPA провадить група експертів, застосовуючи таку процедуру:

- визначає першопочаткові причини небажаного результату і пошук даних за частотою та наслідками впливів;
- вибирає окрему пару причина-наслідок;
- ідентифікує рівні захисту, які запобігають тому, щоб причина призводила до небажаного наслідку, аналізуючи результативність;
- ідентифікує незалежні рівні захисту (IPL) (не всі рівні захисту незалежні);
- кількісно оцінює імовірність відмови кожного IPL;
- поєднує частоту першопочаткової причини з імовірностями відмови кожного IPL та імовірностями будь-яких умовних модифікаторів (наприклад, чи буде присутня людина, на яку чинитиметься вплив), щоб визначити частоту виникнення небажаного наслідку. Частоту та імовірності визначають з використанням порядків величини;
- порівнює обчислений рівень ризику з рівнями толерантності до ризику, щоб визначити потребу додаткового захисту.

IPL – це система пристроїв або дії, які спроможні запобігати тому, щоб сценарій призводив до свого небажаного наслідку, незалежно від причинної події чи будь-якого іншого рівня захисту, пов’язаних з цим сценарієм. IPL охоплюють:

- конструктивні особливості;
- пристрої фізичного захисту;
- системи блокування та вимикання;
- засоби сигналізування у критичних ситуаціях і ручне втручання;
- фізичний захист після настання події;

- системи аварійного реагування (процедури та інспекційні перевірки не є незалежними рівнями захисту).

Має бути вироблено рекомендації щодо будь-яких допоміжних засобів контролювання та щодо результативності цих засобів контролювання стосовно зменшення ризику.

LOPA - це одна з методик, використовуваних для загального оцінювання SIL у разі розглядання систем, пов'язаних з безпекою, та контрольно-вимірювальних систем.

Переваги:

- потребує менше часу та ресурсів, ніж аналіз дерева відмов або цілком кількісне загальне оцінювання ризику, але більш строгий за якісні суб'єктивні судження;
- сприяє ідентифікуванню найкритичніших рівнів захисту та зосередженню ресурсів на них;
- дає змогу ідентифікувати операції, системи та процеси, засоби захищання яких є недостатніми;
- зосереджує увагу на найважчих наслідках.

Обмеження:

- LOPA зосереджує увагу одночасно на одній парі причина-наслідок і одному сценарії. Складні взаємодії між ризиками або між засобами контролювання не розглядають;
- кількісні ризики можуть не враховувати відмови загального характеру;
- LOPA не застосовний до дуже складних сценаріїв з багатьма парами причина-наслідок або різноманітними наслідками, що впливають на різні зацікавлені сторони.

Література [2, 5, 7].

Рекомендована література

Базова

1. ДСТУ ISO 31000:2018 (ISO 31000:2018, IDT) Менеджмент ризиків. Принципи та настанови. [Чинний від 2019-01-01]. Вид. офіц. Київ: ДП «УкрНДНЦ», 2019. 28 с.

2. ДСТУ IEC/ISO 31010:2013: Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). [Чинний від 2014-07-01]. Вид. офіц. Київ: Мінекономрозвитку України, 2015. 79 с.

3. ДСТУ ISO Guide 73-2013: Керування ризиком Словник термінів (ISO Guide 73:2009, IDT). [Чинний від 2014-07-01]. Вид. офіц. Київ: Мінекономрозвитку України, 2014. 17 с.

4. ДСТУ OHSAS 18001:2010 Системи управління гігієною та безпекою праці. Вимоги (OHSAS 18001:2007, IDT). [Чинний від 2011-01-01]. Вид. офіц. Київ: Держспоживстандарт України, 2011. 27 с.

5. ДСТУ ISO 45001:2019 Системи управління охороною здоров'я та безпекою праці. Вимоги та настанови щодо застосування (ISO 45001:2018, IDT). [Чинний від 2021-01-01]. Вид. офіц. Київ: ДП «УкрНДНЦ», 2011. 55 с.

6. Хенли Э. Дж., Кумамото Х. Надёжность технических систем и оценка риска: перев. с англ., под общ. ред. В. С. Сыромятникова / Э. Дж. Хенли, Х. Кумамото. М. : Машиностроение, 1984. 528 с.

7. Барлоу Р., Прошан Ф. Статистическая теория надежности и испытания на безотказность : перев. с англ. / Р. Барлоу, Ф. Прошан. М. : Наука, 1984. 328 с.

8. Корчагин А. Б. Надежность технических систем и техногенный риск : учеб. пособие : Ч. 2 : Практикум / А. Б.Корчагин, В. С. Сердюк, А. И. Бокарев. Омск : Изд-во ОмГТУ, 2011. 140 с.

9. Мельчаков А. П. Расчет и оценка риска аварии и безопасного ресурса строительных объектов (теория, методики и инженерные приложения) : учебное пособие. Челябинск: Издательство ЮУрГУ, 2006. 49 с.

10. Ярошевський М. М. Словник термінів і понять з безпеки життєдіяльності : навч. посібник : 2-е вид., доп. і доопр. / М. М. Ярошевський, В. М. Ярошевська, Д. М. Диновський. К. : Професіонал, 2004. 256 с.

Допоміжна

11. Гогіташвілі Г. Г. Управління охороною праці та ризиком за міжнародними стандартами / Г. Г. Гогіташвілі, Є. Т. Карчевські, В. М. Лапін. Київ: Знання, 2007. 367 с.

12. Ярошевський М. М. Словник термінів і понять з безпеки життєдіяльності: навч. посібник : 2-е вид., доп. і доопр. / М. М. Ярошевський, В. М. Ярошевська, Д. М Диновський. К. : Професіонал, 2004. 256 с.

13. Заплатинський В., Матис Й. Безопасность в эру глобализации : монография. ЦУЛ, 2010. 142.

Інформаційні ресурси

14. Освітньо-професійна програма «Охорона праці» другого рівня вищої освіти за спеціальністю №263 «Цивільна безпека». Рівне, НУВГП, 2017. 18 с. URL: http://ep3.nuwm.edu.ua/14781/.

15. Законодавство України/ URL: https://zakon.rada.gov.ua/laws.