КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ЖИТОМИРСЬКИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ КОЛЕДЖ

Дисципліна: Основи охорони праці та безпека життєдіяльності

Тема 3. Застосування ризику орієнтованого підходу для побудови імовірнісних структурно-логічних моделей виникнення та розвитку надзвичайних ситуацій.

Вид заняття: лекція

Мета:

Набуття студентом компетенцій, знань, умінь і навичок для здійснення професійної діяльності за спеціальністю з урахуванням ризику виникнення техногенних аварій й природних небезпек, які можуть спричинити надзвичайні ситуації та привести до несприятливих наслідків на об'єктах господарювання, а також формування у студентів відповідальності за особисту та колективну безпеку і усвідомлення необхідності обов'язкового виконання в повному обсязі всіх заходів гарантування безпеки праці на робочих місцях

Міжпредметні (міждисциплінарні) зв'язки:

Дисципліни, що забезпечують: фізика, біологія, основи охорони праці, захист Вітчизни.
Дисцтпліни, які забезпечуються: торговельне устаткування, товарознавство продовольчих товарів, товарознавство непродовольчих товарів, організація та технологія торговельних процесів, виробництво харчової продукції, організація харчування туристів в готелях та інші.

Забезпечення заняття: конспект лекції

Проведення заняття

I Організаційний момент:

- перевірка готовності групи та аудиторії до заняття, забезпечення санітарного стану аудиторії

II Вступна частина

- Мотивація заняття, визначення та значення заняття в темі та курсі в цілому
- Актуалізація знань, постановка навчальної проблеми
- Роз'яснення технології проведення заняття

План

1.Загальний аналіз ризику. Концепція прийнятого ризику.

2. Оцінка ризику.

III Основна частина

1.Загальний аналіз ризику. Концепція прийнятого ризику.

Ризик - ступінь ймовірності певної негативної події, яка може відбутися у певний час або за певних обставин на території об'єкта підвищеної небезпеки або за його межами.

Об'єкт підвищеної небезпеки - об'єкт, на якому використовуються, виготовляються, переробляються, зберігаються або транспортуються одна або кілька небезпечних речовин чи категорій речовин у кількості, що дорівнює або перевищує нормативно встановлені порогові маси, а також інші об'єкти як такі, що є реальною загрозою виникнення надзвичайної ситуації техногенного та природного характеру

Загальним у всіх наведених визначеннях є те, що ризик включає невпевненість, чи відбудеться небажана подія, чи виникне несприятливий стан, чи відбудеться шкода (людині, довкіллю, інфраструктурі тощо). Помітимо, що відповідно до сучасних поглядів ризик зазвичай інтерпретується як міра ймовірності (очікувана частота) виникнення техногенних або природних явищ, що супроводжуються виникненням, формуванням і дією небезпек, та завданого при цьому соціального, економічного, екологічного та інших видів збитку і шкоди. При певних ситуаціях людина, суспільство не гарантовані від небезпеки і тоді діє система рівнянь, яка виявляє відносну або умовну безпеку.

Загроза безпеки людей найчастіше складається з багатьох складових, наприклад:

- з основного існуючого ризику,
- ризику помилок і
- ризику на який ідуть свідомо під час відповідних подій.

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

На малюнку (Рис.2) наведено спрощений варіант визначення прийнятного (допустимого) ризику.

Рис.2 Визначення прийнятного ризику.

Сутність концепції прийнятного (допустимого) ризику полягає у прагненні створити таку невелику небезпеку, яку приймає суспільство в даний час, виходячи з рівня життя соціального стану, розвитку науки і техніки.

Прийнятний ризик поєднує в собі технічні, економічні, соціальні та політичні аспекти і являє собою деякий компроміс між рівнем безпеки і можливим її досягненням. У першу чергу необхідно мати на увазі, що перевищення рівня захисту від небезпеки автоматично підвищує загальні витрати виробництва.

Зневажливий (нульовий) ризик має настільки малий рівень, що він буває у межах допустимого впливу природного (фонового) рівня.

Гранично допустимий ризик - це максимальний ризик, який не повинен перевищувати надмірний, незважаючи на очікуваний результат.

Надмірний ризик характеризується виключно високим рівнем, який у більшості випадків призводить до негативних наслідків. На практиці досягти нульового рівня ризику, або абсолютної безпеки неможливо.

Тому сучасна концепція безпеки життєдіяльності базується на досягненні прийнятного (допустимого) ризику. Досягнення нульового ризику може обернутися для людини соціальної трагедією і безробіттям. При підвищенні витрат на удосконалення обладнання технічний ризик зменшується, але зростає соціальний.

Сумарний ризик має мінімум при певному співвідношенні між інвестиціями в технічну і соціальну сферу. Ці обставини і слід враховувати при виборі рівня ризику, який потрібно забезпечити у відповідному проекті, технології, об'єкті. Існують сталі уявлення про величини прийнятого(допустимого)та недопустимого ризику (Таб.2).

Таблиця 2. Критерії прийнятного ризику

Ранг ризику	Ймовірність однієї смерті за рік	Ступінь прийнятності ризику
1	Не менш $1*10^{-3}$	Ризик неприйнятний
2	10^{-3}	Ризик прийнятний лише в особливих обставинах
3	10^{-3}	Потрібне детальне обгрунтування прийнятності
4	10^{-3}	Ризик прийнятний без обмежень

Величина ризику (R) визначається як відношення кількості подій з небажаними наслідками (n) до максимально можливого їх числа (N) за конкретний період часу.

$R = \frac{n}{N}$, де: R– ризик за певний період часу.

Наведена формула дозволяє розрахувати величину загального та групового ризику. При оцінці загального ризику величина N визначає максимальну кількість усіх подій, а при оцінці групового ризику – максимальну кількість подій у конкретній групі. Характерним прикладом визначення загального ризику може служити розрахунок числового значення загального ризику побутового травматизму зі смертельними наслідками. Відповідно до статистичних даних, за 1998 рік в Україні загинуло у побутовій сфері 68,2 тис. осіб. Наразитись на смертельну небезпеку в побуті практично міг кожен із загального числа громадян, що проживали в Україні на цей період, тобто N= 50 000 000 осіб. Тоді числове значення загального ризику смертельних випадків у побутовій сфері в 1998 році складатиме:

R= 68 200 / 50 000 000 = 0,001 362 = 1 362 x 10^{-6}.

Це означає, що з кожного мільйона громадян, які проживали в Україні, у побутовій сфері загинуло у 1998 році 1 362 осіб.

Слід уяснити, що для оцінки шкоди небезпек необхідно провести аналіз видів, наслідків і критичності відмовлень (АВНВ, АВНКВ). Для розуміння

цього питання слід розглянути методи АВНВ і АВНКВ, а також дієвість та надійність заходів щодо зменшення імовірності виникнення ризику.

Ризик завжди асоціювався з імовірністю нещасливих подій І (НП) та їхніми наслідками. Його розрахункова залежність відбивається, як правило, в мультиплікативній формі, котра дозволяє оцінити величину очікуваного наслідку:

$R=\{<s_i,p_i,x_i>\},i=1,2,...N$ (2.1)

де R — ризик, що оцінюється; s_i, — сценарій НП; p_i — ймовірність того, що НП станеться; x_i -, — можливі наслідки НП, якщо вона станеться за *і* -им сценарієм.

Для індивідуального ризику R_i умову (2.1) може бути подано як:

$R_i = P_f P_{d/f}$ (2.2)

де P_f— ймовірність нещасної події, $P_{d/f}$ — ймовірність наслідку (наприклад, смертельного виходу) для індивідуума від даної НП, передбачаючи відсутність захисту індивідуума від небезпеки.

Таким чином R_i — це властивість зони, що досліджується, в межах якої існує ймовірність НП (ця ймовірність створюється потенційно небезпечними об'єктами, природним явищем тощо), тому індивідуальний ризик є зручною характеристикою для просторового планування. Для індивідуального ризику R_i, верхня межа може бути визначена ґрунтуючись на статистичних обчисленнях.

2. Оцінка ризику.

Оцінка ризику – це аналіз походження (виникнення) і масштабів ризику в конкретній ситуації. Головне призначення її - це визначення пріоритетів серед спектра негативних впливів і в пов’язаному з цим порівнянням застосованих заходів (зіставлення позитивних та негативних чинників, вигод та шкоди). Оцінка ризику запроваджується, щоб визначити причини існуючих проблем. Процес розробки рішення про те, як усунути причини відповідних небезпек є- керування ризиком.

Зіставлення ризиків і встановлення «ризикових» пріоритетів означає їхнє ранжування для визначення прийнятності ризику. Він зіставляється з низкою «ризикових» соціально-економічних та екологічних чинників: вигоди від використання конкретного устаткування, препарату, системи, технології в господарській діяльності; витрати, обумовлені використанням цього устаткування, системи, технології препарату (повною або частковою забороною, зміною його іншими, тощо); наявності та можливості регулюючих заходів з метою зменшити потенційний негативний вплив на навколишнє середовище і здоров’я людини.

У зіставлені «не ризикових» чинників із «ризиковими» виявляється сутність процесу керування ризиком. Можливі три варіанти прийнятих рішень:

- ризик приймається цілком,
- частково,
- не приймається.

Наступний етап – прийняття регулюючого рішення – визначення нормативних актів (законів, постанов, інструкцій) та їхніх положень відповідно реалізації того «типового» заходу, що було встановлено на попередній стадії.

Заключним етапом керування ризиком є контроль і коригування результатів обраної стратегії з урахуванням отриманої інформації.

- це міра очікуваної небажаної події (невдачі), усвідомлена
- кількісна оцінка ймовірності виникнення події з певними небажаними наслідками.

Інженерний – спирається на статистику, розрахунки частоти проявлення небезпек, імовірнісний аналіз безпеки та на побудову “дерев” небезпек;

Модельний – базується на побудові моделей впливу небезпек як на окрему людину так і на соціальні, професійні групи;

Експертний – за ним ймовірність різних подій визначається досвідченими спеціалістами-експертами;

Соціологічний (соціометрична оцінка) – базується на опитуванні населення та працівників.

Управління ризиком. Основне питання теорії й практики безпеки «Як підвищити рівень безпеки»? Очевидно, що для цієї мети кошти можна витрачати за трьома напрямами:

а) удосконалювання технічних систем та об’єктів;

б) підготовка персоналу;

в) ліквідація наслідків.

Апріорно важко визначити співвідношення інвестицій по кожному напряму. Необхідний спеціальний аналіз із використанням конкретних даних та умов. Висновки можуть бути при цьому досить непередбачуваними.

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*.

Перехід до ризику відкриває принципово нові можливості підвищення безпеки технічної сфери. До технічних, організаційних, адміністративних додаються економічні методи керування ризиком. До останніх відноситься: страхування, грошова компенсація ушкодження, платежі за ризик тощо. Спеціалісти вважають доцільним у законодавчому порядку запровадити квоти на ризик.

Для розрахунку ризику необхідні обґрунтовані дані. Гостра потреба в даних у нинішній час визнана у всьому світі на національному та міжнародному рівні.

Необхідна чітко аргументована розробка бази і банків даних та їх реалізація в умовах підприємства, регіону.

В основі керування ризиком лежить методика порівняння видатків та вигод, які отримують від зменшення ризику.

Послідовність вивчення небезпек.

Стадія І. Попередній аналіз небезпеки.

Крок 1. Виявити джерела небезпеки.

Крок 2. Визначити частини системи, які можуть викликати ці небезпеки.

Крок 3. Ввести обмеження на аналіз, тобто виключити небезпеки, які не будуть вивчатися.

Стадія II. Виявлення послідовності небезпечних ситуацій, побудова дерева подій та небезпек.

Стадія III. Аналіз наслідків.

Системний аналіз небезпек (САН) – це сукупність методологічних засобів, що використовуються для підготовки та обґрунтування рішень із складних проблем, у даному випадку безпеки.

Система – це сукупність взаємопов'язаних елементів, які взаємодіють між собою таким чином, що досягається певний результат (мета).

Попередній аналіз небезпек (ПАН) — 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. Проте в багатьох випадках цьому аналізу може передувати підготовка попереднього переліку небезпек.

Системи мають якості, яких може не бути у елементів, які їх утворюють. Ця найважливіша властивість систем, що іменується *емерджентністю,* лежить, по суті, в основі системного аналізу взагалі та проблем безпеки у цілому.

Методологічний курс системного аналізу незвичайний: у ньому переплітаються елементи теорії й практики, суворі формалізовані методи поєднуються з інтуїцією та власним досвідом, із евристичними прийомами.

Під елементами (складовими частинами) розуміють не тільки матеріальні об'єкти, а й відношення та зв'язки. Будь-яка машина є приклад технічної системи. Система, одним із елементів якої є людина, називається *ергативною*. Приклади ергативної системи: «людина – машина», «людина – машина – навколишнє середовище» тощо. Інакше кажучи, будь-який предмет може бути представлений як системне утворення.

Принцип системності розглядає явища у їх взаємному зв'язку, як цілісний набір або комплекс. Мету або результат, який дає система, називають *елементом,* що утворює систему. Наприклад, таке системне явище, як горіння (пожежа) можливе за наявності наступних компонентів: горюча речовина, окисник, джерело запалювання. Вилучаючи хоча б один із названих компонентів, ми руйнуємо систему.

Аналіз дерева помилок (АДП) вважається одним з найбільш корисних аналітичних інструментів у процесі системної безпеки, особливо при оцінці надзвичайно складних або деталізованих систем. Завдяки тому що він використовує *дедуктивний логічний метод* (тобто поступово рухається від загального до часткового), він дуже корисний при дослідженні можливих умов, які можуть призвести до небажаних наслідків або яким-небудь чином вплинути на ці наслідки.

«Дерево причин та небезпек» як система. Будь-яка небезпека реалізується, приносячи ушкодження, завдяки якійсь причині або кільком причинам. Без причин нема реальних небезпек. Отже, запобігання небезпекам або захист від них ґрунтується на знанні причин. Між реалізованими небезпеками та причинами існує причинно-наслідковий зв'язок; небезпека є наслідком певної причини (причин), яка , у свою чергу, є наслідком іншої причини і т. ін. Таким чином, причини і небезпеки утворюють ієрархічні, ланцюгові структури та системи. Графічне зображення таких залежностей чимось нагадує дерево, що розгалужується.

У закордонній літературі, присвяченій аналізу безпеки об'єктів, використовуються такі терміни як «дерево причин», «дерево відмов», «дерево небезпек», «дерево подій». У деревах, що будуються, як правило, є гілки причин та гілки небезпек, що повністю відображає діалектичний характер причинних та наслідкових зв'язків. Розділення цих гілок недоцільне, а іноді й неможливе. Тому точніше назвати отримані у процесі аналізу безпеки об'єктів графічні зображення «деревами причин та небезпек».

Побудова «дерев» є виключно ефективною процедурою виявлення причин різних небажаних подій (аварій, травм, пожеж, дорожньо-транспортних подій тощо). Багатоетапний процес розгалуження «дерева» потребує впровадження обмежень з метою визначення його межі. Ці обмеження цілком залежать від мети дослідження. Взагалі, границі розгалуження визначаються логічною доцільністю отримання нових гілок.

Аналіз безпеки може здійснюватися апріорно або апостеріорним методом, тобто до або після небажаної події. У обох випадках використовуваний метод може бути прямим і оберненим.

А п р і о р н и й а н а л і з. Дослідник вибирає такі небажані події, які є потенційно можливими для даної системи, і намагається скласти набір різних ситуацій, що можуть призвести до їх появи.

А п о с т е р і о р н и й а н а л і з. Виконується після того, як небажані події вже відбулися. Мета такого аналізу – розробка рекомендацій на майбутнє.

Апріорний та апостеріорний аналізи доповнюють один одного. Прямий метод аналізу полягає у вивченні причин, щоб передбачити наслідки. При оберненому методі аналізуються наслідки, щоб визначити причини, тобто аналіз починається із кінцевої події. Кінцева мета завжди одна – запобігання небажаним подіям.

Маючи імовірність та частоту виникнення первинних подій, можна, рухаючись знизу вгору, визначити імовірність кінцевої події. Основною проблемою під час аналізу безпеки є встановлення параметрів та меж системи. Якщо система буде занадто обмежена, то з’являється можливість отримання розрізнених несистематичних попереджувальних заходів, тобто деякі небезпечні ситуації можуть залишитися без уваги. З іншого боку, якщо розглядувана система надто велика, то результати аналізу можуть виявитися надто невизначеними. Перед дослідником стоїть питання також про те, до якого рівня потрібно вести аналіз. Відповідь на це питання залежить від конкретної мети аналізу.

IV Заключна частина

Контрольні запитання:

1. Визначення наявних проблем з безпеки і захисту ОГ у НС, рівня їхнього ризику.
2. Галузеві вимоги і норми щодо забезпечення сталого функціонування ОГ та контролю за станом його основних фондів