МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Факультет мехатроніки та комп'ютерних технологій

Кафедра прикладної механіки та машин

Дипломна магістерська робота

на тему: Оцінювання ризиків складних організаційно-технічних систем за вимогами ДСТУ ISO 31010

Виконав: студентка групи МгЯС-20
спеціальності 152 Метрологія та інформаційно-вимірювальна техніка
(шифр і назва спеціальності)

Вікторія СОВИЧ

Керівник Ганна ХІМІЧЕВА

Рецензент Володимир ДВОРЖАК
(ініціали , прізвище)

Київ 2021

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Факультет мехатроніки та комп'ютерних технологій

Кафедра прикладної механіки та машин

Спеціальність 152 Метрологія та вимірювальні техніка

Освітня програма Якість, стандартизація та сертифікація

ЗАТВЕРДЖУЮ

Завідувач кафедри ПММ

_____Олександр МАНОЙЛЕНКО

«___»_____2021 року

З А В Д А Н Н Я

НА ДИПЛОМНУ МАГІСТЕРСЬКУ РОБОТУ СТУДЕНЦІ

Сович Вікторії Іванівні

(прізвище, ім'я, по батькові)

1. Тема роботи: Оцінювання ризиків складних організаційно-технічних систем за вимогами ДСТУ ISO 31010.

Науковий керівник роботи Хімічева Ганна Івнівна, д.т.н. проф.

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладом вищої освіти від "04" жовтня 2021року № 286

2. Строк подання студентом роботи 15 грудня 2021 рік.

3. Вихідні дані до роботи: Методи аналізу ризику згідно ДСТУ ISO 31010, шкала оцінювання ефективності та результативності СОТС від 0 до 1, управління безпекою СОТС згідно міжнародних стандартів IEC 61508, IEC 61511, валідація ризиків згідно діючих нормативних документів, оцінювання ризиків, якісне та кількісне.

4. Зміст дипломної роботи (перелік питань, які потрібно розробити) Вступ. Розділ 1 Аналіз термінів, вимог та методів щодо оцінювання ризику. Розділ 2 Теоретичні основи оцінювання ризиків складних організаційно-технічних систем. Розділ 3 Практичні рекомендації щодо оцінювання ризиків безпеки складних організаційно-технічних систем. Загальні висновки.

Список використаних джерел. Додатки.

Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Вступ	Ганна ХІМІЧЕВА проф. каф. ПММ		
Розділ 1	Ганна ХІМІЧЕВА проф. каф. ПММ		
Розділ 2	Ганна ХІМІЧЕВА проф. каф. ПММ		
Розділ 3	Ганна ХІМІЧЕВА проф. каф. ПММ		
Висновки	Ганна ХІМІЧЕВА проф. каф. ПММ		

5. Дата видачі завдання "05" жовтня 2021 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Вступ	14.10.2021	
2	Розділ 1 Аналіз термінів, вимог та методів щодо оцінювання ризику	27.10.2021	
3	Розділ 2 Теоретичні основи оцінювання ризиків складних організаційно-технічних систем	15.11.2021	
4	Розділ 3 Практичні рекомендації щодо оцінювання ризиків безпеки складних організаційно-технічних систем	01.12.2021	
5	Загальні висновки	03.12.2021	
6	Оформлення дипломної магістерської роботи	06.12.2021	
7	Здача дипломної магістерської роботи на кафедру для рецензування (за 14 днів до захисту)	10.12.2021	
8	Перевірка дипломної магістерської роботи на наявність ознак плагіату (за 10 днів до захисту)	14.12.2021	
9	Подання дипломної магістерської роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	17.12.2021	

Студент _____ Вікторія СОВИЧ
(підпис)

Керівник роботи _____ Ганна ХІМІЧЕВА
(підпис)

Директор НМЦУПФ _____ Олена ГРИГОРЕВСЬКА
(підпис)

АНОТАЦІЯ

Сович В.І. Оцінювання ризиків складних організаційно-технічних систем за вимогами ДСТУ ISO 31010. – Рукопис.

Дипломна магістерська робота за спеціальністю 152 Метрологія та вимірювальна техніка. Освітня програма: Якість, стандартизація та сертифікація – Київський національний університет технологій та дизайну, Київ, 2021 рік.

Дипломна магістерська робота присвячена питанням щодо оцінювання ризиків та безпеки складних організаційно-технічних системи з урахуванням чинної нормативно-правової документації, зокрема міжнародних стандартів ДСТУ ISO 31010.

В роботі проаналізовано терміни щодо визначення поняття ризик і запропоновано трактувати «ризик» як результат невизначеності завдань, які охоплюють події, що можуть відбутися, а можуть не відбутися та привести до несприятливих ситуацій або наслідків. Доведено, що рівень невизначеності обумовлюється неясністю чи неточністю інформації щодо ризику, джерел, подій та наслідків. Система нормування ризиків повинна базуватися на єдності методологічних підходів та уніфікації методів нормування. В роботі запропоновано методи аналізу ризику поділити на детерміновані, ймовірнесно-статистичні, комбіновані та ті що застосовуються в умовах невизначеності нестохастичної природи.

Складна організаційно-технічна система являє собою ієрархічний людинно-машинний комплекс, який в процесі функціонування реалізує його властивості щодо досягнення мети для якої його було створено. Для оцінювання безпеки СОТС розроблена схема, яка враховує перелік властивостей та числові значення, які отримані шляхом вимірювання, випробування підрахунку. Такий підхід дозволяє з достатнім ступенем достовірності організувати безпеку СОТС.

Для валідації ймовірнисного аналізу ризику розроблено загальну схему, яка включає в себе такі складові: планування аналізу, моделювання аварій

(небезпеки), підрахунок наслідків аварії, документування, ідентифікацію небезпеки, підрахунок ймовірності аварії, підрахунок ризику, заходи щодо зниження рівня ризику. Для прийняття рішень, щодо зменшення ризиків, запропоновано застосовувати низку міжнародних стандартів, зокрема ISO 9001, ISO 31000, ISO 37120, ДСТУ ISO/IEC 25000 тощо. Для оцінювання ідентифікації ризиків розроблено покроковий алгоритм в основу якого покладено вимоги ДСТУ ISO 31010.

Ключові слова: *складна організаційно-технічна система, методи оцінювання ризиків, безпека, алгоритми, методики, невизначеність.*

SUMMARY

Sovich VI Risk assessment of complex organizational and technical systems according to the requirements of DSTU ISO 31010. - Manuscript.

Master's thesis in the specialty 152 Metrology and Measurement Engineering. Educational program: Quality, standardization and certification - Kyiv National University of Technology and Design, Kyiv, 2021.

The master's thesis is devoted to issues of risk and safety assessment of complex organizational and technical systems taking into account the current legal documentation, in particular the international standards DSTU ISO 31010.

The paper analyzes the terms for defining the concept of risk and proposes to interpret "risk" as a result of uncertainty of tasks that cover events that may or may not occur and lead to adverse situations or consequences. It is proven that the level of uncertainty is due to ambiguity or inaccuracy of information about risk, sources, events and consequences. The risk rationing system should be based on the unity of methodological approaches and unification of rationing methods. The paper proposes methods of risk analysis to be divided into deterministic, probabilistic-statistical, combined and those used in conditions of uncertainty of non-stochastic nature.

A complex organizational and technical system is a hierarchical human-machine complex, which in the process of functioning realizes its properties to achieve the purpose for which it was created. To assess the safety of the WTO, a scheme has been developed that takes into account the list of properties and numerical values obtained by measuring and testing the calculation. This approach allows you to organize the security of the SOTS with a sufficient degree of reliability.

To validate probabilistic risk analysis, a general scheme has been developed, which includes the following components: analysis planning, accident modeling (hazards), accident consequence calculation, documentation, hazard identification, accident probability calculation, risk calculation, risk reduction measures. It is proposed to apply

a number of international standards, in particular ISO 9001, ISO 31000, ISO 37120, DSTU ISO / IEC 25000, etc., to make decisions on risk reduction. To assess the identification of risks developed a step-by-step algorithm based on the requirements of DSTU ISO 31010.

Key words: *complex organizational and technical system, risk assessment methods, security, algorithms, methods, uncertainty.*

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ОПН – Об’єкт підвищеної небезпеки

РП – Ризикоутворююча причина

НП – Надзвичайна подія

PHA – Попередній аналіз небезпеки (Process Hazard and Analysis)

FMEA – Аналіз виду і наслідків події (Failure Mode and Effects Analysis)

AEA – Аналіз помилкових дій (Action Errors Analysis)

CHA – Концептуальний аналіз ризику (Concept Hazard Analysis)

CSR – Концептуальний огляд безпеки (Concept Safety Review)

Human HAZOP – Аналіз людських помилок (Human Hazard and Operability)

HRA – Аналіз впливу людського чинника (Human Reliability Analysis)

HIRA – Методика визначення і ранжирування ризику (Hazard Identification and Ranking Analysis)

FMECA – Аналіз виду, наслідків і критичності події (Failure Mode, Effects and Critical Analysis)

HRQ – Кількісне визначення впливу людського чинника (Human Reliability Quantification)

MDEA – Методика аналізу ефекту доміно (Methodology domino effects analysis)

MPRDE – Методика визначення та оцінки потенційного ризику (Methods potential risk determination and evaluation)

ASP – Причини послідовності нещасних випадків (Accident SequencesPrecursor)

ETA –Аналіз дерева подій (Event Tree Analysis)

FTA – Аналіз дерев відмов (Fault Tree Analysis)

SCRA – Оцінка ризику мінімальних шляхів від ініціюючого до основної події (Short Cut Risk Assessment)

HAZOP – Метод аналізу небезпеки і працездатності (Hazard and Operability Study)

MCAA – Аналіз максимальної можливості виникнення нещасного випадку (Maximum Credible Accident Analysis)

RBD – Блок-схема надійності (Reliability Block Diagram)

SA – Аналіз безпеки (Safety Analysis)

SRA – Аналіз надійності структури (Structural Reliability Analysis)

ORA – Повний аналіз ризику – методика оптимального аналізу ризику (Optimum Risk Analysis)

MOSAR – Метод організованого систематичного аналізу ризику (Method Organised Systematic Analysis Risk)

QRA – Кількісна оцінка ризику (Quantitative Risk Assessment)

СОТС – Складна організаційно-технічна система

RPN – Альтернативні способи обчислення числа пріоритетів ризику

BN – Байєсівської мережі

SPN – Стохастичної мережі Петрі

STPA – Системно-теоретичний аналіз процесів

RMA – Підхід матриці ризиків

IBA – Підхід на основі показників

СУТП – Систем управління технологічними процесами

SIS – Інструментальна система безпеки

SIF – Інструментальна функція безпеки

PE – Програмована електроніка

SIL – Safety integrity level

PFD – Ймовірність відмови за запитом

ВСТУП

Актуальність теми. Сьогодні складні організаційно-технічні системи є ефективним підґрунтям для сталого розвитку економіки країни. Це пов’язано з тим, що вони забезпечують об’єктивну інформацію щодо оцінювання якості та безпеки продукції, послуг та персоналу. Тобто точну інформацію щодо прийнятності шкоди або втрати ефективності функціонування СОТС. Одним із ефективних шляхів вирішення цього завдання є застосування існуючих нормативних документів щодо питань безпеки продукції (процесів, робіт, послуг) для життя, здоров'я, майна громадян, охорони довкілля та об'єктів національної економіки з урахуванням ризику виникнення природних і техногенних катастроф.

Для оцінювання ризиків СОТС доцільно застосовувати міжнародні стандарти, зокрема ISO 31000. Проте на сьогодні для багатьох типів складних організаційно-технічних систем практично відсутні методики оцінювання ризиків безпеки, а вже існуючі часто містять недоліки та невідповідності з міжнародними нормами. Тому виникає потреба у дослідженнях і розробленні сучасних методів, принципів і підходів щодо оцінювання стану безпеки СОТС.

Таким чином дослідження пов’язані з оцінюванням ризиків складних організаційно-технічних систем за вимогами ДСТУ ISO 31010 є актуальними і своєчасними.

Мета роботи полягає в розроблені принципів, методів та підходів щодо оцінювання ризиків та безпеки складних організаційно-технічних систем з урахуванням вимог міжнародних стандартів

Для досягнення поставленої мети було сформульовано та вирішено такі **завдання**:

1. Проаналізувати терміни, вимоги та методи щодо оцінювання ризику.
2. Дослідити теоретичні основи оцінювання ризиків складних організаційно-технічних систем
3. Практичні рекомендації щодо оцінювання ризиків безпеки складних

організаційно-технічних систем

Об’єктом досліджень є удосконалення процесу оцінювання ризиків та безпеки складних організаційно-технічних систем.

Предметом дослідження є методи оцінювання, ризики, безпека, вимоги міжнародних стандартів, властивості складних організаційно-технічних систем.

Методи дослідження. В роботі застосовано методи системного аналізу та математичного моделювання, експертних оцінок, стандартизації.

Наукова новизна.

1. Запропонована модель, що пов’язує ризик, джерела ризику, та наслідки. Дана модель дозволяє оцінити стан невизначеності щодо джерел, подій та наслідків.

2. Запропоновано ієрархію залежності ризиків від впливу та ймовірності їх виникнення. Рівень ризику поділено на дуже високий, високий, середній, низький, незначний.

Практичне значення.

1. Запропоновано покроковий алгоритм щодо ідентифікації ризиків СОТС в основу якого покладено вимоги ДСТУ ISO 31010.

2. Запропоновано методику управління безпекою складної організаційно-технічної системи. В основу, якої покладено вимоги до заходів безпеки та їх функцій, опис елементів та критерії безпеки СОТС, а також їхній взаємний вплив. При застосуванні методики для визначення невпевненості доцільно використовувати метод порядкової статистики.

Апробація результатів досліджень. Результати роботи були представлені та обговорені на V міжнародній науково-практичній конференції «Мехатронні системи: інновації та інжиніринг» - «MSIE-2021» 04 листопада 2021 року, м. Київ.

Структура й обсяг магістерської роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, який включає 66 найменування та додатків. Повний обсяг роботи становить 84 сторінок, 8 таблиця, 22 рисунків та один додаток.

РОЗДІЛ 1 АНАЛІЗ ТЕРМІНІВ, ВИМОГ ТА МЕТОДІВ ЩОДО ОЦІНЮВАННЯ РИЗИКУ

1.1. Загальна характеристика визначення поняття системи «ризик-ймовірність-невизначеність».

На сьогодні немає однозначного розуміння сутності ризику, що обумовлено його багатоаспектністю. Крім того, ризик являє собою складне явище, що має безліч незбіжних, а іноді протилежних реальних основ. Тому існує велика кількість визначень поняття «ризик». Проаналізуємо деякі з них.

Так, згідно Оксфордського словника англійської мови ризик являє собою ймовірність небезпеки, поганих втрат тощо. В свою чергу Вебстерський словник трактує поняття «ризик» як можливість втрат, пошкодження, шкоди або руйнування. У сучасних підручниках ризик трактується як «ризик – це частота, з якою може проявлятися можлива небезпека».

Автори роботи [1] дають таке визначення ризику «ризик – ймовірність людських жертв і матеріальних витрат або травм іпошкоджень». В роботі [2] наголошується, що ризик це подія або група споріднених випадкових подій, що завдають шкоди об’єкту, якому належить цей ризик.

Поняття ризику є універсальною кількісною мірою потенційної небезпеки, що дає змогу провести коригування вихідних цілей і стратегії щодо вирішення завдань аналізу ризику, порівняння небезпек різного походження та механізмів їх дії; класифікацію та ранжирування потенційних джерел небезпеки стосовно їхнього внеску в інтегральні показники ризику; вивчення механізм і дослідження причинно-наслідкового зв'язку щодо виникнення і розвитку небажаних подій, а також впливу на показники ризику різних факторів техногенного, природного та соціального походження; забезпечити спрямування зниження ризиків шляхом оптимального управління технічними та організаційно-методичними факторами впливу (зниження ймовірності, зменшення величини збитку тощо).

Таким чином ризик – це поєднання ймовірності події і його наслідків [3].

Основними його властивостями є характеристика майбутніх станів об’єкта, що пов’язана з випадковими подіями та явищами (проявлення ризику-умовна подія).

В роботі [4] пропонується ризик розглядається як двовимірну величину, що складається з можливості події та обсягу, спричинених подією збитків рис 1.1.

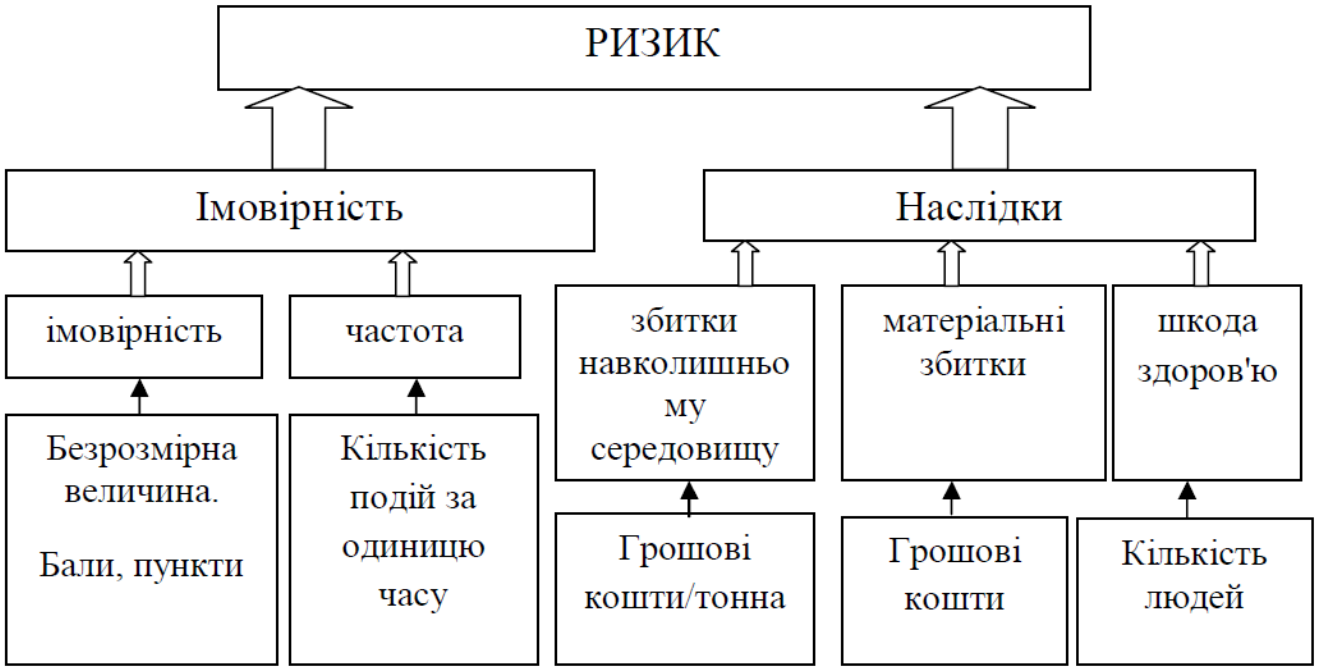

Рис. 1.1 Компоненти ризику, як двомірної величини

Ризик може бути визначений як частота або ймовірність виникнення події Б при настанні події А і є безрозмірною величиною, що знаходятьсяв межах від 0 до 1.

Під поняттям ризик також розуміють не тільки ймовірність, а і події та об’єкти, що призводять до втрат і збитків. Тобто в цьому поняття ризик слід розглядати в трьох аспектах як: ймовірність нанесення збитків; певна подія чи сукупність подій; певний об’єкт прояву.

Для оцінювання ризику використовують математичні методи із застосуванням теорії ймовірності за такими показниками, як частота настання події та максимальний збиток, який виникає внаслідок її реалізації.

Згідно з стандартом ISO 31000 ризик є «результатом невизначеності завдань», де «невизначеність охоплює події, які можуть відбутися і можуть не відбутися, причому невизначеність викликана неясністю чи нестачею інформації» [2].

В роботі доведено, що існує тісний зв'язок ризику, ймовірності та невизначеності. Так, ризик – потенційна, чисельно вимірна можливість втрати. Це поняття характеризується невизначеністю, що пов'язана з можливістю виникнення несприятливих ситуацій і наслідків.

Отже, виходячи з вищенаведеного для визначення поняття «ризик», необхідно ще визначити такі поняття, як «ймовірність» та «невизначеність». Це пов'язано з тим, що саме ці два поняття обумовлюють ризики.

Під поняттям невизначеність слід розуміти наявність декількох ймовірних результатів кожної альтернативи. Тобто це поняття припускає наявність чинників, за умов яких результати дій не є детермінованими, а ступінь можливого впливу цих факторів на результати невідома.

Таким чином невизначеність – це неповне або неточне уявлення про значення різних параметрів у майбутньому, що породженні різноманітними причинами. Наприклад, неповнотою або неточністю інформації про умови реалізації рішення.

Однією з основних причин, що породжують невизначеність є випадковість багатьох явищ, які через свою природу до кінця не можуть бути визначені.

Існує поняття нестохастична невизначеність, яка може бути обумовлена декількома причинами:

– невідомо про існування фактору або про характер його впливу про стан об'єкта;

– неможливо виміряти значення відомого фактору з необхідною точністю (метрологічна невизначеність);

– фактор визначається поведінкою інших об'єктів або елементів системи, що мають свої цілі;

– умови невизначеності обумовлено тим, що системи в процесі свого функціонування відчувають залежність від цілої низки причин.

Залежність видів невизначеності від різних факторів наведено на рис. 1.2.

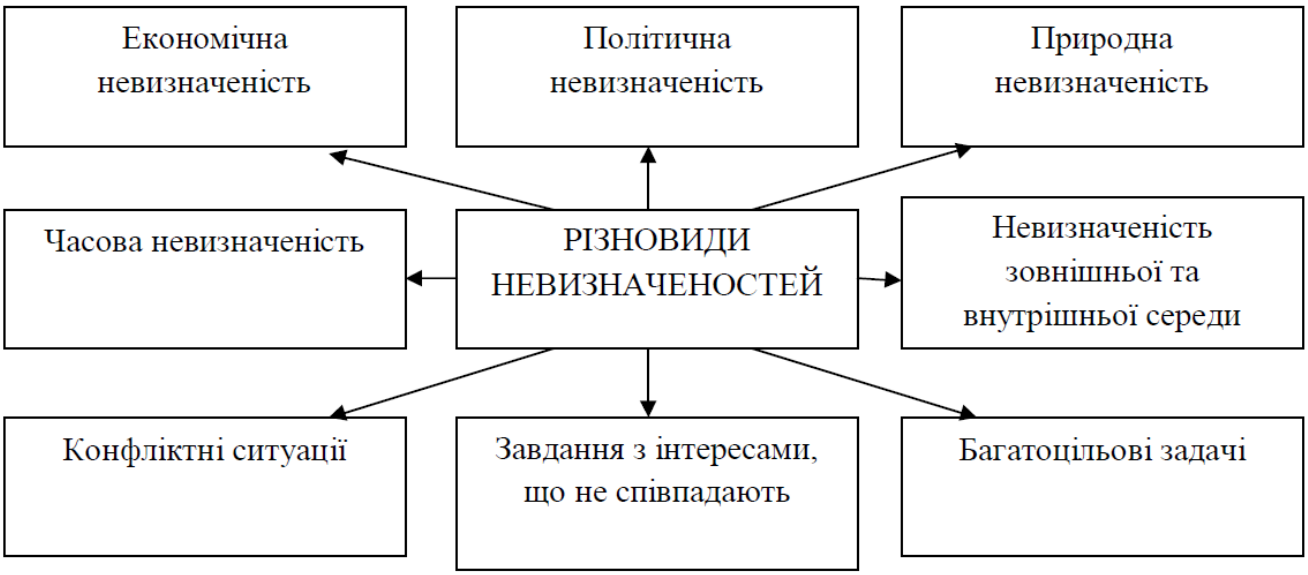

Рис. 1.2 Залежність видів невизначеностей від різних факторів

Економічну невизначеність обумовлено несприятливими змінами в економіці (невизначеність ринкового попиту і пропозиції, асиметрична інформація, слабка передбачуваність ринкових цін тощо). Політичну невизначеність – зміною політичної обстановки, що впливає на підприємницьку діяльність. Соціальну невизначеність – змінами демографічної ситуації переваг і моральних установок населення, що впливають на різні види діяльності.

Отже природні процеси та людська діяльність є основними причинами існування ризику. Тому при прийнятті рішень потрібно враховувати вплив невизначених факторів та розглядати усі ймовірні наслідки альтернатив. Як правило для цього застосовують спеціальні моделі, які забезпечують структуровану обробку інформації щодо наявної проблеми.

1.2. Вимоги нормативно-правових документів щодо визначення ризиків та їх прийнятних рівнів

Нормування ризиків являє собою розроблення і затвердження норм техногенної та природної безпеки, правил і регламентів діяльності національної економіки. Воно є тим засобом, який встановлює межі допустимості техногенної діяльності та межі захисту від небезпечних природних явищ.

Згідно [5] система нормування ризиків має забезпечити:

– єдність методологічних підходів до оцінювання ризиків та джерел небезпеки різного походження і різного виду;

– уніфікацію методів нормування;

– урахування вагомості всіх наслідків соціально-економічного, природно-ресурсного, екологічного та іншого характеру;

– урахування особливостей різновидів виробничої діяльності, техногенного навантаження територій, природно-кліматичних особливостей;

– галузеву і територіальну диференціацію нормативів ризиків;

– урахування всіх чинників, що впливають на величину ризику;

– періодичне коригування нормативів ризиків.

Нормативна база ризиків надзвичайних ситуацій техногенного і природного походження базується на двох основних нормативних рівнях: мінімальному і граничнодопустимому. На практиці використовується поняття прийнятний рівень ризику. Це ризик, менший або такий, що дорівнює граничнодопустимому. Мінімальний – рівень ризику, нижче від якого подальше зменшення ризику є економічно недоцільним. Ризик, значення якого менше або дорівнює мінімальному, вважається абсолютно прийнятним. Тобто будь-яка діяльність із таким низьким значенням ризику є прийнятною і не потребує жодних додаткових зусиль для його зниження. Ризик, значення якого більше за граничнодопустиме, вважають абсолютно неприйнятним.

Для кожної галузі економіки, небезпечної виробничої діяльності, території, типу техногенного чи природного об’єкта визначають свої нормативи мінімального і граничнодопустимого рівнів ризиків, які мають знаходитись у межах аналогічних загальнонаціональних значень.

Для розроблення методів принципів та підходів щодо управління ризиками міжнародною організацію зі стандартизації розроблені спеціальні стандарти. Пріоритетним напрямком цих стандартів є застосування ризик- менеджменту. Ризик-менеджмент – система понять щодо виконання управлінських рішень, які спрямовані на зменшення впливу наслідків реалізації ризиків на діяльність

організації (підприємства) [6].

До основних стандартів слід віднести:

– ISO Guide 73:2009 Risk management – Vocabulary – базовий словник термінів ризик-менеджменту (визначаються поняття ризику та його особливостей, розглядаються такі поняття, як менеджмент ризиків, політика і план менеджменту тощо) [7];

– ISO 31000: 2018 Risk management — Guidelines – wей документ призначений для використання людьми, які створюють і захищають цінність в організаціях, керуючи ризиками, приймаючи рішення, встановлюючи та досягаючи цілей та покращуючи ефективність [8];

– IEC 31010:2019 Risk management — Risk assessment techniques – є керівництвом до вибору методів оцінки ризику залежно від етапу розвиткупроекту або від типу аналізу [9].

Основними нормативно-правовими документами України, що стосуються визначення ризиків та їх прийнятних рівнів є:

– Закон України «Про об’єкти підвищеної небезпеки» [10];

– Постанова Кабінету Міністрів України «Про ідентифікацію та декларування безпеки об’єктів підвищеної небезпеки [11];

– Методика визначення ризиків та їх прийнятних рівнів для декларування безпеки об’єктів підвищеної небезпеки [12].

У цих документах визначається порядок проведення аналізу небезпеки та оцінки ризику об’єктів підвищеної небезпеки (ОПН), встановлюються методичні принципи, терміни і визначення поняття ризик, визначаються критерії прийнятних ризиків та їх рівні.

Так Закон визначає правові, економічні, соціальні та організаційні основи діяльності, пов’язаної з ОПН. Даний документ спрямований на захист життя і здоров’я людей від шкідливого впливу аварій на ОПН шляхом запобігання їх виникненню, обмеження (локалізації) розвитку і ліквідації наслідків.

В Постанові дається визначення порогових мас небезпечних речовин для ідентифікації ОПН, а також затверджується Порядок ідентифікації та обліку даних

об’єктів та Порядок декларування безпеки ОПН.

Документом, який визначає порядок проведення аналізу небезпек та оцінки ризиків ОПН, є Методика визначення ризиків та їх прийнятних рівнів для декларування безпеки об’єктів підвищеної небезпеки . У даній Методиці на законодавчому рівні встановлюються методичні принципи, терміни і поняття аналізу ризику, а також визначаються критерії прийнятних ризиків. Проте вона має ряд недоліків: не описано метод оцінки ризику від декількох джерел небезпеки; не враховується людський фактор; достатньо трудомістка.

Для визначення показників виникнення ризику надзвичайних подій, зокрема їх кількісної характеристики використовують наступні терміни, що наведенні в таблиці 1.1:

Таблиця 1.1

Термін	Визначення
Ризикоутворююча причина (РП)	об’єктивне або суб’єктивне явище або сукупність явищ, безпосередньо пов’язаних з діяльністю людини, які під впливом негативних факторів породжують несприятливі події.
Надзвичайна подія (НП)	результат дії ризикоутворюючої причини або сукупності таких причин під впливом негативних факторів, що призводять до втрати працездатності (повної або часткової) або загибелі людини.
Ризик	імовірність виникнення надзвичайної події, що сталася або може статися в умовах невизначеності, в результаті чого можливе виникнення певної шкоди.
Шкода	кількісна характеристика ризику, що відображає втрату працездатності (повну або часткову) або випадки загибелі людини при виникненні надзвичайної події і яка вимірюється її кількістю, зокрема зі смертельними наслідками за певний період часу.

На рисунку 1.3 показано логічний взаємозв’язок наведених вище термінів

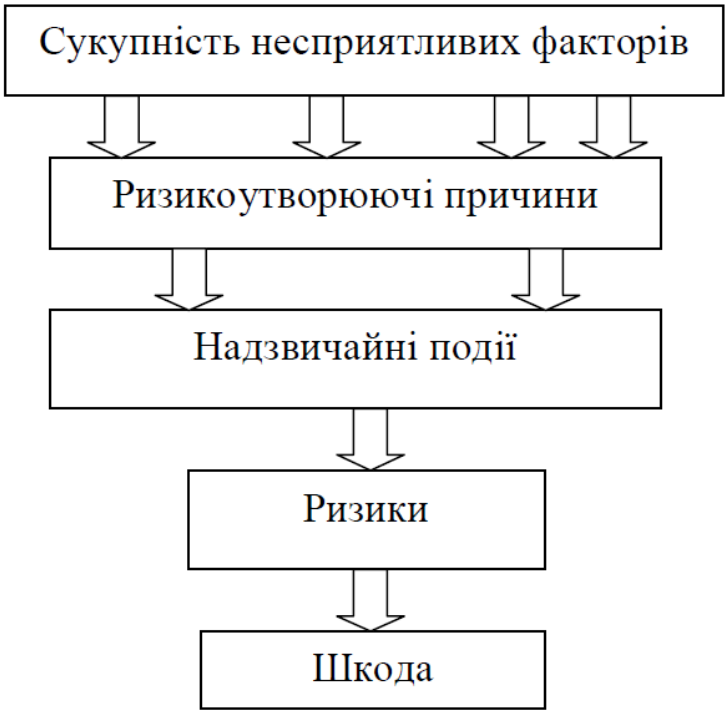

Рис 1.3 Взаємозв'язок понять, які обумовлюють кількіснухарактеристику ризику

Таким чином, проаналізований комплекс понять, дозволяє більш точно та повно визначити характеристики, що обумовлюють виникнення подій і являють собою основу щодо методологічного забезпечення та процедури оцінювання ризику згідно чинних нормативно-правових документів.

1.3. Методи аналізу ризику

На рисунку 1.4 наведено основні методи, які використовуються для аналізу ризику.

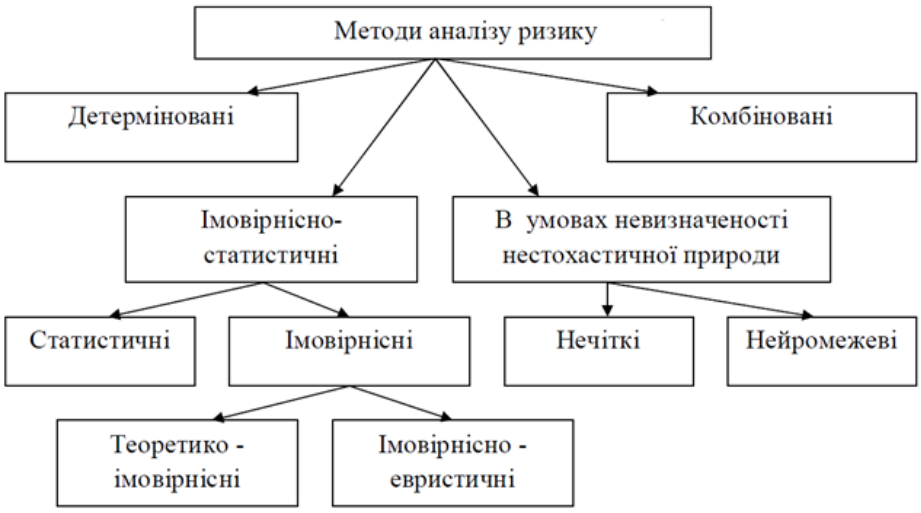

Рис. 1.4 Методи аналізу ризику

Як видно з рисунку дані методи поділяються на: детерміновані, ймовірнісно-статистичні, комбіновані, та ті що застосовуються в невизначеності нестохастичної природи. Розглянемо більш детально кожен з них.

Детерміновані методи базується на певній кількісній диференціації та розподілі надзвичайних ситуацій та наслідків надзвичайних ситуацій. Вони передбачають аналіз етапів розвитку подій від вихідної до кінцевого результату. Недоліками цих методів є: потенційна можливість упустити ланцюжки розвитку події; складність побудови достатньо адекватних математичних моделей; необхідність проведення складних і дорогих експериментальних досліджень.

Ймовірнісні методи є більш прогресивними. Це пов'язано з тим, що вони дозволяють знаходити оптимальний варіант рішення, який базується на кількісній залежності між небезпечними факторами та ймовірністю їх реалізації. Тобто дозволяють знаходити оптимальні технічні рішення для конкретних об’єктів.

Ймовірнісно-статистичні методи припускають як оцінку ймовірності виникнення несприятливої події, так і розрахунок відносної ймовірності того або іншого шляху розвитку процесу. При цьому аналізуються розгалужені ланцюжки умов і факторів, вибирається відповідний математичний апарат і оцінюється повна ймовірність. Розрахункові математичні моделі при цьому можна істотно спростити в порівнянні з детермінованими методами.

Методи аналізу ризиків в умовах невизначеностей нестатистичної природи,

як правило застосовуються для опису невизначеності джерела ризику, що пов’язано з відсутністю або неповнотою інформації.

Вище наведені методи поділяються на якісні та кількісні . В ході проведеного аналізу до детермінованих якісних методів було віднесено:

1. Що буде, якщо…? (What – If?), перевірочний лист (Check – List) або їх комбінація. Ці два методи є найбільш простими, дешевими і ефективними при дослідженні добре вивчених об’єктів з відомою технологією або об’єктів з незначним ризиком.

2. Попередній аналіз небезпеки (Process Hazard and Analysis) (PHA) – це індуктивний метод аналізу, метою якого є ідентифікація небезпек, які можуть завдати шкоди діяльності, об’єкту або системі.

3. Аналіз вигляду і наслідків події (Failure Mode and Effects Analysis) (FMEA) – застосовується для кожного окремого елементу (блоку, виробу, устаткуванню) або його частини ще до моменту несправності (вид або причина відмови) і яким був б вплив відмови на систему.

4. Аналіз помилкових дій (Action Errors Analysis) (AEA) – моделювання умов і обставин, щодо скоєння помилкових дій(відтворення всієї послідовності та умов діяльності).

5. Концептуальний аналіз ризику (Concept Hazard Analysis) (CHA).

6. Концептуальний огляд безпеки (Concept Safety Review) (CSR).

7. Аналіз людських помилок (Human Hazard and Operability) (Human HAZOP) – структурований і систематичний огляд планованого або існуючого процесу або діяльності з метою виявлення й оцінювання проблем, які можуть становити небезпеку для персоналу або обладнання, або перешкоджають ефективній роботі.

8. Аналіз впливу людського чинника (Human Reliability Analysis) (HRA) – залежність працездатності людини від багатьох факторів, таких як вік, душевний стан, фізичне здоров’я, стосунки, емоції, схильність до певних загальних помилок

9. Логічний аналіз.

До кількісних детерміованих методів віднесено:

1. Ранжирування (експертні оцінки).

2. Методика визначення і ранжирування ризику (Hazard Identification and Ranking Analysis – HIRA) – виявлення і аналіз небезпек, їхніх масштабів, наслідків та ідентифікація небезпек, оцінка ризиків і контроль для ефективного управління небезпеками.

3. Аналіз вигляду, наслідків і критичності події (Failure Mode, Effects and Critical Analysis) (FMECA) – застосовується для аналізу проектів складних технічних систем або при модифікації небезпечних виробництв.

4. Кількісне визначення впливу людського чинника (Human Reliability Quantification) (HRQ)– сукупність засобів аналізу частот у сфері впливу людини на показники роботи системи.

5. Методика аналізу ефекту доміно (Methodology domino effects analysis).

6. Методика визначення та оцінки потенційного ризику (Methods potentialrisk determination and evaluation)– процес кількісної оцінки рівня ризику, пов’язаного з конкретною небезпекою.

До ймовірнісно-статистичних якісних методів відносяться: карти потоків; причини послідовності нещасних випадків (Accident Sequences Precursor) (ASP); експертне оцінювання; метод аналогій для визначення сценаріїв розвитку аварій.

В свою чергу до кількісні ймовірнісно-статистичних відносяться: контрольні карти; аналіз дерева подій (Event Tree Analysis) (ETA); аналіз дерев відмов (Fault Tree Analysis) (FTA); оцінка ризику мінімальних шляхів від ініціюючого до основної події (Short Cut Risk Assessment) (SCRA);дерево рішень; бальні оцінки; суб’єктивні оцінки вірогідності небезпечних наполягань; узгодження групових рішень на підставі коефіцієнтів конкордації;методи попарних порівнянь.

В умовах невизначеності нестатичної природи до якісних методів відносять: метод аналізу небезпеки і працездатності (Hazard and Operability Study) (HAZOP, а також методи, що засновані на розпізнаванні образів (нечітка логіка тощо).

До кількісних методів, що застосовуються в умовах невизначеності статичної

природи відносять: методи прогнозування порушень, відмов (нейронні мережі прямогорозповсюдження, рекурентні); методи, засновані на розпізнаванні образів для ідентифікації передаварійних ситуацій (нейронні мережі адаптивного резонансу).

До комбінованих якісних методів відносяться: логіко-графічні методи аналізу ризику; аналіз максимальної можливості виникнення нещасного випадку (Maximum Credible Accident Analysis) (MCAA); блок-схема надійності (Reliability Block Diagram) (RBD); аналіз безпеки (Safety Analysis) (SA); аналіз надійності структури (Structural Reliability Analysis) (SRA); таблиці полягань і аварійних поєднань.

До комбінованих кількісних методів в ході дослідження віднесенно: повний аналіз ризику – методика оптимального аналізу ризику (Optimum Risk Analysis) (ORA);комплексний підхід до вибору оптимального методу аналізу ризику; метод організованого систематичного аналізу ризику (Method Organised Systematic Analysis Risk) (MOSAR); кількісна оцінка ризику (Quantitative Risk Assessment).

Ймовірнісно-евристичні методи використовуються при недостатніх статистичних даних і у разі рідкісних подій, коли можливості вживання точних математичних методів обмежені через відсутність достатньої статистичної інформації. Вони ґрунтуються на використовуванні суб’єктивної інформації, що одержана за допомогою експертного оцінювання. Застосування методів залежить від стадії аналізу ризику і цілей дослідження. Вони можуть застосовуватися незалежно або на додаток один до одного.

Також існують інші методи, які використовують у процесі аналізу та оцінки ризику на різних всіх етапах життєвого циклу. Це відомості перевірок, загальний аналіз відмов, моделі опису наслідків, індекси небезпек, метод Монте-Карло, метод Делфі, аналіз Маркова, мозковий штурм, структуровані і напівструктуровані інтерв’ю, аналіз небезпечних чинників і критичних точок управління, аналіз корінної причини, аналіз рівнів надійності засобів захисту, мережі Бейєса, матриці наслідків/ймовірностей тощо.

Метод Делфі дозволяє скоротити розкид експертних оцінок шляхом

встановлення зворотного зв’язку між кінцевими результатами досліджень і думками експертів.

Метод Монте-Карло ґрунтується на визначенні стохастичних параметрів, тобто на визначенні випадкових чисел, і використовується тоді, коли існує необхідність вибору найбільшої ймовірності ризику або вірогідності помилки.

Аналіз Маркова ґрунтується на лінійних диференціальних рівняннях, що встановлюють можливі збої через певний період часу.

Таким чином застосування вищенаведених методів дозволяє своєчасно реагувати на фактори (чинники), що обумовлюють ризики діяльності будь-якої сфери національної економіки у тому числі і складні організаційно-технічні системи. Вибір методу залежить від об’єкту досліджень, його життєвого циклу та умов виробництва і експлуатації.

У стратегії розвитку міжнародної організації зі стандартизації на 2021-2030 рр. Наголошується, що найважливішим компонентом щодо підвищення якості та безпечності продукції (послуг) є стандарти. Зокрема це стосується стандартів, що пов’язані з оцінюванням ризиків та безпеки. Наприклад у стандарті IEC 60812:2018 [13] наведено процедури, які стосуються аналізу режимів відмов та ефектів (FMEA), у т.ч. і варіантів відмов, ефектів та аналізу критичності (FMECA).

Слід зазначити, що метою аналізу режимів відмов та ефектів (FMEA) є встановлення, як елементів або процесів, що не виконують свою функцію, так і заходів щодо їх поліпшення. Таким чином FMEA це системний метод, який дозволяє виявляти відмови разом з їх наслідками як для локальних об’єктів та процесів, так і для глобальних. Він також дозволяє визначати режими відмов, що є пріоритетним для розроблення та впровадження рішень стосовно запобігання небезпек.

У випадку, якщо рейтинг критичності має досить великий ступінь тяжкості наслідків застосовується метод критичності (FMECA). Зокрема це стосується обладнання, програмного забезпечення, процесів, включаючи дії людини, та їх інтерфейсів у будь-якій комбінації.

В останню редакцію стандарту [13] внесено суттєві зміни. Зокрема додано: приклади програм для безпеки, автомобілебудування, програмного забезпечення та (сервісних) процесів; альтернативні способи обчислення числа пріоритетів ризику (RPN); метод, що заснований на матриці критичності та надано зв'язок з іншими методами аналізу надійності.

На практиці досить часто застосовують метод аналіз дерева відмов (FTA) [14] та дослідження небезпеки та працездатності (HAZOP) [15]. Ці методи побудовані на дедуктивному підході в основу якого покладено неодноразові запитання: як це може статися(конкретна небажана подія), і які причини цієї події? Тобто він включає логічну схему, яка показує зв'язок між компонентами системи та їх відмовами.

У [9] наведено переваги та недоліки методу FTA. Перевагами FTA є можливість одночасного аналізування декількох причин відмови. Таким чином комбінація застосування двох цих методів (FTA та HAZOP) дозволяє враховувати усі ризики.

HAZOP – це якісний прийом, який зазвичай використовується на етапі планування розвитку системи. Він визначає небезпеки, шляхом виявлення відхилення від специфікації конструкції системи і використовується для виявлення критичних аспектів з методою їх подальшого аналізу. Для його застосування створюється мультидисциплінарна команда з 5-6 аналітиків на чолі з керівником. Команда HAZOP визначає різні сценарії, які можуть призвести до небезпеки або експлуатаційної проблеми, а потім визначаються та аналізуються їх причини та наслідки .

Існує багато методів щодо оцінки ризику, у т.ч. моделі та варіації, що розроблені для конкретних цілей. Порядок оцінювання залежить від багатьох факторів: джерела інформації для оцінки, історії відмов, оцінки експертів тощо. При дослідженні та оцінюванні ризиків спочатку розглядаються основні елементи (концепція ризику, перспектива ризику, невизначеність, неоднозначність та складність).

У випадку, якщо існує невизначеність даних, то причинно-наслідкове

формулювання може бути описано та оцінено за допомогою ймовірнісних методів. При цьому доцільно застосовувати байєсівські мережі або марковські процеси. У деяких випадках [16] немарківські процеси можна подавати у вигляді марківських шляхом розширення їх «поточного» і «майбутніх» станів. Таким чином для опису невизначеності («ризику»), доцільно використовуються ймовірнісні методи.

"Небезпека" – це стан і ризик, що виражає ймовірність (або іншу невизначеність), пов'язану з режимом відмов. Залежно від умов наслідки можуть бути серйозними.

В [17] наведено підходи щодо формалізованого поєднання байєсівської мережі (BN) та стохастичної мережі Петрі (SPN). Поєднання цих двох методів дозволяє постійно оновлювати прогноз щодо відмов.

В роботі [18] для аналізу динамічної поведінки систем запропоновано використовувати метод STPA. В основу цього методу покладено модель системи, яка складається з діаграми функціонального контролю і базується на теорії систем. Він розглядає безпеку як проблему контролю (обмеження) системи, а непроблему відмови компонента. Перевагою STPA є ефективність.

За даними [11], метод STPA враховує взаємодії компонентів системи та розглядає оцінену систему та її компоненти як сукупність взаємодіючих контурів управління. Тому його застосування вимагає схеми структури управліннядля аналізу небезпек, що складається з компонентів системи та їх шляхів управління, а також зворотного зв'язку, тобто підтвердження.

Метод STPA застосовується у два етапи. На першому етапі визначають потенціал неадекватного контролю за системою, який в подальшому може призвести до її небезпечного стану. На другому – визначають за рахунок чого може відбутися потенційно небезпечна контрольна дія (тобто проводять пошук причинних факторів). Неадекватна контрольна дія може призвести систему до небезпечного стану. Наприклад, не застосовується необхідна контрольна дія; застосовується небезпечна (неправильна) контрольна дія; управлінська дія застосовується занадто рано або занадто пізно (неправильний час або

послідовність); дія керування зупиняється занадто рано або застосовується занадто довго. Під терміном «застосовується» слід розуміти правильну передачу дії управління або наказу від одного компонента системи до іншого.

Таким чином для застосування STPA необхідно мати функціонально-структурну схему управління системою та всі цикли управління в системі, що ідентифікуються з нею. Крім того для кожного циклу управління потрібно ідентифікувати всі компоненти, які сприяють небезпечній поведінці системи, що досліджується. До цих компонентів відноситься: давачі та виконавчі механізмів, які являють собою потенційні фактори ризику. Для оцінки таких факторів ризику використовується кілька методів. Наприклад, кількісна оцінка ризику (QRA), аналіз дерева подій (ETA), підхід матриці ризиків (RMA) та підхід на основі показників (IBA) тощо. При цьому одним із найбільш ефективних методів оцінки факторів ризику є метод моделювання структурних рівнянь, що дозволяє оцінити зв'язки із прихованими змінними [19].

Слід зазначити, що розвиток засобів зв'язку та інформаційних технологій стирають просторові межі між об'єктами взаємодії з одного боку, а з іншого – ускладнюють їх організаційну і функціональну структуру. Отже, інтеграція технічної та організаційно-інформаційної структури призводить до ускладнення організаційно-технічних структур, якість та ефективність функціонування яких залежить як від технічної компоненти, так і від організаціїсистеми.

Висновки до першого розділу

1. Проаналізовано поняття «ризику» та доведено, що останнє потрібно розглядати в форматі «ризик-ймовірність-невизначеність». Такий підхід дозволяє враховувати три аспекти, зокрема ймовірність нанесення збитків, певну подію чи сукупність подій та певний об’єкт прояву.

2. Нормативно-правова база щодо оцінювання ризиків складається із законів, постанов, спеціальних методик та стандартів, що побудовані на ризик-орінтованому підході.

3. Запропоновано для оцінювання ризиків застосовувати якісні і кількісні методи аналізу. Останні поділяються на детерміновані, ймовірнісно-статистичні, комбіновані та методи, що використовуються в умовах невизначеності і нестохастичної природи.

РОЗДІЛ 2 ТЕОРЕТИЧНІ ОСНОВИ ОЦІНЮВАННЯ РИЗИКІВ СКЛАДНИХ ОРГАНІЗАЦІЙНО-ТЕХНІЧНИХ СИСТЕМ

2.1 Структурні складові організаційно-технічних систем та їх властивості

Складна організаційно-технічна система (СОТС) – це ієрархічний людино-машинний комплекс, який в процесі функціонування реалізує його властивості, щодо досягнення мети для якої його було створено. Під метою слід розуміти бажаний результат діяльності, який досягається в межах деякого інтервалу часу [21]. Необхідний результат, як правило, отримують шляхом перетворення енергетичних, інформаційних та інших ресурсів. Такий підхід дозволяє перетворити ресурси у потрібну продукцію (послугу).

На практиці складна організаційно-технічна система являє собою ієрархічну систему, що утворена множиною елементарних організаційно-технічних систем. При цьому організаційна складова системи охоплює спосіб взаємозв'язку і взаємодії між елементами СОТС. Вона поділяється на постійну (інваріантну) та змінні частини. Перша частина визначає структуру організаційно-технічної системи, а друга - програму її функціонування [20]. За вертикальним поділом ця складова має дві підсистеми: керуючу і керовану. В свою чергу технічна складова являє собою матеріальні засоби виробництва, комунікації тощо. Вона поділяється на основні та допоміжні складові. Об'єкти, що не входять в СОТС, є зовнішнім середовищем. Проте вони можуть впливати як на саму СОТС, так і на ресурси або результат її функціонування. В цілому зовнішні фактори визначають випадковий характер умов її функціонування і застосування. В роботі [21,22] наведено у вигляді матриці фактори, що впливають як на умови функціонування СОТС, так і її елементів (рис. 2.1).

	Види діяльності та небезпек	Вторинні прояви небезпек	Витяг підземних вод	Введення матеріалу (рідини)	Видалення рослинності	Зміна сільського	Урбанізація	Будівництво (навантаження) інфраструктури	Інфраструктура (навантаження)	Заповнення грунтом	Будівництво водосховища та	Дренаж та зневоднення	Додавання води	Хімічний вибух	Горіння (пожежа)
		Первинні прояви небезпек	1	5	6	7	8	9	11	12	13	14	15	16	17
1.	Надземні	Витяг підземних вод													
2.		Видобуток нафти / газу	з	з			д, з	д, з	д, з					з	
3.		Будівництво підземної інфраструктури								з, п		д, з		з	
4.		Надземний видобуток	з				д, з	д, з	д, з	з, п	д, з	д, з		з	
5.		Введення матеріалу (рідини)						д, з	д, з						
6.	Використання площ	Видалення рослинності					п								
7.		Зміна сільського господарювання	з, п		д, з		п					д			д, з
8.		Урбанізація	з, п	з, п	д, з	з, п		д, з, п	д, з, п	д	д, з, п	д	з, п		
9.	Видобування	Будівництво інфраструктури			д		п		з, п	п		д, з		з	
10		Видобуток корисних копалин / поверхні	з		д		д, з	д, з	д, з	з, п	д, з, п	д, з		з	
11	Завантаження	Інфраструктура (навантаження)			д		з, п	д, з, п							
12		Заповнення грунтом					п		п						
13		Будівництво водосховищ та дамб						д, з	д, з, п						
14	Над і підземні	Дренаж та зневоднення	п				п		п				з, п		
15		Додавання води										з, п			
16		Хімічний вибух								п					
17		Горіння (пожежа)													

Рис. 2.1 Фактори впливу на функціонування СОТС і її елементів.

Як видно з рис. 2.1 дана матриця дозволяє проаналізувати ступінь взаємодії та їх вплив на систему безпеки СОТС. Таким чином матриця взаємодії та часова класифікація взаємодій небезпек (потенційних ризиків) дозволяє виявити ці взаємодії, які потрібно враховувати при визначенні впливу небезпечних процесів на СОТС. Тобто часовий код, що пов’язує вторинний небезпечний процес (що відкладений по горизонталі) з первинними небезпечними процесами (який відкладений по вертикалі). Кожна з клітин матриці включає в себе часовий код, що

описує чи відбувається пов’язаний з цим вторинний небезпечний процес до (Д), під час (З), або після (П) первинного небезпечного процесу. У комірці (Д) ідентифіковані зв’язки, показано одна, дві або три з цих літер.

Схема функціонування елементарної СОТС наведено на рис.2.2.

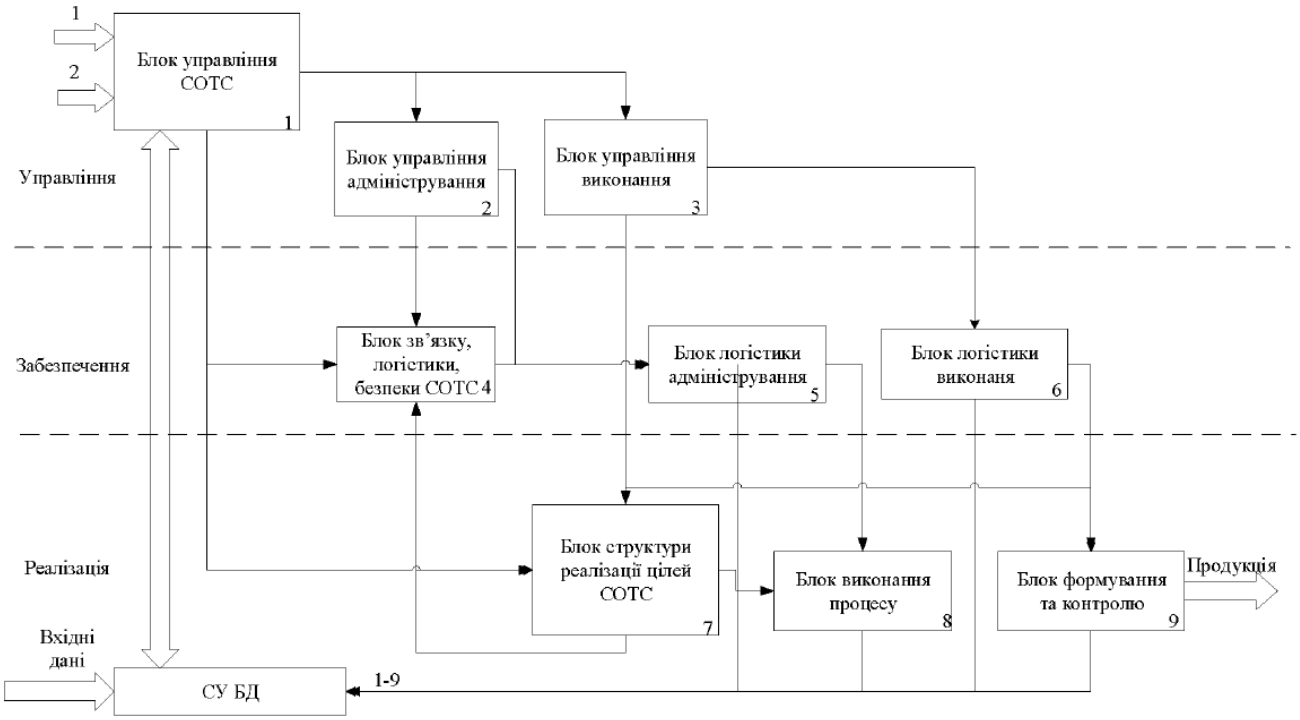

Рис. 2.2 Функціональна схема управління СОТС

Під якістю СОТС слід розуміти якість її будови. Тобто її властивості залежать тільки від властивостей об'єктів (елементарних ОТС), які створюють єдине ціле.

Таким чином, якість СОТС – це властивість або сукупність властивостей, які обумовлюють її придатність для застосування за призначенням на різних етапах життєвого циклу [23].

Аналіз літературних джерел [24, 25] доводить, що існує співвідношення понять безпеки і ризику щодо управління якістю. Зокрема це стосується таких понять як «безпека, безпечність, небезпека, ризик, загроза». Наприклад, характеристикою безпечності продукції (виробів, процесів, послуг з точки зору їх технічного забезпечення) є її якість як узагальнюючий критерій.

Одним із ефективних механізмів щодо підвищення безпеки є застосування стандартів ISO як до продукції так і робіт, які підвищують її якість. Зокрема побудови систем управління якістю за вимогами міжнародних

стандартів.

Існує досить багато трактувань поняття безпеки як ризику. Наприклад, ISO/IEC надає розробникам стандартів рекомендації щодо аспектів безпеки. Останні пов’язані з людьми, власністю або навколишнім середовищем, або комбінацією одного чи декількох з них. Тобто вони застосовують підхід, що спрямований на зменшення ризику, який виникає внаслідок використання продуктів, процесів або послуг [26].

Слід зазначити, що безпека має першочергове значення для потенційних споживачів продукції. Тому в міжнародних та національних стандартах пропонується для забезпечення безпеки застосовувати ризик орієнтовані підходи. Крім того більшість стандартів вимагають розроблення механізмів та інструментів щодо оцінювання ризиків продукції метою яких є демонстрації відповідності вимогам безпеки.

Безпека складної організаційно-технічної системи являє собою стан при якому ризик виникнення небезпек і спричинення ними шкідливих наслідків знаходиться на прийнятному рівні. Це забезпечується завдяки тому, що частина відомих небезпек для об'єкта відсутня, а від наявних небезпек існує адекватний захист.

Безпека характеризується низкою складних властивостей. До найбільш важливіших відносяться такі як економічність і ефективність.

Ефективність - властивість, що характеризує пристосованість процесу функціонування (застосування) СОТС щодо досягнення мети. У випадку, якщо корисний ефект проявляється у формі настання деякої події (явища), тобто має якісний характер, то і його величина теж є якісною та оцінюється за допомогою значень бінарної шкали (І-ефект має місце, 0- ефект відсутній). У випадку, якщо корисний ефект проявляється у формі речовини, енергії, інформації або настання сукупності цих подій, то його величина є кількісною і вимірюється за шкалою відношень або абсолютною шкалою. На рис 2.3 наведено шкалу ефективності оцінювання СОТС.

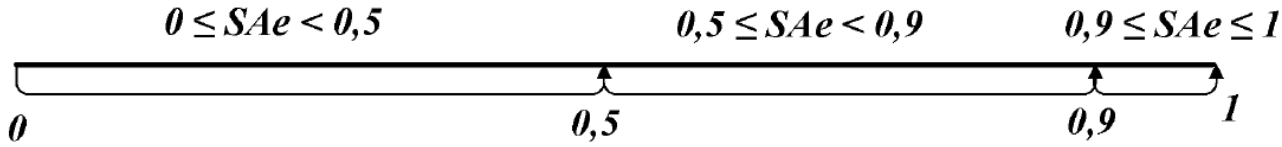

Рис. 2.3 Відносна шкала ефективності оцінювання СОТС,

де SAe = 0 – процес оцінювання функціонує неефективно і потребує докорінного перегляду;

0<SAe≤0,5 – процес оцінювання функціонує неефективно, потребує розроблення значних контролюючих дій;

0,5<SAe≤0,9 – процес оцінювання функціонує ефективно, але для його покращення потрібно розробити незначні коригуючі дії;

0,9<SAe≤1 – процес оцінювання функціонує ефективно, але для його покращення потрібно розробити запобіжні дії;

SAe>1 – процес оцінювання функціонує ефективно і не потребує втручання.

Економічність являє собою властивість, що характеризує раціональність використання ресурсів в процесі їх перетворення в результат [26]. Вона оцінюється у величині якісного характеру і може бути відображена відносною шкалою (рис 2.4):

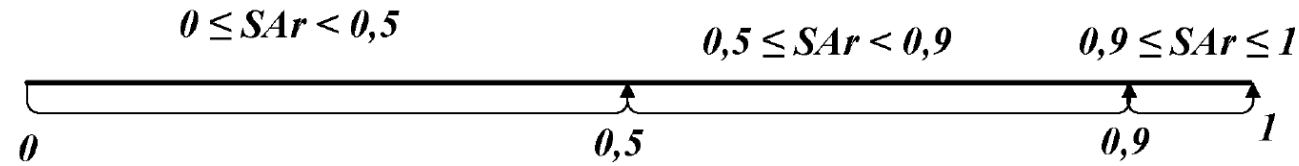

Рисунок 2.4 – Відносна шкала результативності оцінювання СОТС,

де SAr = 0 – процес оцінювання не функціонує і потребує докорінного перегляду;

0<SAr<0,5 – процес оцінювання функціонує не результативно, потрібно розроблення значних коригувальних дій;

0,5≤SAr<0,9 – процес оцінювання функціонує результативно, проте вимагає розроблення незначних коригувальних дій;

0,9≤SAr<1 – процес оцінювання функціонує результативно, проте вимагає розроблення запобіжних дій;

SAr=1 – процес оцінювання функціонує результативно і не потребує втручання.

Проведені дослідження доводять, що існують різні підходи щодо ризику, відповідних типів доказів та методів аналізу .

Один із підходів вважає, що ризик є фізичною властивістю, яку можна охарактеризувати об'єктивними фактами. В основу такого підході покладено величини, отримані в результаті технічного аналізу, як уявлення про цю фізичну властивість. Цей підхід розглядає ймовірнісний аналіз ризику (PRA) як інструмент для оцінки "справжнього" ризику. Інший підхід передбачає, що ризик це конструкція, а ймовірність аналізу ризику це інструмент формалізації суджень щодо ризику. Тобто існує два підходи в контексті щодо перевірки ймовірності аналізу ризику: реалістичне тлумачення та суб'єктивне тлумачення.

Для першого підходу вірогідність - це вимірювання фізичної властивості, а для другого – ймовірність це аргумент, а не інструмент для розкриття щодо суті ризику. Проте більш важливими ніж ймовірність є такі поняття як: типи доказів, що лежать в основі суб'єктивної міри невизначеності та аргументи, що наведено для присвоєння певної ймовірності.

В [27, 28] наведено аналіз ризиків, що базується на доказах інтуїції досвіду та правдоподібного припущення.

Для оцінювання безпеки СОТС необхідно визначити: перелік тих властивостей, сукупність яких достатньо для її характеристики, числові значення, що отримано шляхом вимірювання, випробування та підрахунку. Отриманий таким чином результат буде з достатнім ступенем достовірності характеризувати безпеку СОТС.

Безпека готової продукції визначається двома факторами – якістю розроблення та якістю створення продукції. При цьому більш вагомим є фактор створення продукції, який пов’язаний з безпекою і ризиками її виготовлення.

Для реалізації принципів рикик-орінтованого підходу щодо управління безпекою СОТС потрібно враховувати всі етапи її життєвого циклу (рис. 2.5).

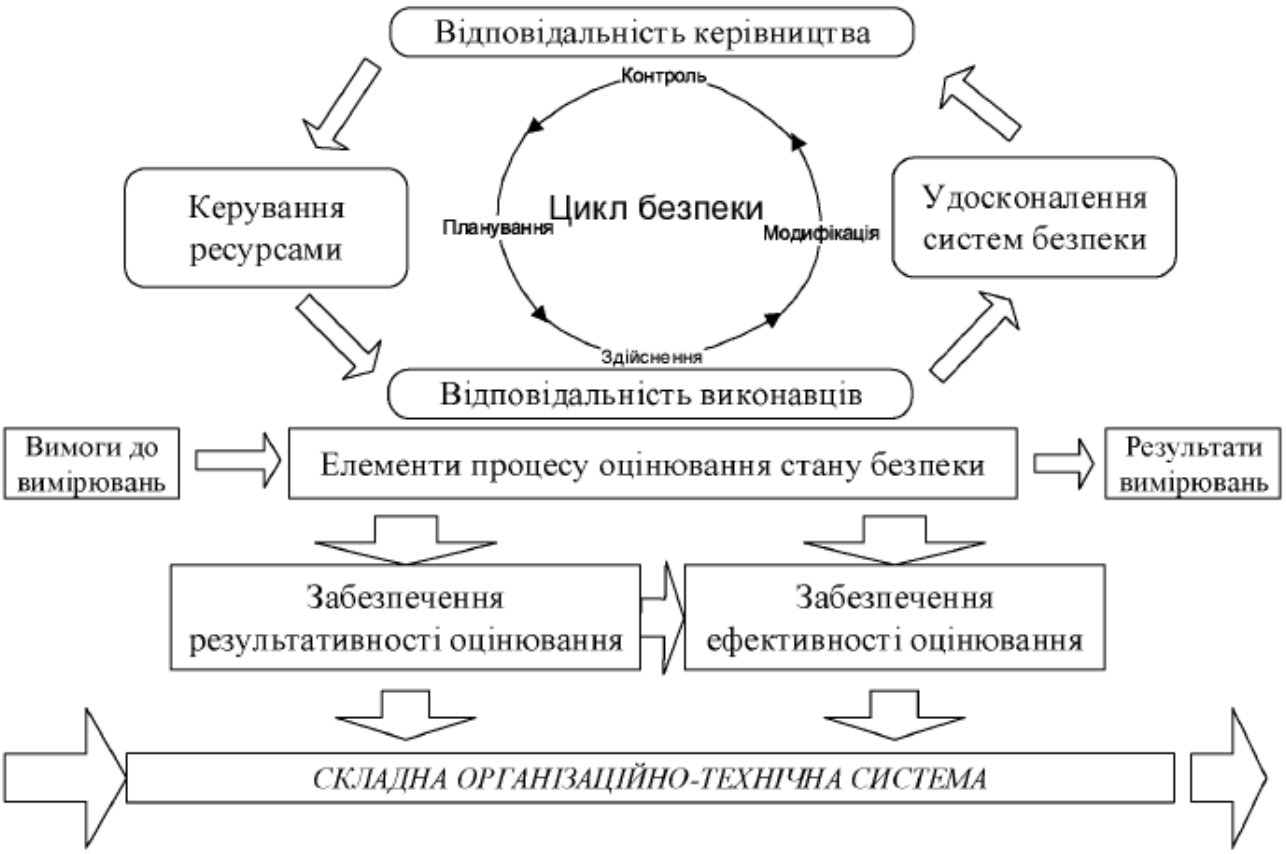

Рис. 2.5 Модель життєвого циклу безпеки складної організаційно-технічної системи

Як видно з рисунку основні процеси у моделі (рис.2.5) – це планування, ідентифікація і аналіз небезпек та ризиків, вибір методів і планування необхідних дій; здійснення, виконання запланованих заходів щодо системи безпеки; модифікація: розроблення рішення на основі отриманих оцінок та внесення коригуючих дій; контроль – оцінювання результатів здійснення заходів з безпеки та виявлення невідповідностей.

Таким чином на основі вище наведеного доцільно оцінювати безпеку продукції, процесів та послуг та здійснювати ефективне управління протягом усього життєвого циклу безпеки СОТС. При цьому також може проводитись діагностика функціонального стану продукту (устаткування), оперативне виявлення причини погіршення встановлених вимог до безпеки об’єктів, що досліджуються і методичне вдосконалення робіт.

Будь-який об'єкт в процесі експлуатації (споживання) знаходиться у взаємозв'язку з середовищем та з людиною тобто існує система «людина-

середовище-об’єкт». Взаємозв’язки між елементами цієї системи наведено на рис. 2.6.

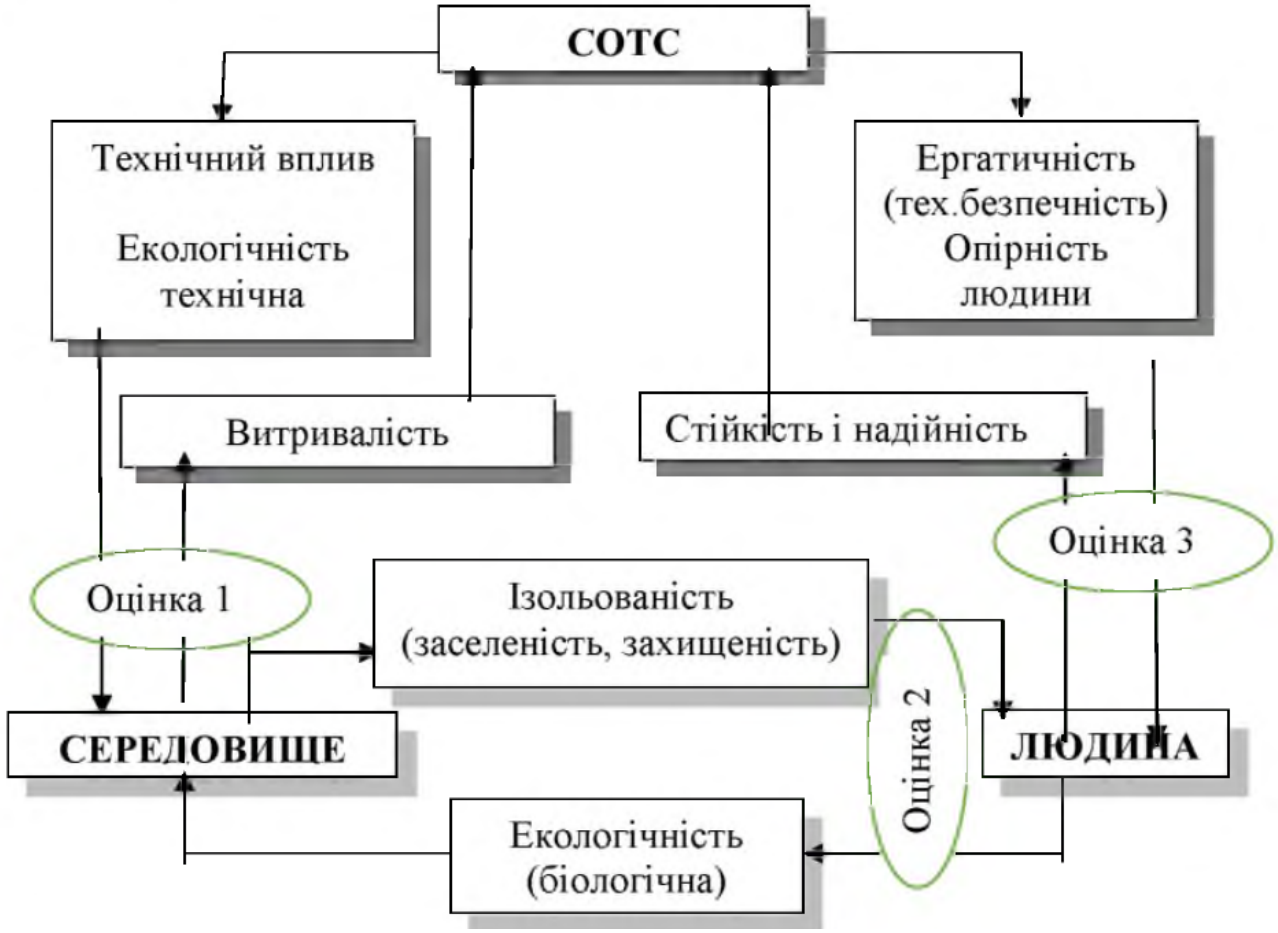

Рис. 2.6 Взаємозв'язок елементів системи «людина-середовище-об'єкт»

Як видно з рис. 2.6 сукупний вплив на середовище з боку і СОТС (екологічність технічна), і людини (екологічність біологічна) визначається як екологічність. Вплив на людину з боку СОТС (ергономічність - безпека) і з боку середовища (ізольованість-захищеність) визначається як безпечність.

Таким чином комплекс наведених зв'язків дозволяє виявити основні напрями щодо оцінювання безпеки СОТС.

2.2. Ризик-орієнтовані підходи щодо оцінювання складових організаційно-технічної системи складних організаційно технічних систем

Проведений аналіз доводить, що процедури контролю якості методів аналізу ризиків на даний час недостатньо розроблені. Зокрема це стосується критеріїв якості PRA [29], а також валідації в процесі аналізу ризиків. Одним з

підходів згідно [26]стосовно питань валідації PRA в системах із низьким ступенем ймовірності події та з високою шкодою є те, що модель ризику повинна мати наступні рішення: у випадку якщо зацікавлені сторони в ситуації прийняття рішення не мають заперечень проти припущень моделювання, даних, експертних суджень та зроблених висновків, то аналіз ризиків слід вважати достатнім. Типові підходи щодо аналізу ризиків наведено в таблиці 2.1.

Таблиця 2.1

Обгрунтованість PRA за різних підходів [28].

Підхід до PRA	V1	V2	V3	V4
1 Традиційний статистичний аналіз, великий обсяг відповідних даних	Так	-	-	Так/Ні
2 Традиційний статистичний аналіз в інших випадках	Ні	-	-	Так/Ні
3 Ймовірнісний частотний та байєсівський підходи щодо оцінки неспостережуваних параметрів	Ні	Так/Ні	Так/Ні	Так/Ні
4 Баєсові підходи прогнозування спостережуваних параметрів	-	Так/Ні	Так/Ні	Так

Згідно табл. 2.1 перевірка PRA полягає в переосмислені критеріїв дійсності V2, V3 і V4 [27]. При цьому у випадку якщо експерт здатний перетворити сприйняті невизначеності, що пов'язані з величиною, у міру ймовірності (V2), за умови що всі невідомі величини враховані в моделі ризику (V3), і якщо потрібні величини адресовані для того, щоб застосувати прийняті критерії ризику (V4), то PRA діє як інструмент системи підтримки прийняття рішень (СППР).

Таким чином, наслідком прийняття реалістичних або конструктивістських рішень для перевірки аналізу ризиків можна вважати наступне. Для реалістичних – це спроба підтвердити, що оцінки близькі до «істинного» значення, а для конструктивістких рішень – валідація ґрунтується на виборі зроблених тверджень про ризик, тобто є напівформальним, розмовним та аргументованим процесом.

Існують різні методи щодо валідації ймовірнісного ризику. В основу одного з методів щодо оцінювання якості аналізу ризику покладено контрольний

список. Оцінка базується на документації аналізу. Остання повинна бути досить детальною. Рішення щодо повноти врахування всіх аспектів аналізу залишається за оцінювачем. Наприклад, не пропонуються конкретні методи, які можуть бути або повинні застосовуватися; передбачається, що оцінювач має необхідні знання щодо застосовних методів та критеріїв для відбору. Інший метод стосується важливості спостережуваних недоліків. Він передбачає оцінювання впливу відсутніх або дефектних факторів на оцінку ймовірності несприятливої події та її наслідків. Метод не включає процедури ранжування для визначення пріоритетів аспектів. Рішення формуються на виваженому судженні оцінювача[28].

У національних та міжнародних стандартах наведено підходи щодо забезпечення якості. При цьому особлива увага приділена ефективності їх застосування щодо зворотного зв'язку з клієнтами. Тобто зворотного зв'язку з PRA критичної ситуації, яку зазнавали користувачі.

Одним із важливих питань є те, що PRA часто сприймають як надмірну концентрацію уваги на технічних питаннях аналізу. При цьому занадто мало уваги приділяють виявленню потреб користувачів, обробленню інформації та питанням комунікації. Баланс у діяльності, пов'язаний з дослідженням PRA, може бути досягнений за рахунок застосування процесу контролю якості.

Для забезпечення узгодженості аналізів PRA у різних підрозділах СОТС, технічна система якості повинна бути побудована на принципах ієрархії. Тобто вона повинна мати документи, що стосується питань філософія компанії, потреби споживача, методи роботи та культура безпеки [39]. Рекомендації стосуються методів та стратегій для проведення різних типів досліджень, зокрема детальні інструкції щодо використання окремих інструментів PRA (моделі, дані, параметри тощо) [29].

В роботі [30] наведено принципи побудови анкети для забезпечення якості та оцінювання валідності моделей для розрахунку наслідків основних небезпек. Вона базується на п'яти концепціях: наукове забезпечення якості, алгоритмічне забезпечення якості, забезпечення якості комп'ютеризації,

забезпечення якості інтерфейсу людина-машина та перевірка моделі на аналіз чутливості.

В [31] наведено модель валідації, в основу якої покладено модель процесу щодо типового аналізу ризику. Ці процеси включають: надання ресурсів, встановлення контексту, виявлення небезпечних результатів, побудову моделей, оцінку ризику, оцінку ризику, планування дій та передача результатів.

Поняття та принципи встановлення обґрунтованості, а також рамки та методи перевірки методів аналізу ризиків та їх результати є важливими елементами для зміцнення розуміння предмету аналізу ризику [26]. Наприклад, для розробників систем є PRA як інженерний метод, який дозволяє обґрунтовано убрати процедури контролю якості аналізу ризиків.

Згідно з визначенням ризику як «невизначеність щодо тяжкості подій та наслідків діяльності стосовно того, що цінують люди»[4], існує чотири підходи до PRA: традиційний статистичний аналіз, частота ймовірності [28] та байєсівські підходи (оцінка неспостережуваних параметрів, що орієнтується на основний дійсних ризиків та спостережуваних), не фокусуються на базовому справжньому ризику [32]. В даному випадку застосовують чотири критерії дійсного підходу:

V1. Ступінь точності отриманих цифр у порівнянні з основним справжнім ризиком.

V2. Ступінь, до якого призначені суб'єктивні ймовірності адекватно описують невизначеності оцінювача щодо невідомих розглянутих величин.

V3. Ступінь завершення епістемічної оцінки невизначеності.

V4. Ступінь, в якому аналіз враховує правильні величини.

Густина розподілу ймовірності – це теоретичне поняття, що трактується у випадку, якщо розглянута ситуація може повторюватися знову і знову. Проте для ризику безпеки вона не завжди доречна. Це пов’язано з тим, що в умовах безпеки, події часто мають унікальні характеристики. Тобто вони охоплюють як безпеку так і охорону [33].

Для концептуалізації ризику використовують параметр часу. На рис. 2.7

наведено модель, що пов’язує ризик, джерела ризику, події та наслідки.

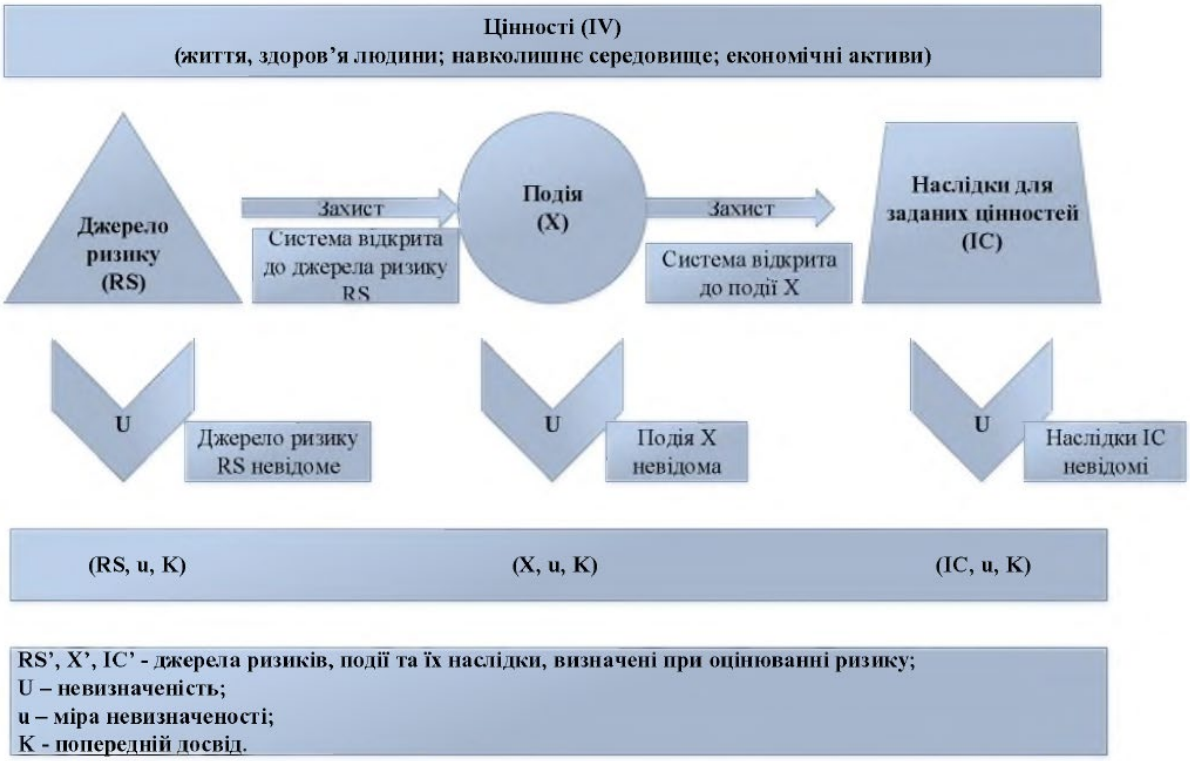

Рис. 2.7 Модель, що пов'язує ризик, джерела ризику, події та наслідки ((RS, X, IC) - фактичні джерела ризику, події та наслідки та (RS', X' та IC') - джерела ризику, події та наслідки, зазначені в оцінці ризику.

Як видно з рис. 2.7 невідомо, які події X насправді відбудуться і якими будуть наслідки, оскільки стосовно цього існують невизначеності U. Джерела ризику також можуть піддаватися невизначеності. На даному рисунку "U" виражає невизначеність того, які джерела ризику будуть реалізовуватися, і які при цьому будуть відбуватися події X та які будуть наслідки IC. Тобто, U посилається на стан невизначеності щодо RS, X та IC.

Відповідно до теорії вимірювань розрізняють поняття ризику та спосіб вимірювання або опису ризику. В оцінці ризику надають опис (характеристику) майбутнього, а також вказують RS', X' і IC' джерел ризику, подій та наслідків, а також міру (u) для опису або вимірювання невизначеності (U), пов'язаних з ними.

Якщо обмежуватись фактичною наявністю або появою RS чи події X, то ми маємо поняття вразливість. Тобто сукупність наслідків діяльності та пов'язаних з нею невизначеностей.

Для моделі ймовірнісного аналізу ризику СОТС потрібно описати або

виміряти вразливість форми (IC', u, K I RS' / X'), тобто ризик, що описано через (IC', u, K), який залежать від виникнення джерела ризику RS' або події X'. Як правило подання невизначеності [34] подають у вигляді аксіоми, інтерпретації, процедури.

На рисунку 2.8 наведено узагальнену схему валідації ймовірнісного аналізу ризиків.

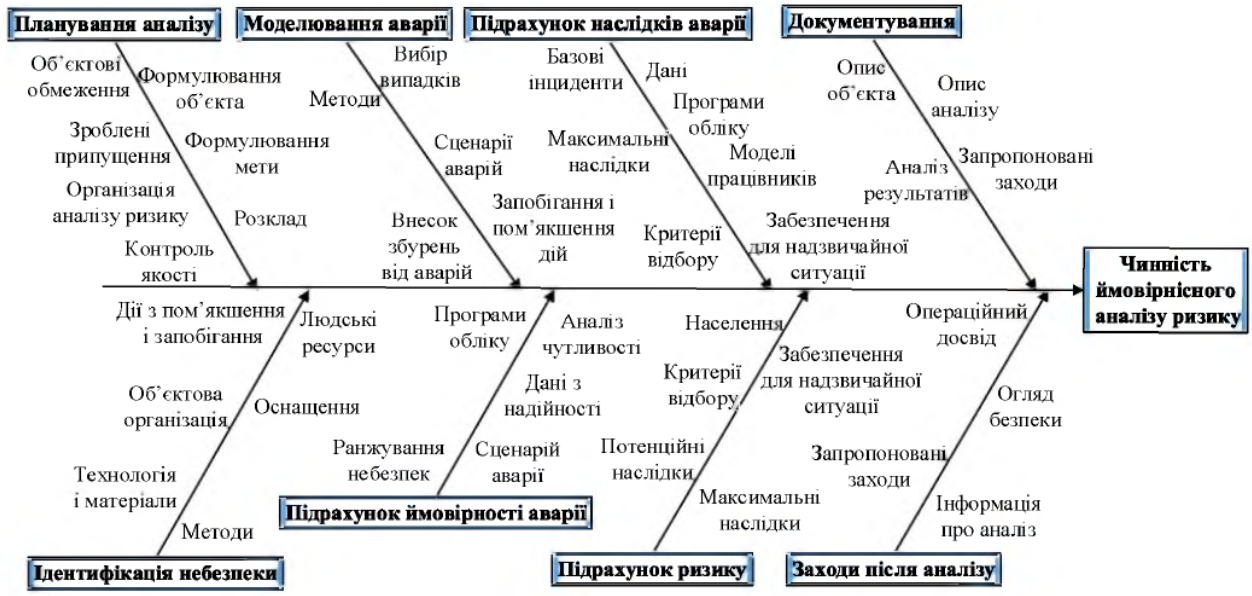

Рис.2.8 Узагальнена схема валідації ймовірнісного аналізу ризиків.

Основним питанням щодо прагматичної обгрунтованості PRA є використання аналізу. Емпірично визначити точність PRA неможливо: «один із найпотужніших наукових методів - експериментальні спостереження - непридатний для оцінки загального ризику» [30]. Передумовою точності є надійність: умова, що при повторному вимірюванні результати є "подібними".

Вимога про економічну корисність означає, що виконання PRA забезпечує перевагу для безпеки, яка є значно вищою, ніж передбачена методами, які не покладаються на кількісну оцінку. Це потрібно для відстеження змін ризику з часом. Цілком імовірно, що обізнаність про шляхи, в яких система може вийти з ладу, знання про домінуючі сценарії захисту системи, фактори, що сприяють виходу з ладу, інформацію про безпеку, що отримано при виконанні PRA надає переваги для управління ризиками. При цьому кількісна оцінка допомагає процесу, навіть якщо цифри є не досить точні.

В умовах практичної реалізації моделі валідації застосовується експертний

метод. При валідації враховують оцінки структури моделі, змісту, дискретизації, параметризації та поведінки. Даний метод використовують для прийняття обґрунтованого рішення щодо придатності PRA для використання.

В таблиці 2.2 наведено приклади категорій норм для перевірки PRA.

Таблиця 2.2

Приклади категорій норм для перевірки PRA, [1, 28]

Категорія норми	Пояснення	Приклад норми
Повна	Залучення всіх важливих елементів та проблем	Переконайтесь, що не пропущено випадковості, оскільки вони є суперечливими або не піддаються кількісній оцінці
Досвідчена	Опирається повністю на наявні знання	Не покладайтесь на оцінювачів ризику, які працюють в організаціях
Обґрунтована	Ґрунтується на відповідних даних та судженнях	Не слід використовувати статистичні дані, які не диференціюються за основними причинами відмов
Інтегрована	З' єднання частин в ефективне ціле	Переконайтесь, що оцінка ризику включає знання, які розділені на багато частин
Системна	Робота з взаємодіями та системами в іншому	Аналізуйте системні якості, такі як складність та зв'язок, а не прогнозуйте детальні послідовності подій
Напрямна	Допомога людям, які використовують оцінку, в її ефективному застосуванні	Покажіть, як процеси оцінювання ризиків підвищують обізнаність та перевіряють припущення, а не забезпечують певний результат
Відкрита	Бути відкритим щодо проблем і скромним щодо досягнень	Визнайте можливу відсутність даних про причини, які лише нещодавно з'явились як причини
Консультативна	Залучення зацікавлених сторін та врахування проблем	Слід широко оглядати на робочому рівні,у т.ч. нібито неавторитетні джерела знань
Своєчасна	Отримати результати досить швидко, щоб за ними можна було діяти	Проводьте оцінювання досить рано, щоб вплинути на проект рішення, які можуть бути скасовані дорогою ціною
Доступна	Зрозуміло людям із натовпу	Забезпечте прості способи переходу від висновків до аналізу та припущень
Допоміжна	Забезпечує допоміжні підстави для опрацювання ризиків	Тестуйте культуру волевиявлення в організації в питаннях дій задля аналізу ризиків

В [58] наведено сучасні підходи, щодо аналізу ризику. Зокрема пропонується динамічний аналіз, при якому картина ризику постійно оновлюється з появою нової інформації. Це забезпечує прийняття більш ефективних рішень та підвищує безпеку СОТС.

На рис. 2.9 наведено схему повторного процесу оцінювання ризику та

зменшення ризику.

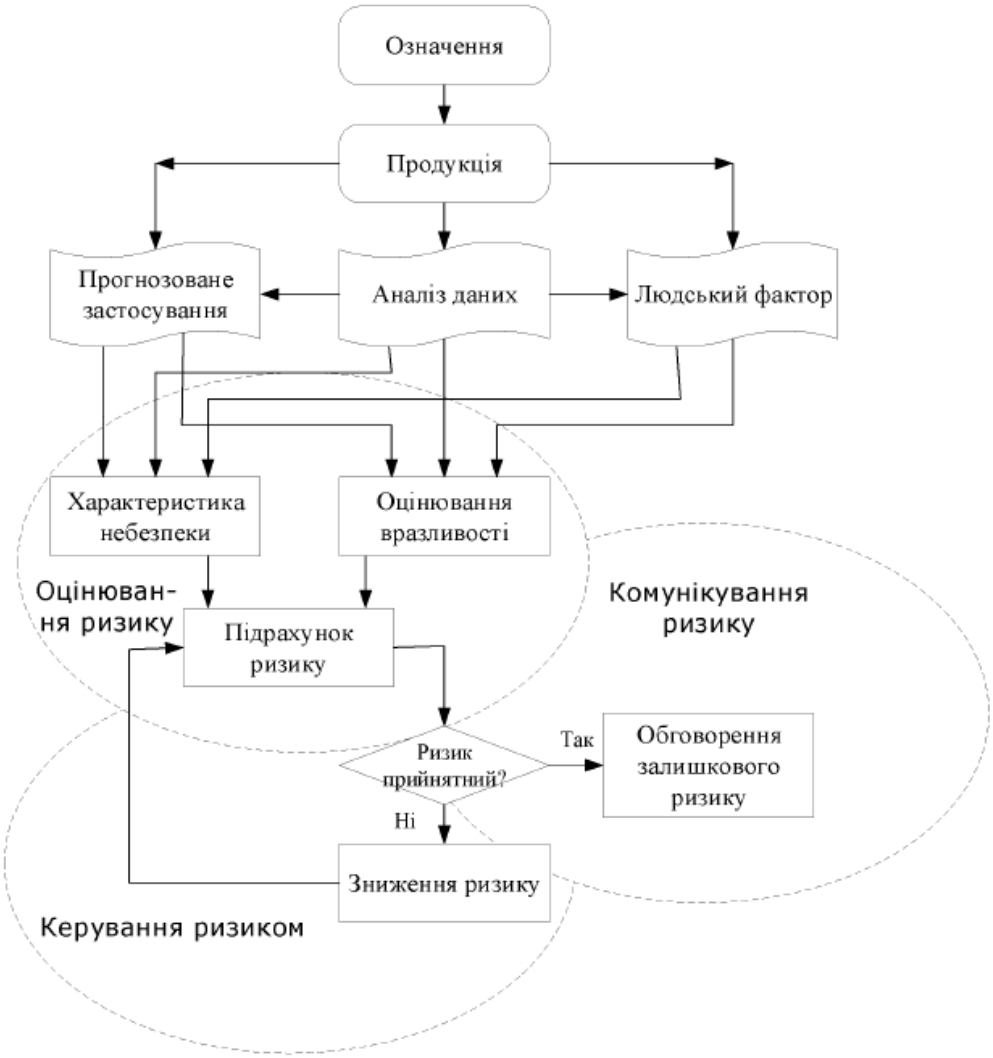

Рис. 2.9 Повторний процес оцінки ризику та зменшення ризику

Як видно з рис. 2.9 ризик складається з двох різних складових – небезпеки та вразливості. Ризик може створюватися або генеруватися під час виробництва або виробничого процесу.

Які б аспекти безпеки не охоплював стандарт, вони повинні бути зрозумілі постачальникам, дизайнерам, консультантам, технічним працівникам, фабричним робітникам та субпідрядникам. Пропозиція повинна наголошувати на необхідності дати вказівки щодо чіткого умовного підходу, що базується на результатах, до аспектів безпеки при розробці стандартів.

Виходячи з визначення «шкідлива подія» згідно [35], це поява такої обставини, при яких люди, майно чи навколишнє середовище піддаються дії одного або декількох небезпечних ситуації щодо потенційного джерела шкоди

(небезпеки), який призводить до фізичної травми або пошкодження здоров'я людей, або майна або навколишнього середовища.

Тому інструкції та інформація, що надаються, повинні охоплювати безпечні умови експлуатації продукції (процесу або послуги). Наприклад, що стосується продукції, інструкція повинна охоплювати використання, вплив на навколишнє середовище, очищення, технічне обслуговування, демонтаж та знищення / утилізацію. Тобто безпека є першорядною цінністю для споживачів.

Для створення більш безпечнішого споживчого середовища потрібно ефективніше використовувати керівництва, стандарти та ресурси оцінки відповідності. Тому оцінка ризику та безпека мають першочергове значення в стандартах та інших нормативних документах. Наприклад Guide ISO / IEC 51 визначає основні аспекти безпеки при розробці нормативних документів всіх рівнів та категорій. Дані рекомендації побудовано на підході, що спрямований на зменшення ризику і охоплює повний життєвий цикл продукту (процесу та послуги).

Сьогодні при аналізі ризиків враховують три основних компоненти. Це оцінку ризику, управління ризиками та інформування щодо ризику. Оцінка ризику, як правило, проводиться шляхом характеристики ризиків та оцінки вразливості. Управління ризиками - це усталена дисципліна. Визначення ризиків включає запитання, що, чому, де, коли і як може виникнути небезпека. Підходи, що використовуються для виявлення ризиків, включають в себе контрольні списки, судження (засновані на досвіді та записах), блок- схеми, методи мозковий штурм та аналіз сценаріїв тощо.

Існують також альтернативи ймовірності [39] для представлення та вираження невизначеності в оцінці ризику. Один з варіантів стосується того, що суб'єктивна ймовірність не підходить. При цьому часто зустрічається одна аргументація: якщо фонові знання досить слабкі, то буде складно або неможливо з певним рівнем впевненості вказати суб'єктивну ймовірність. Проте завжди можна призначити суб'єктивну ймовірність. Проблема полягає в тому, що призначена суб'єктивна ймовірність відображається набагато сильніше, ніж можна

обґрунтувати і тому для неї використовують інтервальні ймовірності [40].

При оцінці ризику метою є не лише нейтрально представлені наявні знання, а й висловлення переконання експертів, тому ймовірність для цього є корисним інструментом. Таким чином ймовірність та альтернативні підходи доповнюють один одного.

Якщо суб'єктивні ймовірності використовуються для вираження невизначеності, то потрібно приділяти увагу знанням, які їх підтверджують. Наприклад, можуть бути дві ситуації. Одна, коли сума знань, щодо ймовірності, значна або незначна, а друга, коли сила знань слабка, при цьому ймовірності можуть бути однаковими [36]. Цим обґрунтовано невизначеності, які на додаток до ймовірностей також включають характеристику суми знань, що визначають ймовірність.

Таким чином небезпека СОТС вимірюється за ймовірністю відмови будь-якого елементу. При цьому наслідки можуть бути включені як якісні характеристики важливості складної організаційно-технічної системи.

2.3 Стандартизовані заходи щодо управління безпекою в процесах розвитку складних організаційно-технічних систем

Для прийняття рішень щодо зменшення ризиків, тобто підвищення рівня безпеки СОТС міжнародною організацією зі стандартизації розроблено ряд нормативних документів. Це ISO 9001:2015 Системи управління якістю. Вимоги [37], ISO 18091:2019 Системи управління якістю. Керівництво по застосуванню ISO 9001 в органах місцевого самоврядування [38], ISO 37120:2018 Сталі міста та громади. Показники міської служби та якості життя [39], ISO 31000 Управління ризиками. Керівні принципи [40], IEC 31010 Керування ризиком. Методи загального оцінювання ризиків [41], ISO 22301:2012 Безпека суспільства. Системи менеджменту неперервюстю діяльності. Вимоги [42], ISO 20121:2012 Системи управління стійкістю подій. Керівництво для використання [43], ДСТУ ISO/IEC 25000:2016 Вимоги до якості систем і програмних засобів та її оцінювання

(SQuaRE) [44].

Для цілей управління у сфері акредитації й сертифікації застосовується серія стандартів ISO 17000: ISO/IEC 17000:2004 (словник), ISO/PAS 17001:2005 (вимоги), ISO/PAS 17002:2004 (конфіденційність), ISO/PAS 17003:2004 (скарги й апеляції), ISO/PAS 17004:2005 (розкриття інформації), ISO/PAS 17005:2008 (застосування систем управління), ISO/IEC 17007:2009 (підготовка нормативних документів) , ISO/IEC 17011:2004 (акредитація), ISO/IEC 17020:2012 (органи з інспектування), ISO/IEC 17021:2011 (аудит), ISO/IEC TS 17022:2012 (звіт стосовно аудиту), ISO/IEC 17024:2003 (персонал), ISO/IEC 17025:2005 (компетентності випробувальних та калібрувальних лабораторій), ISO/IEC 17030:2003 (знаки відповідності), ISO/IEC 17040:2005 (взаємне визнання), ISO/IEC 17043:2010 (кваліфікація лабораторій), ISO/IEC 17050-1:2004 (відповідальність), ISO/IEC 17050-2:2004 (підтверджувальна документація), ISO/IEC 17065 (сертифікації продукції, процесів і послуг).

Відповідно до міжнародного стандарту ISO IEC 31000:2018 [41], ризик - це ефект невизначеності цілей, можливість того, що деякі події можуть мати негативний вплив на певні цілі. В свою чергу оцінка ризиків, як складова частина управління ризиками, є структурованим процесом для виявлення ризиків та їх впливу на досягнення цілей компанії. В форматі цього процесу ризики аналізуються як з точки зору їх наслідків, так і у зв'язку з вірогідністю їх виникнення. Такий підхід дозволяє організації (підприємству) приймати адекватні рішення щодо зменшення або усунення негативних наслідків ризиків. На сьогодні широко використовується підхід щодо управління ризиками, опис якого наведено в [44] і який для спеціалістів відомий як "Рамка 7С".

На рис. 2.10 наведено структуру складових компонентів управління ризиком згідно з ISO IEC 31010:2013.

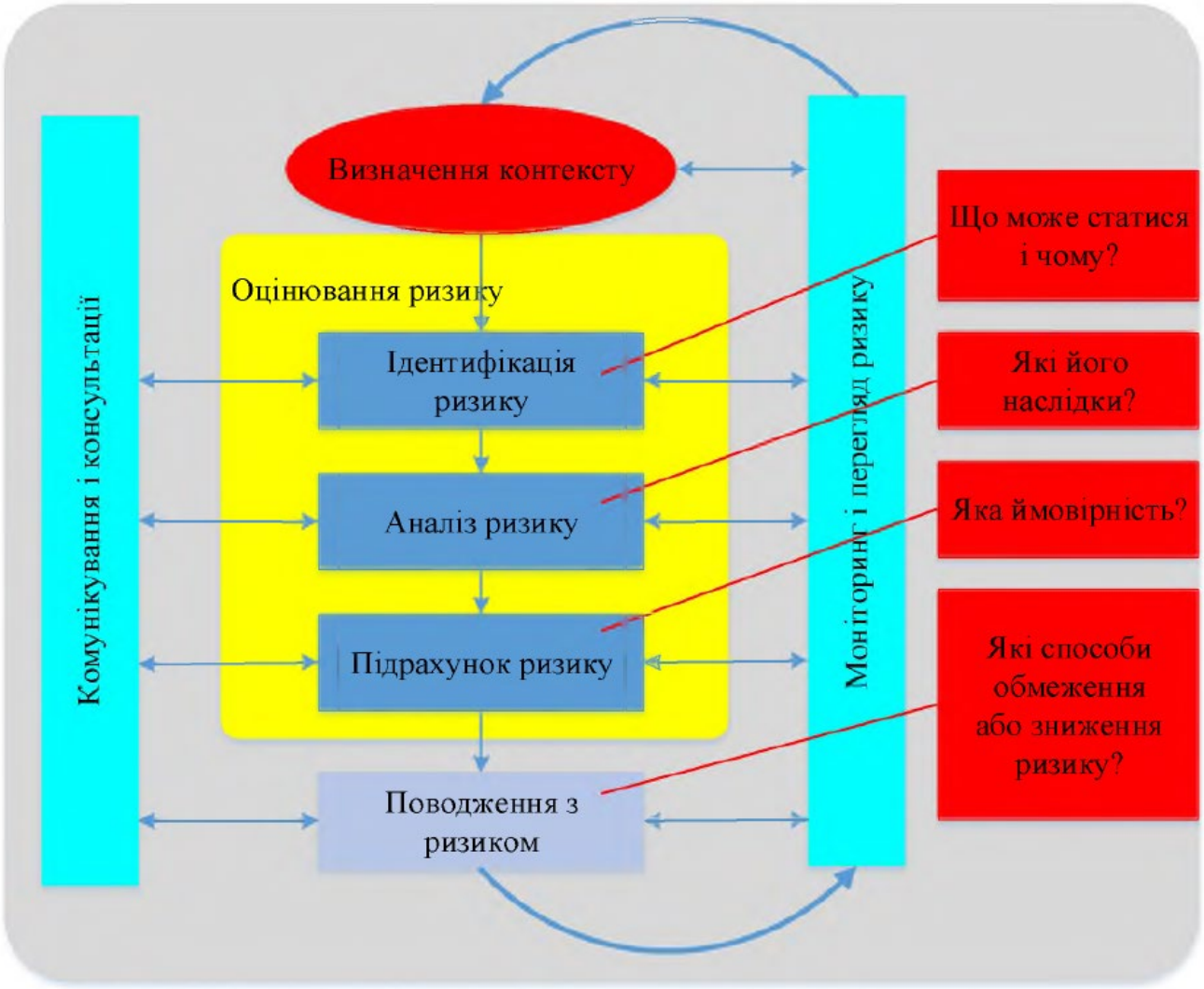

Рис 2.10 Структура складових компонентів управління ризиком згідно з ISO IEC 31010:2013

Як видно з рисунку проходження етапів ідентифікації ризиків, класифікації ризиків, складання реєстру ризиків та матриць ризиків під час аналізу ризиків проводиться за допомогою різних методів. При цьому для пыдвищення ефективності запропонованим стандартом методів в процесі аналізу може бути надана IT підтримка. Це дозволяє отримати правильні реакції на ризик. Визначальними факторами реакції на ризик є: можливий ефект ризику, частота, тобто ймовірність виникнення ризику та вартість заходів щодо його зменшення ризику [45-47]. На реакцію на ризик також впливає чутливість осіб, які приймають рішення щодо ризику. Висока чутливість до ризику забезпечує основу для більш повного розвитку, але нижчого рівня невизначеності. Низька чутливість до ризику має більш швидкий розвиток зі значно вищим рівнем невизначеності.

Таким чином, управління ризиками являє собою потужний інструмент, щодо прийняття рішень стосовно їх зменшення.

Першим етапом управління ризиками є ідентифікація ризику, оцінка потенційних небезпек, їх наслідків та ймовірності виникнення ризику. На цьому етапі, як правило, усувають ті ризики, які не відповідають цілям а також ризики з незначними наслідками або з дуже низькою ймовірністю виникнення. Ідентифікація ризиків проводилась з урахуванням як внутрішніх, так і зовнішніх факторів. Внутрішні ризики (на відміну від зовнішніх) - це ті ризики, які керівництво компанії тримає під контролем або може суттєво вплинути на них.

Відповідно до впливу ризиків та ймовірності їх виникнення, для складання ієрархії ризиків застосовується бальне оцінювання (табл. 2.3).

Таблиця 2.3

Ієрархія ризиків залежно від впливу та ймовірності виникнення

Вплив ризику і ймовірність виникнення	Рівень ризику (інтерпретація)	Класифікація ризику
Великий вплив і велика ймовірність виникнення. Великий вплив і середня ймовірність виникнення	Дуже висока. Це найбільші ризики, на які компанія повинна звертати особливу увагу.	A
Середній вплив і велика ймовірність виникнення	Високий. Ці ризики мають або велику ймовірність виникнення, або значний вплив	B
Середній вплив і середня ймовірність виникнення	Середнє. Існує середня ймовірність того, що можуть виникнути ризики зі значним впливом.	C
Середній вплив і мала ймовірність появи. Низький вплив і середня ймовірність появи	Низька. Ці ризики можуть виникати за певних обставин і мати низький або середній вплив	D
Низький вплив і мала ймовірність виникнення	Незначний. Це ризики з низькою ймовірністю виникнення та малим впливом. З цих причин їх можна ігнорувати.	E

Спосіб присвоєння оціночного ризику відповідно до ймовірності виникнення та впливу здійснюється на основі аналізу матриці ризиків (таблиця 2.4).

Таблиця 2.4

Матриця ризиків відповідно до ймовірності виникнення ризику та його впливу

Ймовірність виникнення ризику	Низький вплив (Незначний його лише потрібно зареєструвати)	Середній вплив (Розумний вплив, потребує моніторингу)	Високий вплив (Буде мати значний вплив)
Низька (менш ймовірно)	E	D	C
Середня (можливе виникнення у визначених межах)	D	C	B
Висока (ймовірно виникають)	C	B	A

Реєстр ризиків, їх оцінка та матриця ризиків являють собою первинні дані для виявлення та оцінки ризиків за допомогою методу моделювання, наприклад, Монте- Карло [48-49]. Метод Монте-Карло - це багатоітераційний статистичний метод, який базується на різних повторюваних сценаріях. В результаті застосування даного методу оцінюють вплив різних видів ризиків, визначають адекватні програми для зменшення ризиків та пріоритетність заходів щодо їх зменшення або усунення. Тобто розробляють «реєстр ризиків», який включає усі потенційні джерела ризику, враховує їх за видами та категоріями, а також робить оцінку щодо наслідків, які можуть спричинити ці ризики.

Відповідно до типології ризиків для проектів існують різні методи та рамки для оцінки та пом'якшення їх наслідків. Наприклад, екологічні ризики, як правило, не являють собою ризики, що впливають на терміни реалізації інвестиційних проектів. Проте вони мають значний фінансовий вплив в результаті впровадження заходів, необхідних для зменшення наслідків. Тому вони можуть вплинути на програму реалізації інвестиційних проектів. Для оцінки впливу екологічних ризиків за допомогою методу Монте Карло потрібно використовувати спеціальне IT-програмне забезпечення, наприклад майстер-PERT. Дане програмне забезпечення дозволяє провести багатоітераційний аналіз, щодо наслідків ризику [50]. При цьому багатоітераційний даний аналіз проводиться із врахуванням впливів на різні види проектних робіт та пов'язаних з ними ризики.

Вплив є змінною величиною і включається в основу розрахунку відповідно

до матриці ризиків та присвоєного оцінювання. В результаті аналізу отримують різні звіти, що показують оцінені ефекти з часової та фінансової точок зору та враховують ймовірність впливу різних ризиків.

Таким чином використання методу моделювання Монте-Карло для оцінки впливу ризику в цілому [51-53] та для екологічних ризиків зокрема, дозволяє встановити рівень невизначеності у досягненні запланованих ключових показників ефективності. Крім того застосування цього методу дозволяє встановити ризики та вплив цих ризиків на навколишнє середовище, технічні процеси, безпеку здоров'я та безпеку праці. Тобто впровадження системи управління безпекою СОТС повинно базуватися на використанні адекватних методів аналізу впливу ризику. Такий підхід є важливим інструментарієм щодо прийняття рішень стосовно розроблення, впровадження та експлуатації складних організаційно-технічних систем.

Висновки до другого розділу

1. Складна організаційно-технічна система являє собою ієрархічний людинно-машинний комплекс, який в процесі функціонування реалізує свої властивості і ресурси (енергетичні, інформаційні та інші) у потрібну продукцію (послугу). При цьому безпека СОТС, це стан при якому ризик виникнення небезпек і спричинення ними шкідливих наслідків знаходиться на прийнятому рівні.

2. Для оцінювання безпеки складної організаційно-технічної системи потрібно визначити перелік властивостей, що її характеризують та числові значення їх параметрів (показників) шляхом вимірювання, випробування та підрахунку.

3. Для аналізу ризику доцільно застосовувати принцип валідації суть якого полягає у виявленні небезпечних результатів щодо оцінки ризику. Для реалізації моделі валідації застосовуються експертні методи. При цьому враховують оцінки структури моделі, змісту, дискретизації, параметризації та поведінки.

4. При аналізі ризиків враховують три основні компоненти: оцінку ризику, управління ризиками та інформацію щодо ризику.

РОЗДІЛ 3
ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ СКЛАДНИХ ОРГАНІЗАЦІЙНО-ТЕХНІЧНИХ СИСТЕМ

3.1. Методика оцінювання безпеки життєвого циклу складної організаційно-технічної системи

До недавнього часу в промисловості включали необхідні заходи безпеки до базових систем управління технологічними процесами (СУТП). Для інтеграції системи СУТП розроблено кілька міжнародних стандартів зокрема IEC 61508 [54], IEC 61511[55], ANSI/ISA 84 [56]. Ці стандарти, особливо IEC 61508 та IEC 61511, є основними стандартами щодо життєвого циклу безпеки. Вони поширюються на вироби електротехніки, електроніки та програмованої електроніки (E/E/PE).

В основу даних стандартів покладено принцип щодо якого при порушенні процесу або відмові системи чи обладнання, система змогла б самостійно керувати безпекою процесу за допомогою системи управління на основі оцінки ризиків. Для цього система контролю безпекою повинна складатися з апаратної та програмної системи управління, яка застосовується для контролю об’єкту в його робочих межах. У випадку, коли на об'єкті виникає будь-який стан ризику, повинен спрацьовувати сигнал тривоги. Це дозволяє максимально зменшити всі види ризиків. Життєвий цикл безпеки, згідно зі стандартом IEC, являє собою циклічний процес або замкнуту петлю, що включає в себе циклічний спосіб підтвердження та ідентифікації аналізу за стандартом ISO/IEC 31010.

На рис. 3.1 наведено фактори, що обумовлюють ризики у форматі життєвого циклу безпеки.

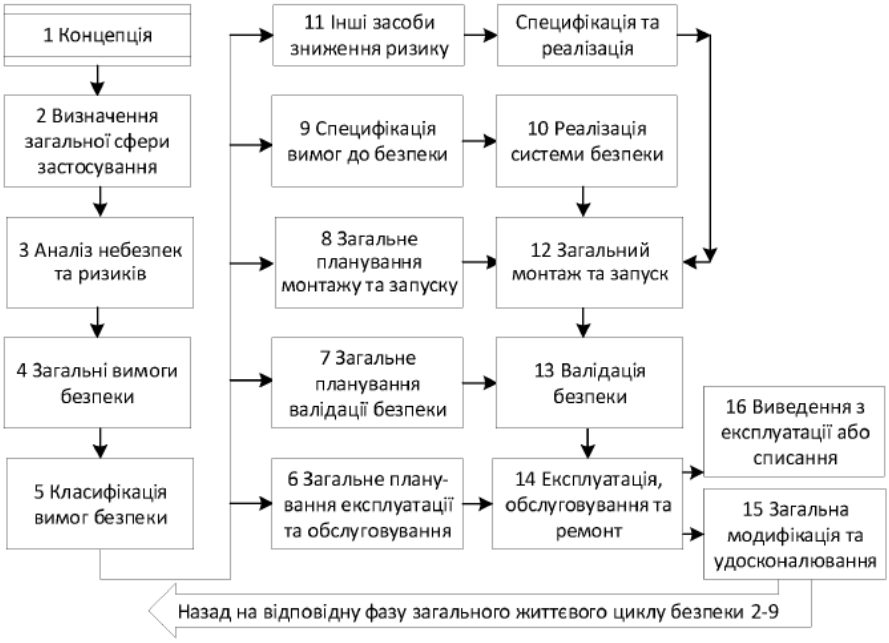

Рис. 3.1 Вплив на ризики у життєвому циклі безпеки

Відповідно до керівництва ISO / IEC 51, IEC 61508, ризик - це «поєднання ймовірності настання шкоди та тяжкості цієї шкоди». Звідси випливає, що ризик стосується ймовірності того, що небезпека може спричинити фактичну шкоду. Аварія - це небажана, незапланована (але не завжди може бути несподіваною) подія, яка призведе до певного рівня збитків (здоров'я, майна, виробництва тощо).

Необхідними елементами основної системи управління процесом і установкою (BPCS), яка забезпечує управління процесом та моніторинг процесу, відповідно до IEC 61511 є такі [57]:

1. Інструментальна система безпеки (SIS). SIS призначена для запобігання виникненню небезпечних подій шляхом переведення процесу в безпечний стан, коли у системі виникає заздалегідь визначений або заздалегідь встановлений стан. Це поєднання давачів, логічних розв'язувачів та кінцевих елементів управління. Наприклад, у програмованій електроніці (PE) складається як з апаратного, так із програмного забезпечення.

2. Інструментальна функція безпеки (SIF). SIF складається з давачів, логічних розв'язувачів та остаточної комбінації елементів управління. SIF переносить систему або процес у безпечну зону у випадку небезпечної ситуації /

події, яка визначається заздалегідь визначеними умовами процесу

3. Safety integrity level (SIL). Рівень цілісності безпеки - це показник ефективності SIS, що визначається ймовірністю відмови за запитом (PFD) для SIF (SIS). Існує чотири рівні SIL, представлені цифрами: SIL 1, 2, 3, 4. Чим вище число SIL, тим краща буде ефективність і нижчим буде значення PFD. Однак із збільшенням числа SIL вартість і складність системи зростають, а рівень ризику зменшується. Сертифікація SIL може бути видана компанією або іншим компетентним органом.

4. Ймовірність відмови за запитом (PFD). Це ймовірність того, що SIF / SIS не виконує передбачувану функцію безпеки під час потенційно небезпечного стану. PFDavg, як правило, використовується в розрахунках, коли COTC регулярно перевіряється та тестується.

Типовий макет SIS, який складається з давачів, кінцевих елементів управління та логічних розв'язувачів показано на рис. 3.2.

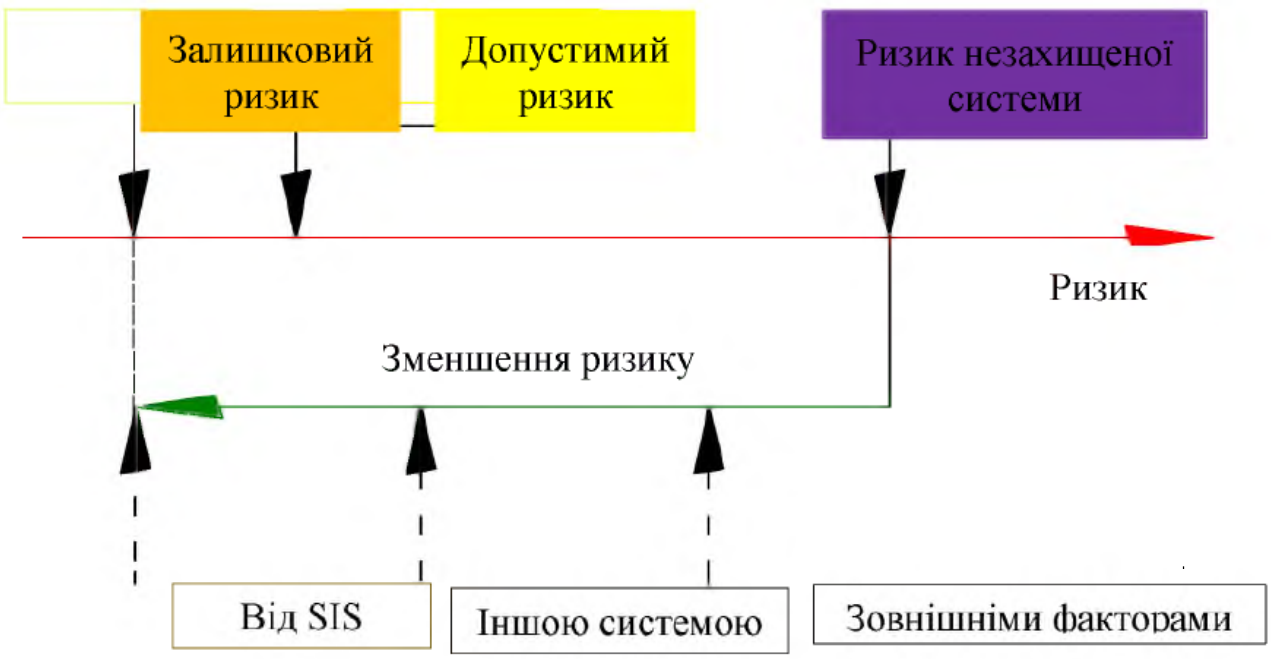

Рис 3.2 Типовий макет SIS, який складається з давачів, кінцевих елементів управління та логічних розв'язувачів [31].

Як видно з рисунку користувацький інтерфейс та інтерфейс з BPCS показано через комунікаційну шину. Слід зазначити, що BPCS та SIS можуть існувати окремо, або їх можна інтегрувати, якщо вони відповідають вимогам

міжнародних стандартів IEC 61508/61511 або ANSI / ISA 84.

Функціональна безпека є важливою складовою для життєвого циклу безпеки. Вона спирається на такі положення: усі процеси або виробничі системи мають властиві небезпеки; в усіх процесах або виробничих системах є властива кількість відмов, яка не може бути доведена до нульового значення; усі процеси або виробничі системи мають допустимий рівень відмов, не завдаючи шкоди системі. Для всіх процесів або виробничих систем показники відмов можна віднести до категорії SIL.

Розглянемо систему безпеки як загальний для даного виробництва процес, що об'єднує п+1 локальних підпроцесів, 15:і 5:п, кожен з яких має вхід Xi та вихід Yi. Враховуючи різноманітність можливостей побудови системи безпеки, виходи одних її підсистем, можуть бути входами інших підсистем чи зв'язків із метасистемою. В [55] показано, що існує деяка функція - J_{ss}, яку доцільно застосовувати для оцінювання процесу функціонування системи безпеки.

Будемо вважати, що метою функціонування системи безпеки є максимізація функції якості J_{SQ}, отримана шляхом ефективного погодження множини елементів J_i системи безпеки та множини зв'язків T_s між елементами системи безпеки.

Умову максимізації функції якості JSQ можна забезпечити шляхом оптимального використання наявних елементів та зв'язків, що еквівалентно, з точки зору системного аналізу [6, 7], прийняттюефективних управляючих рішень, які системи безпеки можна представити у виді множини рішень:

$$D_{M3} = \{D_1, D_2, \dots D_i, \dots D_{n+1}\} \rightarrow \text{opt} \qquad (3.1)$$

Вибираючи із множини можливих рішень D_{M3} оптимальні можна добитися максимізації функції якості J_{sQ} системи безпеки.

Типову структуру системи безпеки можна представити у виді трьохрівневої ієрархічної системи [58]. Перший рівень – це система безпеки – J_{sQ}, другий – підсистема забезпечення результативності заходів безпеки - J_R, та підсистема забезпечення ефективності безпеки - J_E. Третій – елементи: J_{ID} - забезпечення ідентифікації ризиків; J_{AA} - забезпечення відповідності оцінювань; J_{MA} -

стандартизація методик оцінювань; J_{TA} - забезпечення відповідності оцінювань; J_{ME} - метрологічна експертиза КД таТД; J_{MU} - державний ринковий нагляд; J_{GU} - державний контроль; J_{EQ} - кваліфікація фахівців; J_{DB} - організаційна структура безпеки.

Згідно [59] існує два основних принципи системного підходу. Це засоби досягнення мети, що визначаються самою метою та мета нижнього рівня системи, яка має бути засобами досягнення мети вищого рівня. Такий підхід забезпечує адитивність властивостей системи, що дозволяє провести лінійну згортку показників ефективності від нижніх рівнів до верхнього.

На рис. 3.3 наведено графічну модель системи безпеки.

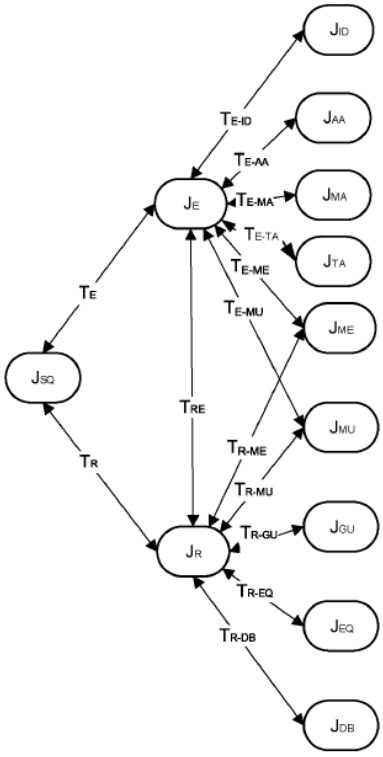

Рис. 3.3 Графічна модель декомпозиції системи безпеки СОТС

Як видно з рисунку дана модель дозволяє здійснити декомпозицію функцій елементів за ієрархічними рівнями та забезпечити обґрунтований аналіз та встановлення раціональних значень та співвідношень між показниками якості окремих елементів системи безпеки на стадії виготовлення продукції.

Умову максимізації функції якості J_{SQ} шляхом прийняття ефективних управляючих рішень (3.2) можна відобразити наступною формулою, яка також

відображає вплив функцій якості підсистем та елементів J_i на функцію якості.

$$J_{SQ} \xrightarrow{D \to opt} \sum_{i=1}^{n} T_i \cdot J_i = \sum_{i=1}^{n} T_i \cdot \sum_{j=1}^{m} T_{ij} J_{ij} \ , \tag{3.2}$$

де T_i - вага зв'язку і-ї підсистеми J_i; із J_{SQ}; T_{ij} - множина (вага) зв'язку j-го елемента з і-ю підсистемою.

Декомпозицію функцій якості системи безпеки здійснимо вважаючи, що ефективність елементів системи безпеки, в першу чергу визначається ефективністю перетворення входів x_{ij} (цілей) у виходи y_{ij}, що можна відобразити залежністю (3.3):

$$J_{ij} = e_{ij} \frac{x_{ij}}{y_{ij}} \xrightarrow{d_{opt}} max \ , \tag{3.3}$$

де e_{ij} – ефекти перетворення входів x_{ij} у виходи y_{ij} , що визначають якість виконання своєї функції окремим елементом безпеки.

На практиці для реальних систем безпеки досить важко однозначно визначити ефект перетворення входів x_{ij} у виходи $y_{ij.}$ Тому для вирішення цієї задачі використовують теорію вибору оптимального рішення.

Прийняття рішень передбачає наявність певної мети, на досягнення якої направлене рішення. Існування проблеми щодо прийняття рішення свідчить про те, що не всі рішення з множини D забезпечують досягнення мети. Виконаємо розбиття множини D на три підмножини [60]:

$$D = D^+ \cup D^0 \cup D^- \ , \tag{3.4}$$

де D^+ – «хороші рішення» (наближають до мети); D^- – «погані рішення», (віддаляють від мети); D^0 - "нейтральні рішення" (не впливають на досягнення мети).

Оптимальне рішення d_{opt} повинно належати до множини хороших рішень: daptED+. Задача прийняття рішення передбачає обов'язкове існування критерію Q прийняття рішення. В умовах сучасних технологій визначальним є відповідність рівню безпеки та забезпечення конкурентоздатності продукції, тому вектор оптимальних рішень повинен враховувати вектори пріоритетів

виробника - W_1 та контролю - W_2:

$$d_{opt} \in D^{+}_{W1} \cap D^{+}_{W2} \quad . \tag{3.5}$$

В даний час вектори пріоритетів виробника – W_1 та споживача – W_2 чисельно встановлюються у вигляді нормування ризиків виробника - α та споживача – β. Проте в умовах відсутності формалізованих методів встановлення зв'язку цих ризиків з безпековим ризиком втрати якості продукції створює додаткові труднощі щодо оперативного прийняття оптимальнго рішень. Тому для таких складних організаційно-технічних систем, таких як система безпеки, прийняття оптимальних рішень не може бути однократною дією, а має здійснюватися періодично із врахуванням зміни умов її функціонування.

Важливим завданням максимізації функції якості J_{SQ} є створення методики вдосконалення. Остання дозволить шляхом виконання ітераційних процедур дозволить оптимізувати ефективність системи безпеки при виконанні умов мінімізації безпекових ризиків споживача та виробника.

Для формалізації вимог до системи безпеки представимо узагальнене зображення елемента системи безпеки у вигляді моделі відношень (рис. 3.4).

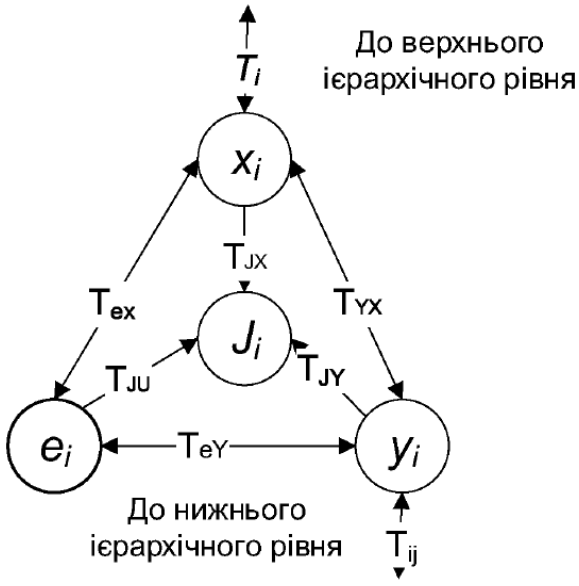

Рис. 3.4 Графічна модель відношень і-го елемента безпеки.

Тоді із врахуванням моделі відношень (рис. 3.2) функцію якості J_i і-го

елемента представимо у вигляді:

$$J_i = \left|T_{eX}, T_{Je}, T_{JY}\right| e_i \frac{x_i \cdot \left|T_{eX}, T_{JX}, T_{YX}\right|}{y_i \cdot \left|T_{eY}, T_{JY}, T_{YX}\right|} \tag{3.6}$$

Для складних систем важко однозначно врахувати вплив взаємозв'язків M_{ij} між x_{ij}, y_{ij}, e_{ij}, тому при побудові реальних систем необхідно мінімізувати вплив не основних зв'язків, забезпечуючи виконання умов:

$$\begin{aligned} &T_{eX}, T_{JX}, T_{JY}, T_{eY} \Rightarrow 0 \\ &T_{Je}, T_{YX} \Rightarrow set \end{aligned} \tag{3.7}$$

Тоді вираз (3.6) можна спростити до наступного вигляду:

$$J_i = T_{JE} \cdot e_i \frac{x_i}{y_i} + Y_{YX} e_i \frac{x_i}{y_i} \approx Y_{JE} \cdot e_i \frac{x_i}{y_i} + \varepsilon_{JI} \ , \tag{3.8}$$

де $\varepsilon_л$ - неточність оцінювання функції якості J_i і-го елемента.

Враховуючи формулу (3.3) можна вважати, що функція якості J_i і-го елемента залежить від ефективності перетворення входів x_i у виходи y_i причому ця ефективність визначається відповідним e_i . У багатьох випадках визначення ефектів перетворення e_i елементів системи безпеки є складним завданням, яке важко відобразити у вигляді функціональної залежності. Тому одним із шляхів вирішення цього завдання є використання логіко-математичного моделювання [61]. Такий підхід дозволить підвищити ступінь формалізації процесу вдосконалення безпеки. Оскільки ефект перетворення e_i по своїй суті визначає ступінь кореляції між x_i та y_i , то його логічно виражати у виді коефіцієнта кореляції [62].

Для моделі системи безпеки, представленої на рис. 3.3, вираз для функції якості, із врахуванням (3.2), (3.3), (3.8) матиме такий вигляд:

$$\begin{aligned} &J_{SQ} \xrightarrow{D \to opt} T_E \times J_E \cap T_R \times J_R + \varepsilon_{SQ}, \\ &J_E = \left\| T_{E-i} \right\|^{i=\overline{1,n}} \times \left\| e_{ij}^E \right\|_{j=\overline{1,m}}^{i=\overline{1,n}}, \\ &J_R = \left\| T_{R-i} \right\|^{i=\overline{1,n}} \times \left\| e_{ij}^R \right\|_{j=\overline{1,m}}^{i=\overline{1,n}} \end{aligned} \tag{3.9}$$

Таким чином для оцінювання ефективності безпеки та її окремих елементів доцільно застосовувати метод структурування їх функції якості.

3.2 Побудова алгоритму щодо ідентифікації ризиків СОТС згідно 31010

Процедура ідентифікації ризиків полягає у визначенні ймовірних подій, що несуть негативний вплив. Серед ефективних механізмів управління ризиками будь-якого процесу, зокрема і технологічного, є застосування міжнародного стандарту ДСТУ ISO 31010:2013 «Керування ризиком. Методи загального оцінювання ризику» [60]. Згідно з даним стандартом однією з початкових процедур аналізу й загального оцінювання ризиків є їх ідентифікація. Дана процедура є першим етапом для оцінювання ризиків. Вона базується на вивченні, усвідомленні й систематичному виявленні причин і джерел виникнення можливих небезпек та факторів (чинників), щодо їх негативного впливу на досліджуваний об'єкт. Згідно з вимогами стандарту [59] блок-схему ідентифікації ризиків СОТС наведено на рис. 3.5.

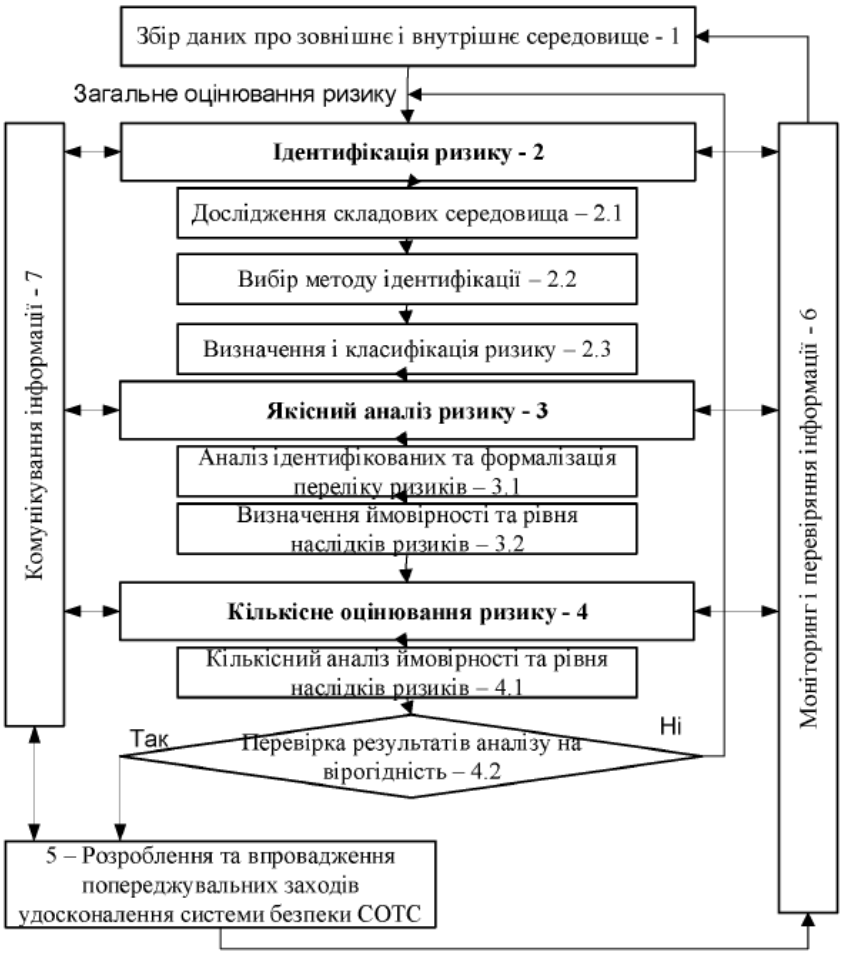

Рис. 3.5 Схема етапів ідентифікації ризиків згідно ДСТУ ISO 31010:2013

В ході дослідження було розроблено методику ідентифікації ризиків. Вона

складається з трьох етапів.

На першому етапі формується робоча група із залученням експертів та зацікавлених сторін. У роботах [61,62] наведено критерії щодо якісних та кількісних характеристик, яким повинні відповідати потенційні претенденти в експерти та алгоритм формування групи експертів. Основним завданням першого етапу є збір інформації стосовно СОТС, досконале вивчення матеріальних ресурсів, факторів впливу та організаційно-технічних чинників, що впливають на проведення процедур оцінювання та формування їх переліку.

На другому етапі проводиться документування ризиків, які впливають на безпеку процесу та обґрунтовуються найбільш суттєві фактори, що їх обумовлюють.

На третьому етапі для побудови типових організаційно-технічних заходів, щодо зменшення ризиків проводиться їх класифікація. У роботі [63 наведено основні вимоги до її проведення. Зокрема, це стосується використання трирівневого підходу, який дозволяє оцінити вплив пріоритетів верхніх рівнів на пріоритети нижніх рівнів та систематизувати ризики за їх ознаками.

Слід зазначити, що для поліпшення результатів кожен етап ідентифікації потребує постійної класифікації, тобто перевірки вірогідності отриманої інформації. Далі за результатами моніторингу, для СОТС слід розробити і впровадити запобіжні заходи щодо мінімізації негативного впливу ризиків та сформувати їх типовий реєстр, який включатиме перелік факторів, що обумовлюють ризики за ознаками, причини їх виникнення та типові заходи щодо їх зменшення. Такий підхід дозволяє підвищити якість оцінювання стану безпеки і сприяє підвищенню якості функціонування СОТС.

Для оцінки ризиків СОТС розроблено спеціальний чотирикроковий алгоритм, який дозволяє оцінювати ризики на всіх етапах його життєвого циклу. Механізм базується на системному підході, принципах загального управління якістю (TQM), управлінні ризиками та вимогах стандарту ДСТУ ISO 31010:2013. Практична реалізація цього алгоритму передбачає загальну оцінку

ризиків шляхом ідентифікації якісного аналізу та кількісного оцінювання [64]. Для цього застосовуються наступні методи: «Дослідження небезпек і працездатності», структурований метод «Що – якщо», метод «Аналізування видів і наслідків відмов», «Аналізування причин і наслідків», «Технічне обслуговування, зорієнтоване на забезпечення безвідмовності», а також показники ризику, матриця «наслідок-ймовірність» та багатокритеріальне аналізування рішень.

Вибір методу ідентифікації залежить від особливостей виробничого процесу та є прерогативою СОТС.

Загальне оцінювання ризиків (рис. 3.5) має чотири складові: 1 – збір даних про зовнішнє і внутрішнє середовище; 2 – ідентифікація ризиків; 3 – якісний аналіз ризиків; 4. – кількісне оцінювання ризику. Застосування даних процедур передбачає визначення впливу негативних факторів на СОТС, шляхом використання методів структурованого аналізу.

Стандарт [54] рекомендує для ідентифікації ризиків застосовувати 26 основних методів із 31 загальної кількості інструментів. Проте, повний набір для всіх етапів властивий лише 15 методам, з яких в ході досліджень було встановлено, що для СОТС найбільш придатними є чотири методи: «Аналізування видів і наслідків відмов», «Технічне обслуговування, зорієнтоване на забезпечення безвідмовності», матриця «наслідок-ймовірність» та багатокритеріальне аналізування рішень.

Розглянемо більш детально кожен з них.

Метод дослідження небезпек і працездатності (IEC61882 HAZOP) - якісний, достатньо складно структурований і призначений для стадії проєктування СОТС за умови високого рівня специфікації системи і високої вартості витрат. Спрощений альтернативний варіант HAZOP - це метод "Що - якщо", який застосовують на рівні систем за нижчого рівня докладності для дослідження наслідків змін та ризиків від них. Його перевагою є більш широка застосовність, швидше отримання оцінки за менших витрат. Проте він має досить високу ймовірність не вірної ідентифікації ризику або небезпеки.

Метод аналізування видів і наслідків відмов (IEC 60812 FMEA) - напівкількісний або кількісний за умови використання даних щодо фактичної інтенсивності відмов, як під час проєктування так після, в т.ч. для процесів і процедур. У випадку можливості прокласифікувати кожен з ідентифікованих видів відмов відповідно до його критичності (FMECA), застосовують з числом пріоритетності ризику (RPN) - напівкількісною мірою критичності, яку одержують шляхом множення чисел ранжувальних шкал (від 1 до 10), що відповідають наслідку відмови, на вірогідність відмови та спроможність виявити проблему. Якщо проблему важко виявити, то їй надають найвищий пріоритет.

Метод аналізування причин і наслідків поєднує у собі дерево відмов і дерево подій з розширенням функційності застосуванням хронології з часовими затримками. Допускається кількісне подання способів реагування системи, що стає оцінкою ймовірності різних можливих наслідків критичної події. Для цього спочатку встановлюють ймовірність кожного виходу блоку або стану, а потім проводять операції множення або додавання за схемою до кожного конкретного наслідку.

Метод керування відмовами технічне обслуговування, зорієнтоване на забезпечення безвідмовності (IEC 60300-3-11 RCM) реалізується шляхом виконання належного результативного технічного обслуговування. Він заснований на загальному оцінюванні ризику за типом FMECA, проте вимагає спеціального підходу до ідентифікації відмов устаткування.

Напівкількісною мірою ризику є показники ризику, що отримані з використанням підходу бальних оцінок на основі порядкових шкал. Оцінки застосовують до кожного складника ризику для їх порівняння. Якщо є всі дані про систему, то вони дозволяють привести до єдиної числової бальної оцінки низку чинників, які впливають на рівень ризику. Невизначеність може бути враховано шляхом аналізуванням чутливості параметрів та зміною оцінок для їх виявлення. При цьому можна ранжувати різні ризики та об'єднувати їх в бальну оцінку рівня ризику. Недоліком даного методу є хибне тлумачення і мала надійність шкал, у випадку коли немає базової моделі.

Для ранжування рівня ризику застосовують матрицю «наслідок-ймовірність». Зокрема, вона використовується для аналізу критичності у FMECA та для встановлення пріоритетів після застосування HAZOP. При цьому створенні шкали повинні охоплювати весь діапазон наслідків.

Метод багатокритеріальне аналізування рішень (MCDA) полягає в проведені ранжування за принципом переваги наявних варіантів. При цьому аналізування передбачає розроблення матриці варіантів і критеріїв, що ранжовані та агреговані для отримання загальної бальної оцінки кожного варіанта. До його переваг слід віднести: досить просту структуру для ефективного прийняття рішень і висновків. Проте він не надає переконливого чи однозначного результату.

Для визначення ймовірності та рівня наслідків ризиків щодо їх значущості використовується шкала-«низький», «незначний», «середній», «значний», «неприйнятний» (табл. 3.1).

Таблиця 3.1

Ранжування та встановлення класу безпеки СОТС

Значення індексу безпекового показника якості (БПЯ)	Клас безпеки за рівнем БПЯ	Рекомендовані заходи
1,0-0,8	А-повна відповідність БПЯ до вимог	Періодичний моніторинг БПЯ
0,6-0,8	В-незначна невідповідність БПЯ	Оцінювання відповідності системи безпеки СОТС за показниками результативності
0,4-0,6	С - середній рівень БПЯ	Аналіз БПЯ та оцінювання відповідності системи безпеки СОТС за показниками ефективності
0,2-0,4	D-значна невідповідність БПЯ	Мінімізація джерел небезпек та оцінювання відповідності системи безпеки СОТС за показниками ефективності та результативності
0,0-0,2	F - неприйнятний рівень БПЯ	Переформування системи безпеки СОТС та оцінювання її відповідності системі безпеки СОТС за показниками ефективності та результативності

Аналіз ризиків буде ефективним у випадку застосування напівкількісного

ранжування.

Найбільш розповсюдженими методами кількісного оцінювання є матриця наслідків-ймовірностей та картографування ризиків. Суть методу - матриця наслідків/ймовірностей полягає у поєднанні якісних та напівкількісних оцінок ймовірностей та наслідків що дозволяє проранжувати ризики та визначити їх рівень. Даний метод, як правило, застосовується для визначення пріоритетності аналізу ризиків [12]. Він базується на використанні спеціальних шкал, вибір яких обумовлюється діапазоном ймовірності та наслідків, які об'єднуються матрицею. При цьому найнижча ймовірність характеризує найбільш небезпечний ризик. До переваг даного методу слід віднести простоту застосування, а до недоліків труднощі однозначного визначення шкали для різних ризиків при різних категоріях наслідків.

Наступним підетапом загального оцінювання ризиків є перевірка результатів на вірогідність інформації - 4.2, якщо інформація достовірна то можна переходи на підетап - 5. Якщо інформація не достовірна, то перехід відбувається на підетап - 3.1. У разі, якщо якісного аналізу недостатньо, потрібно повернутись на підетап 2.1. До підетапу 4 входять процедури: розроблення (погодження та впровадження) плану дій щодо попереджувальних заходів удосконалення системи безпеки СОТС.

Таких чином застосування даного алгоритму дозволяє своєчасно виявляти ризики та розробляти організаційно-технічні заходи щодо підвищення безпеки складної організаційно-технічної системи.

3.3. Методика управління безпекою складної організаційно-технічної системи

Модель безпеки СОТС повинна охоплювати: вимоги до заходів безпеки та їх функцій; опис елементів безпеки СОТС, їх функцій та суттєвихвзаємозв'язків між ними; перелік критеріїв безпеки СОТС; зв'язок параметрів елементів із критеріями безпеки СОТС.

На рис. 3.6 наведено елементи системи оцінювання безпеки СОТС.

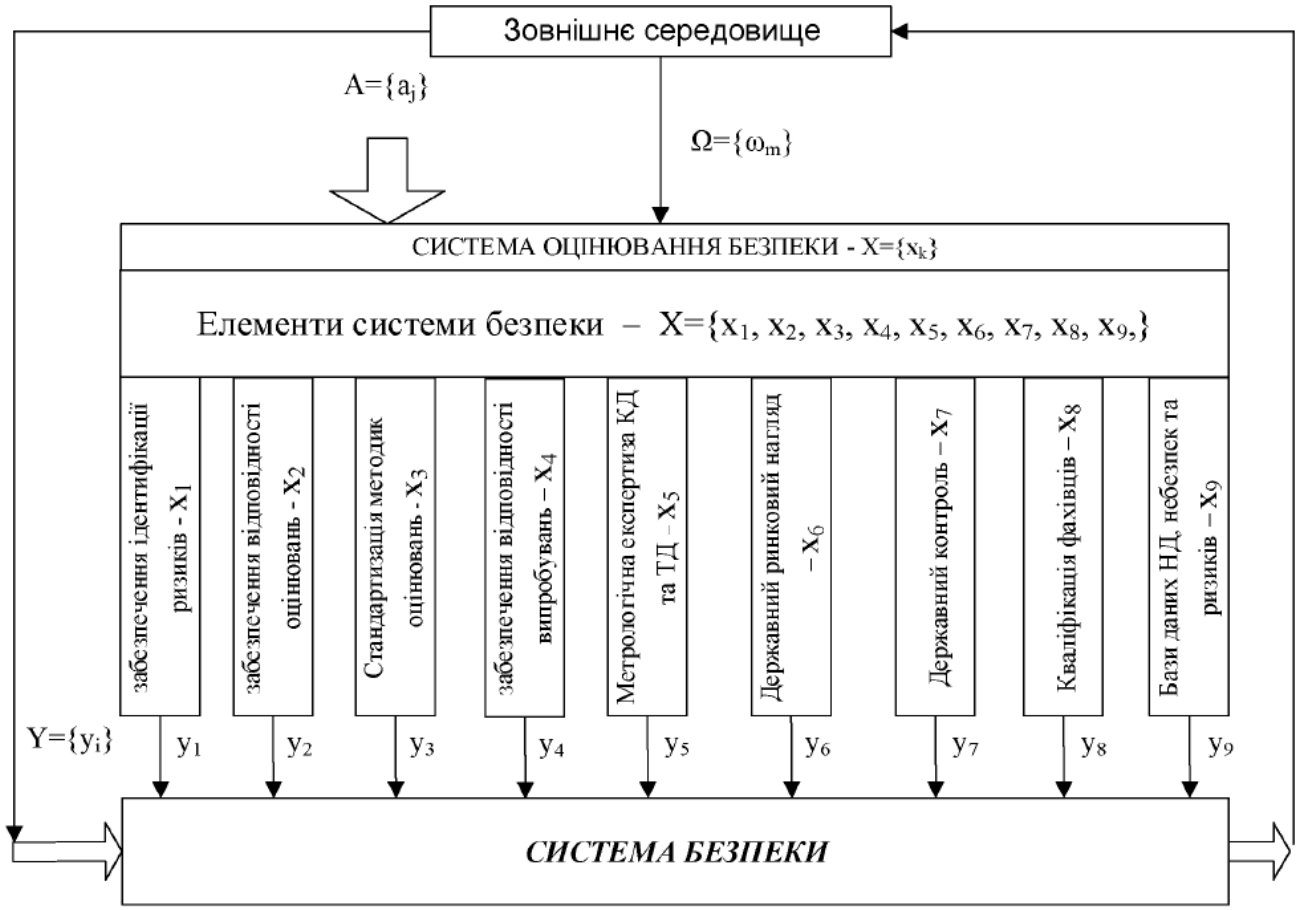

Рис 3.6 Елементи системи оцінювання безпеки СОТС

Формалізація моделі безпеки СОТС та процес оптимізації її структури відображено у вигляді (3.10). При цьому враховано такі обмеження: вплив зовнішнього середовища на СОТС може виходити за межі визначених параметрів; задача є багатокритеріальною і вимагає оптимізації векторного критерію ефективності; для визначення системи безпеки СОТС слід враховувати потенційні можливості її ресурсів для захисту від небезпек та обмеження, що накладаються на витрати з її вдосконалення.

$$SS_W \Rightarrow \begin{cases} Q = Q(x, y, a, \Omega, t) \to extr \\ a = \Phi_1(a^0, y, x, \Omega, t) \\ y = \Phi_2(a, y^0, x, \Omega, t) \\ a^0, a^1 \in A, i = \overline{1, n_A}; x \in X, i = \overline{1, n_X}; \\ y^0, y^1 \in Y, i = \overline{1, n_Y}; t \in R[t_0, t_1]; \\ \omega_i \in \Omega, i = \overline{1, n_\Omega} \to const \end{cases} \tag{3.10}$$

де Q - критерій оптимальності безпеки СОТС; Φ_1 (a^0, y, x, Ω, t) – оператор зміни вхідного показника безпеки СОТС А в залежності від інших впливових факторів та Φ_2(a, y ^{0}, x, Ω, t) – оператор зміни вихідного показника безпеки СОТС Y в залежності від інших впливових факторів; $a^0, a^1 \in A, i = \overline{1, n_A}; x \in X, i = \overline{1, n_X}, y^0, y^1 \in Y, i = \overline{1, n_Y}; t \in R[t_0, t_1]$ обмеження областей існування відповідних параметрів моделі безпеки СОТС.

У цій моделі множина вхідних змінних А={a_j} визначається сукупністю вимог до систем безпеки СОТС державного контролю та нагляду, встановлених у нормативно-правових актах, технічних регламентах та правилах, а також міжнародних нормативних документах та договорах. Множина вихідних змінних У={y_j} характеризує сукупність впливових факторів технологічного процесу на стан безпеки СОТС і визначається структурою СОТС та її діяльністю. Множина змінних Ω={ω_1} впливу зовнішнього середовища охоплює такі виливні фактори: фізичні параметри середовища (температура, вологість, тиск); зовнішні зв'язки та постачання тощо. Подані вище фактори a_i, ω_i, y_i, що впливають на ефективність СОТС, як правило, мають детерміновані впливи, які в межах одного підприємства не завжди доцільно, або і неможливо змінювати, а лише адаптуватися до них.

Для підвищення ефективності безпеки СОТС необхідно оптимізувати структуру та значення її внутрішніх елементів $g_i(X, A, \Omega) \le b_i, i = \overrightarrow{1, m}$ – функція втрат якості і˙-го елементу;

$$X^{opt} = \min g_X(x_k) \to \max_Y P_W$$

b_i - граничне значення функції втрат якості і-го елементу;

P_W - ймовірність досягнення мети заходами безпеки СОТС.

Для розрахунку операторів Φ_1 і Φ_2 згідно з GUM [19] методика оцінювання найкращого результату та його стандартної непевності u_A(x) за методом типу А складається з таких кроків:

1. Обчислити середнє значення (найкращого результату вимірювання):

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \quad ; \tag{3.11}$$

2. Обчислити оцінки дисперсії результатів спостережень:

$$s^2(x_i) = \frac{1}{n-1}\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2 \quad ; \tag{3.12}$$

3. Визначити експериментальну оцінку стандартного відхилення:

$$s(x_i) = \sqrt{s^2(x_i)} = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2} \tag{3.13}$$

4. Обчислити значення стандартної непевності типу А результату за невідомого стандартного відхилення спостережень за формулою (3.14), або за відомого стандартного відхилення за формулою (3.15):

$$u_A(x) = s(\bar{x}) = \frac{s(x_i)}{\sqrt{n}} = \sqrt{\frac{1}{n(n-1)}\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2} \quad ; \tag{3.14}$$

$$u_A(\bar{x}) = \frac{\sigma(x_i)}{\sqrt{n}} \quad ; \tag{3.15}$$

5. Обчислити кількість ступенів свободи: ν = n – 1;

6. Визначити розширену непевність:

$$U_p = t_p(\nu)\cdot u_A(x) \quad ; \tag{3.16}$$

де $t_p(\nu)$ - коефіцієнт розширення - квантиль розподілу Стьюдента; p - рівень довіри;

Відповідно до цього методу умова визначення найкращої оцінки параметра розташування $\hat{\mu}$ результатів спостереження і параметра ширини $\hat{\sigma}$ - розподілу вибірки дослідження (рис. 3.7):

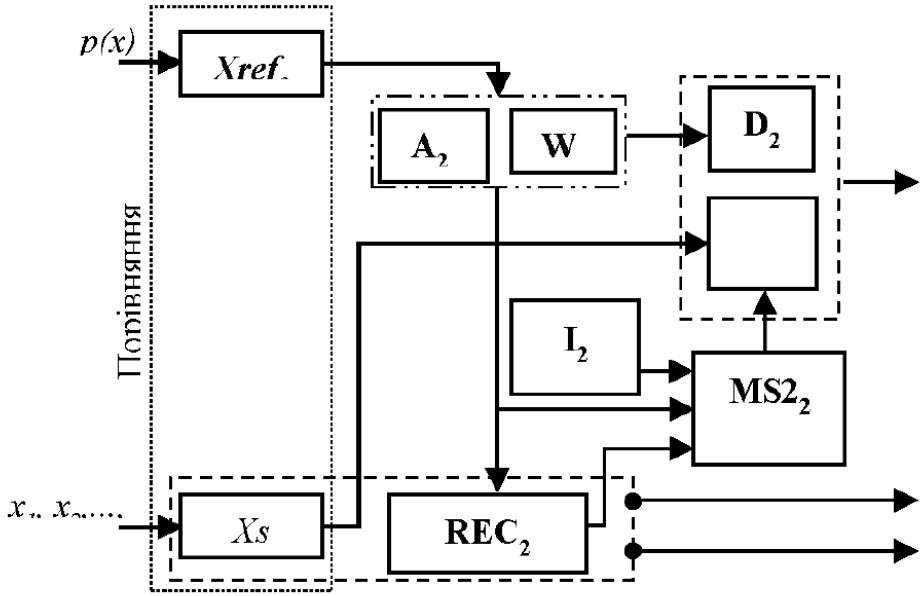

Рис. 3.7 Схема алгоритму опрацювання результатів оцінювань на основі методу порядкових статистик [23].

Порядок застосування алгоритму наступний:

1. Впорядкування спостережень X_s;

2. Вхідні відсортовані спостереження порівнюють не з однією послідовністю зразкових спостережень, а з набором j (j=1, 2,..., J) зразкових спостережень $xref_1=(xref_{1,1}, xref_{2,1},.., xref_{п,1})^T$, $xref_2=(xref_{1,2}, xref_{2,2},..,xref_{п,2})^T$,..., $xref_j=(xref_{1,j}, xref_{2,j},.., xref_{n,j})^T$, які відповідають передбачуваним густинам розподілу $p_1(x)$, $p_2(x)$, ... ,$P_J(x)$, (де $xref_{k,J}$ – зразкові спостереження, обчислюються за формулою $p_j(x)$ $(j=1, 2, \ldots, J)$

3. Для кожної моделі густини $p_J(x)$ (j=1, 2, ... , J) на основі зваженого методу найменших квадратів обчислюють найкращі оцінки параметрів $\hat{\mu}_j$ і $\hat{\sigma}_j$ і вхідних спостережень за формулою $(\hat{\mu}_j; \hat{\sigma}_j)^T = (A^T \cdot W \cdot A)^{-1} \cdot A \cdot W \cdot X_s = REC \cdot X_s$,з якої $REC = (A^T \cdot W \cdot A)^{-1} \cdot A^T \cdot W$.

4. Для кожної моделі густини $p_J(x)$ (j=1, 2, ... , J)) обчислюють незміщену оцінку дисперсії залишкових відхилень $S^2_{R,j}$ за формулою $S_R^2 = \frac{X_s^T \cdot W \cdot (I - A \cdot REC) \cdot X_s}{n-2}$.

5. Визначають для якого розподілу отримали мінімальне значення J = дисперсії залишкових відхилень $j = \min_j \left(S^2_{R,1}, S^2_{R,2},..., S^2_{R,J}\right)$.

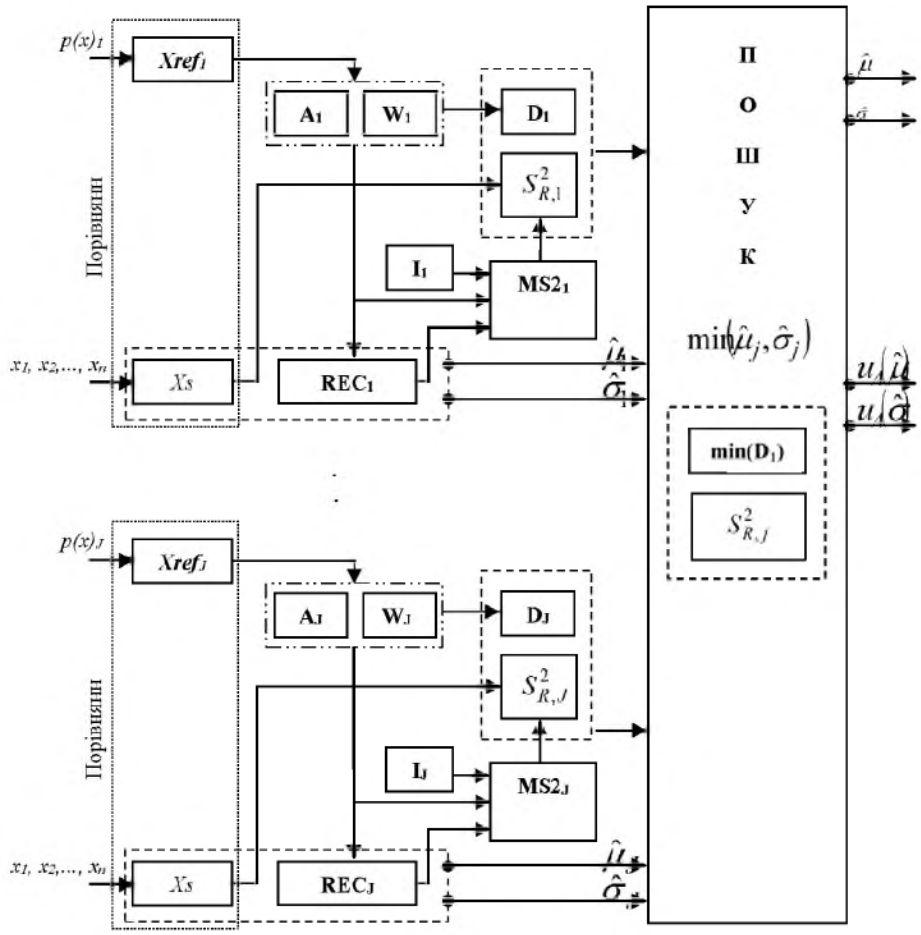

Рис 3.8 Структурна схема алгоритму опрацювання результатів оцінювань на основі методу порядкових статистик (порівняння впорядкованих спостережень з набором j зразкових)

6. За результат приймають значення для яких отримано мінімальні дисперсії параметрів $\hat{\mu} = \hat{\mu}_j$ і $\hat{\sigma} = \hat{\sigma}_j$.

7. Стандартні $u_A(\hat{\mu}_j)$ і $u_A(\hat{\sigma}_j)$і розширені $U_p(\hat{\mu}_j)$ і $U_p(\hat{\sigma}_j)$ непевності цих результатів обчислюють, як для звичайного методу порядкових статистик, підставляючи відповідну матрицю D_J та оцінку дисперсії $S^2_{R,j}$.

Метод Монте-Карло особливо ефективний у випадках, коли аналітичні методи обчислення непевності непридатні та неефективні внаслідок їх складності через величезний обсяг обчислень та занадто великий час на розв'язання задачі, а відповідні спрощення не забезпечують потрібної точності [98]. Оскільки метод Монте-Карло ймовірнісний, то важливо забезпечити статистичну стійкість результатів моделювання [65]. З цією метою обчислення

проводять з великої кількості реалізацій M . Якщо кількість симуляцій становить M, то стандартне відхилення (статистична нестабільність, непевність) досліджуваного параметру буде мати порядок $\sim 1/\sqrt{M}$. Тобто при $M = 10^4$ статистична нестабільність має порядок 1%, а при $M = 10^6$ статистична нестабільність має порядок 0,1%. Тому на практиці, при застосування методу Монте Карло, потрібно вибирати кількість статистичних симуляцій у методі Монте-Карло між 10^4 та 10^6.

Алгоритм опрацювання та оцінювання непевності результату вимірювання за симуляційним методом Монте-Карло полягає у виконанні процедур, що наведено на (рис. 3.9).

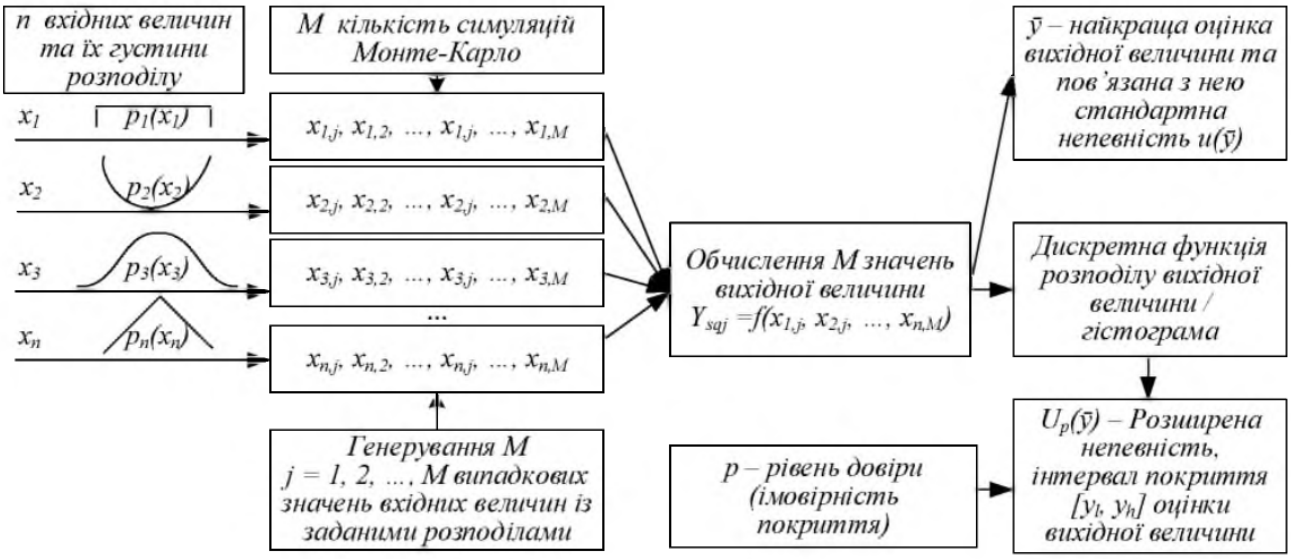

Рисунок 3.9 Загальна схема дослідження непевності результату оцінювання за методом Монте-Карло

Згідно даного алгоритму виконують наступні процедури:

1. Прийняття моделі густини розподілу ймовірності $p_1(x_1), p_2(x_2), p_3(x_3), ..., P_п(x_п)$ для кожної так званої вихідної випадкової величини $x_1, x_2, x_3, ..., x_n$ з параметрами математичного сподівання величини m_x та стандартним відхиленням σ_x;

2. Встановлення кількості спостережень *n*;

3. Присвоєння кількості реалізацій (симуляцій) *M* у ММК;

4. Генерування j = 1, 2,... , *M* випадкових значень кожної із вхідних величин із заданими розподілами та їх параметрами:

$$X = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,j} & \cdots & x_{1,M} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,j} & \cdots & x_{2,M} \\ x_{3,1} & x_{3,2} & \cdots & x_{3,j} & \cdots & x_{3,M} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,j} & \cdots & x_{n,M} \end{pmatrix}; \quad (3.17)$$

5. За основним рівнянням (моделлю) вимірювання $y = f(x_1, x_2, x_3 \ldots, x_п)$ для кожного M наборів згенерованих випадкових значень вхідних величин обчислюють значення вихідної величини $y_j = f(x_{1,J}, x_{2,J}, x_{3,J}, \ldots, x_n)$, $j = 1, 2, \ldots, M$;

6. Проведення обчислення та опрацювання отриманих результатів [116, 35]:

– середнього значення $\bar{y}$, яке використовують як найкращу оцінку шуканої величини $\hat{y} = \bar{y}$:

$$\bar{y} = \frac{1}{M}\sum_{j=1}^{M} y_j; \quad (3.18)$$

– оцінки стандартного відхилення s_y, яку використовують як стандартну непевність оцінки величини $u(\hat{y}) = s_y$:

$$s_y = \sqrt{\frac{1}{(M-1)}\sum_{j=1}^{M}\left(y_j - \bar{y}\right)^2}; \quad (3.19)$$

– сортування значень y_i вихідної величини ys_j за зростанням:

$$ys_j = sort\left(y_j\right); \quad (3.20)$$

– максимального max(y) та мінімального min(y) експериментального значення;

– побудова експериментальної функції розподілу $Fe_J(ys_j) = j/M$, за якою для заданого рівня довіри β визначають нижню $y_н$ та верхню $y_в$ границі інтервалу покриття оцінки результату:

$$y_н = ys_{\left[\frac{1-\beta}{2}M\right]}; \; y_в = ys_{\left[\frac{1+\beta}{2}M\right]}. \quad (3.21)$$

– побудова гістограм;

– стандартної та розширеної непевності результатів спостережень;

– оцінювання асиметрії (контрексцесу) та сплющеності (ексцесу) розподілу та визначення інших необхідних статистичних параметрів отриманих результатів.

Для довільної густини розподілу p(x) та функції розподілу F(x) випадкової величини x теоретична густина розподілу $p_l(x_1)$ мінімального елементу x_1 за відомих параметрів розподілу спостережень описується, як розподіл 1-ої порядкової статистики $p1(x_1) = n \cdot [1 - F(x_1)]^{n-1} \cdot p(x_1)$, максимального елементу x_n описується, як розподіл остатньої n-ої порядкової статистики $pn(x_n) = n \cdot F(x_n)^{n-1} \cdot p(x_n)$. [66].

Таким чином наведені вище методичні рекомендації та алгоритми дозволяють оцінити невизначеність факторів, що впливають на ризик і безпеку складних організаційно-технічних систем.

Висновки до третього розділу

1. Запропоновано безпеку СОТС розглядати у вигляді трьохрівняної ієрархічної системи, де перший рівень – це система безпеки, другий – це підсистеми забезпечення результативності та ефективності заходів безпеки, третій – елементи системи (ідентифікація, оцінювання, методики, метрологічна експертиза тощо).

2. Розроблено алгоритм ідентифікації ризиків в основу якого покладено вимоги стандарту ДСТУ ISO 31010. Алгоритм складається з трьох етапів і дозволяє визначати ризики у форматі життєвого циклу складної організаційно-технічної системи. Для визначення ризиків застосовують якісні та кількісні методи, що наведені в стандарті ДСТУ ISO 31010.

3. Запропоновано методику управління безпекою, яка включає вимоги до заходів безпеки та їх функції, елементи та критерії безпеки і дозволяє шляхом застосування методів порядкових статистик визначати невпевненості результатів обчислень, щодо потенційних ризиків та безпеки складної організаційно-технічної системи.

ЗАГАЛЬНІ ВИСНОВКИ

1. Проаналізовано існуючі поняття щодо «ризику» і визначено, що для СОТС найбільш придатним є поняття згідно стандарту ISO 31000. В даному стандарті ризик – це результат невизначеності завдань, де невизначеність охоплює події, які можуть відбутися і можуть не відбутися, при цьому невизначеність обумовлена неясністю чи нестачою інформації.

2. Нормування ризиків являє собою затвердження норм техногенної та природної безпеки, правил та регламентів діяльності національної економіки. Воно є тим засобом, який повинен забезпечити єдність методологічних підходів щодо оцінювання ризиків та уніфікацію методів їх нормування.

3. Методи аналізу ризику поділяються на детерміновані, ймовірнесно-статистичні, комбіновані та ті що застосовуються в умовах невизначеності нестохастичної природи. Вибір методу залежить від об’єкту досліджень, його життєвого циклу, умов виробництва та експлуатації. Для СОТС застосовуються як якісні, так і кількісні методи оцінювання ризиків.

4. Доведено, що СОТС являє собою ієрархічну систему, яка утворена множиною елементарних організаційно-технічних систем. При цьому організаційна складова системи охоплює спосіб взаємозв’язку і взаємодії між елементами СОТС, а технічна складова – це матеріальні засоби виробництва, комунікації тощо.

5. Безпека СОТС – це стан, при якому ризик виникнення небезпек і спричинення ними шкідливих наслідків знаходиться на прийнятому рівні. Вона характеризується такими властивостями як економічність та ефективність.

6. Для оцінювання і управління ризиками СОТС запропоновано застосовувати ризик-орієнтованих підхід, який дозволяє проводити перевірку аналізу ризиків та передбачає наявність зворотного зв’язку.

7. Запропоновано для визначення джерел ризику застосовувати схему валідації ймовірнісного аналізу ризику на основі застосування експертних методів.

Такий підхід дозволяє оцінити структуру, зміст, дискретизацію та параметризацію ризиків СОТС.

8. Небезпека СОТС вимірюється за ймовірністю відмови будь-якого її елемента. При цьому наслідки можуть мати як якісні, так і кількісні характеристики важливості.

9. Для підвищення рівня безпеки СОТС доцільно застосовувати ряд міжнародних стандартів, зокрема ISO 9001, ISO 18091, ISO 37110, ISO 22301 тощо.

10. Життєвий цикл безпеки згідно зі стандартами IEC являє собою циклічний процес або замкнуту петлю, що включає в себе циклічний спосіб підтвердження та аналізу ризику за стандартом ISO 31010.

11. Запропоновано алгоритм оцінювання ризиків, який складається з чотирьох основних процедур: збір даних про внутрішнє та зовнішнє середовище, ідентифікація ризиків, якісний аналіз ризиків, кількісне оцінювання ризику. В основу алгоритму покладено вимоги ISO 31010.

12. Для визначення невпевненості результатів оцінювання запропоновано застосовувати метод Монте Карло. Це дозволяє скоротити час обчислень та отримати більш точні результати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Березуцький В.В., Адаменко М.І. Небезпечні виробничі ризики та надійність: навчальний посібник-Харків: НТУ «ХІП», 2016. -385 с.

2. Бобало Ю.Я. Математичні моделі та методи аналізу електронних кіл: навч. Посібник/ за ред. д-ра техн. наук, проф. Ю.Я. Бобала та д-ра техн. наук, проф. Б.А. Мандзія. Львів: Видавництво Львівської політехніки, 2013. 320 с.

3. Братченко Г. Д., та ін. Методи та засоби обробки сигналів. Навчальний посібник. Одеса: «Плутон», 2014. 452 с.

4. Агафонов В. Системнь1е принципь1 стратегического планирования. Кластернь1й подход. М.: PalmariumAcademic Publishing, 2014. 572 с.

5. Василевський О.М., Поджаренко В.О. Нормування показників надійності технічних засобів: навчальний посібник- Вінниця: ВНТУ, 2010. 129 с.

6. Головко Д.Б., Скрипник Ю.О. Методи та засоби частотно-дисперсійного аналізу речовин та матеріалів: фізичні основи. К.: ФАДА, ШД, 2000. 200с.

7. ISO Guide 73:2009 Risk management – Vocabulary – базовий словник термінів ризик-менеджменту (визначаються поняття ризику та його особливостей, розглядаються такі поняття, як менеджмент ризиків, політика і план менеджменту тощо).

8. ISO 31000: 2018 Risk management — Guidelines – wей документ призначений для використання людьми, які створюють і захищають цінність в організаціях, керуючи ризиками, приймаючи рішення, встановлюючи та досягаючи цілей та покращуючи ефективність.

9. IEC 31010:2019 Risk management — Risk assessment techniques – є керівництвом до вибору методів оцінки ризику залежно від етапу розвиткупроекту або від типу аналізу.

10. Закон україни про об’єкти підвищеної небезпеки *(відомості верховної ради України (ввр), 2001, № 15, ст.73)*

11. Кабінет міністрів україни постанова від 11 липня 2002 р. n 956 Київ

12. Міністерство праці та соціальної політики україни наказ 04.12.2002 № 637

13. IEC 60812:2018 Failure modes and effects analysis (FMEA and FMECA) – Режим доступу: https://webstore.iec.ch/publication/26359.

14. Дорожовець М. Опрацювання результатів вимірювань: навч. посіб. Нац. ун-т «Львів. політехніка». Львів: Львівська політехніка, 2007. 623 с.

15. Дорожовець М., Стадник Б. Метрологія та вимірювання: навч. посіб [М. Дорожовець, Р. Івах, В. Мотало та ін.]; за наук. ред.: Б. І. Стадник, Львів: Вид- во Львів. політехніки, 2012. 312 с.

16. Зберігаючи енергію - зберігаємо майбутнє. Путівник з енергоефективності. - Івано-Франківськ: Агентство з розвитку приватної ініціативи, 2015 - 112 с.

17. Кулєшов М.М., Уваров Ю.В., Олійник О.Л., Пустомельник В.П., Бєліков А.С. Пожежна безпека будівель та споруд: навчальний посібник. Харків, 2004. 271 с.

18. Куць В. Р. Розвиток нормативної бази з оцінювання якості продукції: автореф.дис... канд. техн. наук: 05.01.02; Нац. ун-т "Львівська політехніка". Л., 2006. 20с.

19. Куць В.Р., Столярчук П.Г., Друзюк В.М. Кваліметрія: навч. посібник, Львів: Видавництво Львівської політехніки, 2012. - 256 с.

20. Ловейкін В.С., Ромасевич Ю.О. Теорія технічних систем, К.: ЦП ,,КОМПРИНТ", 2017. 291 с.

21. Мельник Ю. Ф., Новиков В. М., Школьник Л. С. Основи управління безпечністю харчових продуктів. Навчальний посібник. К.: Вид-во Союзу споживачів України, 2007. 297 с.

22. Микийчук М. М. Метрологічне забезпечення якості продукції на етап виготовлення. Монографія, вид-во Черемош, 2014. -265 с.

23. Микийчук М. М. Метод розгортання функції якості метролопчного забезпечення виробництва, *Вісник Нац. Ун-ту "Львівська політехніка". Сер. : Автоматика, вимірювання та керування.* 2013. № 753. С. 20-25

24. Бегун В. В. Вероятностный анализ безопасности атомных станций (ВАБ) / [В. В. Бегун, О. В. Горбунов, И. Н. Каденко и др.]. – Київ : НТУУ «КПИ», 2000. – 568

с.

25. Михайлюк О.П., Олійник В.В., Михайлюк А.О. Ідентифікація об'єктів підвищеної небезпеки: навч. посібник. Х.: УЦЗУ. 2007. 190 с.

26. Основи метрології та вимірювальної техніки: [підручник для вузів у двох томах]/ [М. Дорожовець, В. Мотало, Б. Стадник та ін.]; За ред. професора Б.І. Стадника. -Львів: Вид-во Національного університету "Львівська політехніка". 2005. ТІ. Основи метрології. 532 с.; Т2. Вимірювальна техніка. 656 с.

27. Походило Є. В., Столярчук П. Г. Імітансний контроль якості: монографія, Львів: Видавництво Львівської політехніки, 2012. 164 с.

28. Сікора Л. С. Когнітивні моделі та логіка оперативного управління в ієрархічних інтегрованих системах в умовах ризику Львів: ЦСД «ЕБТЕС», 2009. 432 с.

29. Теоретичні основи формування та деградації складних організаційно-технічних систем : монографія/ Є.Б. Смірнов, В.І. Ткаченко, І.В. Рубан, В.Г. Малюга, А.В. Тристан. Харків : ХНУРЕ, 2018. 162 с.

30. Управління якістю. Сертифікація: Навчальний посібник / Р.В.Бичківський, П.Г.Столярчук, Л.І.Сопільник, О.О.Калинський. К.: Школа, 2005. 432 с.

31. Бондар О. В. Ситуаційний менеджмент: Навч. посіб. — К. : Центр учбової літератури, 2010. — 326 с.

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

33. Прокопенко Т. О. Теорія систем та прийняття управлінських рішень : навч. посіб. / Т. О. Прокопенко ; М-во освіти і науки України, Черкас. держ. технол. ун-т. – Черкаси : ЧДТУ, 2018. – 187 с.

34. Прокопенко Т. О. Інформаційні технології управління організаційно-технологічними системами : монографія / Т. О. Прокопенко, А. П. Ладанюк. – Черкаси : Вертикаль, вид. Кандич С.Г., 2015. – 224 с.

35. Згуровський М. З. Основи системного аналізу / М. З. Згуровський, Н. Д.

Панкратова. – К. : Вид. група BHV, 2007. – 546 с.

36. Ладанюк А. П. Основи системного аналізу : навч. посіб. / А. П. Ладанюк. – Вінниця : Нова книга, 2004. – 176 с.

37. ISO 9001:2015 Системи управління якістю. Вимоги.

38. ISO 18091:2019 Системи управління якістю. Керівництво по застосуванню ISO 9001 в органах місцевого самоврядування.

39. ISO 37120:2018 Сталі міста та громади. Показники міської служби та якості життя.

40. ISO 31000 Управління ризиками. Керівні принципи.

41. IEC 31010 Керування ризиком. Методи загального оцінювання ризиків

42. ISO 22301:2012 Безпека суспільства. Системи менеджменту. неперервюстю діяльності. Вимоги.

43. ISO 20121:2012 Системи управління стійкістю подій. Керівництво для використання

44. ДСТУ ISO/IEC 25000:2016 Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE).

45. Хаген Граф. Создание веб-сайтов с помощью Joomla! 1.5. – Изд. дом «Вильямс», 2009. – 312 с.

46. Хубка В. Теория технических систем ; пер. с нем. / В. Хубка. – 2-е изд. – М. : Мир, 1987. – 208 с.

47. Александров Л. В. Системный анализ при создании и освоении объектов техники / Л. В. Александров, Н. П. Шепелев. – М. : НПО «Поиск», 1992. – 88 с.

48. Малин А. С. Исследование систем управления / А. С. Малин, В. И. Мухин. – М. : Изд. дом ГУ ВШЭ, 2004. – 400 с.

49. Кириллов Н. П. Признаки класса и определение понятия « технические системы» / Н. П. Кириллов // Авиакосмическое приборостроение. – 2009. – No 8. – С. 32–38.

50. Лавинский Г. В. Построение и функционирование сложных систем управления / Г. В. Лавинский. – К. : Выща шк., 1989. – 336 с.

51. Новиков Д. А. Теория управления организационными системами / Д. А.

Новиков. – М. : МПСИ, 2005. – 584 с.

52. Новиков Д. А. Современные проблемы теории управления организационными системами / Д. А. Новиков // Человеческий фактор в управлении / под ред. Н. А. Абрамовой, К. С. Гинсберга, Д. А. Новикова. – М. : КомКнига, 2006. – С. 391–407.

53. Антонов А.В. Системный анализ. – М.: Высшая школа, 2004. – 454 с.

54. ДСТУ EN 61508-6:2019 Функційна безпечність електричних, електронних, програмованих електронних систем, пов’язаних із безпекою. частина 6. настанови щодо використання IEC 61508-2 та IEC 61508-3 (EN 61508-6:2010, IDT; IEC 61508-6:2010, IDT)

55. IEC 61511-1 functional safety – safety instrumented systems for the process industry sector – part 1: framework, definitions, system, hardware and application programming requirements

56. ISA 84, instrumented systems to achieve functional safety in the process industries

57. Волкова В.Н., Денисов А.А. Теория систем: Учебник для студентов вузов. – М.: Высшая школа, 2006. – 511 с.

58. Гайдес М.А., Общая теория систем (системы и системный анализ). –Винница: Глобус-пресс, 2005. – 201 с.

59. Дудник І. М. Вступ до загальної теорії систем. - К.: Кондор, 2009. – 205 с. Лесечко М.Д. Основи системного підходу: теорія, методологія, практика: Навч. посіб. – Львів: ЛРІДУ УАДУ, 2002. – 300 с.

60. Системологія на транспорті: Підручник: У 5 кн. / За заг. ред. М. Ф. Дмитриченка. К.: Знання України, 2005 – Кн. 1: Основи теорії систем і управління – 344с.

61. Сурмін Ю.П. Аналітична діяльність: Посібник для аналітика неприбуткової організації. – К.: Центр інновацій та розвитку, 2002. – 96 с.

62. Сурмин Ю.П. Теория систем и системний анализ. Учеб. пособис. — К.: МАУП, 2003. – 368 с.

63. Орлов П.І., Луганський О.М. Інформаційні системи та технології в управлінні, освіті, бібліотечній справі: Наук.-практ. посіб. – Донецьк: Альфа-прес,

2004. – 292 с.

64. Чорней Н. Б. Теорія систем і системний аналіз: Навч. посіб. для студ. вищ. навч. закл. – К.: МАУП, 2005. – 256с.

65. Шершньова З.Є. Антикризове управління підприємством : Навч. посібник / В.О. Василенко. – К.: ЦУЛ, 2003. – 504 с

ДОДАТКИ

Міністерство освіти і науки України

Київський національний університет технологій та дизайну

МЕХАТРОННІ СИСТЕМИ: ІННОВАЦІЇ ТА ІНЖИНІРИНГ

ТЕЗИ ДОПОВІДЕЙ

V МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

4 листопада 2021

MSIE 2021

Київ 2021

Міністерство освіти і науки України

Київський національний університет
технологій та дизайну

МЕХАТРОННІ СИСТЕМИ: ІННОВАЦІЇ ТА ІНЖИНІРИНГ

ТЕЗИ ДОПОВІДЕЙ V МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

4 листопада 2021

Рекомендовано Вченою радою
факультету мехатроніки та комп'ютерних технологій
Київського національного університету технологій та дизайну

КИЇВ 2021

УДК 001.891(100)(106)
М 55

Організатори:
Міністерство освіти і науки України
Київський національний університет технологій та дизайну

Рекомендовано Вченою радою
факультету мехатроніки та комп'ютерних технологій
Київського національного університету технологій та дизайну
(Протокол від 22 жовтня 2021 р. №3)

М 55 Мехатронні системи: інновації та інжиніринг : тези доповідей V Міжнародної науково-практичної конференції, 4 листопада 2021 р. Київ : КНУТД, 2021. 260 с.
ISBN 978-617-7506-85-9

У виданні зібрано тези доповідей конференції, що присвячені проблемам в галузі мехатронних систем: інновацій та інжинірингу.

Матеріали подано в авторській редакції

УДК 001.891(100)(106)

ISBN 978-617-7506-85-9

УДК 006.86

ОЦІНЮВАННЯ РИЗИКІВ СКЛАДНИХ ОБ'ЄКТІВ ЗА ВИМОГАМИ МІЖНАРОДНИХ СТАНДАРТІВ

Г.І. Хімічева, доктор технічних наук, професор
Київський національний університет технологій та дизайну
В.І. Сович, магістрант
Київський національний університет технологій та дизайну

Ключові слова: технічні об'єкти, методи оцінювання ризику, міжнародні стандарти, фактори ризику, аналіз ризиків

У стратегії ISO 2021-2030 досить велика увага приділяється стандартам, які забезпечують оцінювання ризиків будь-якої продукції у т.ч. і складних технічних об'єктів. Міжнародною організацією зі стандартизації для прогнозування та запобігання ризиків розроблена ціла серія міжнародних стандартів ISO 31000.

Одним з найбільш затребованих є стандарт ДСТУ IEC/ISO 31010:2013 «Керування ризиком. Методи загального оцінювання ризику». Даний стандарт є універсальним, передбачає логічні, науково-обґрунтовані підходи щодо оцінювання ризиків та дозволяє приймати ефективні рішення в умовах невизначеності. Його процедури щодо загального оцінювання ризику спрямовані на більш точне та повне розкриття сутті впливу ризику на досягнення цілі, отримання більш повної інформації про ризик та його вплив, ідентифікування факторів, що викликають ризики, вибір інструментів та механізмів щодо оброблення ризику. Для ідентифікації ризику Додаток В даного стандарту пропонує застосовувати 15 методів. Методи обираються з урахуванням специфіки об'єкту дослідження.

На практиці для складних технічних об'єктів досить часто застосовують два наступних методи. Це метод «Мозкового штурму» та метод «Аналіз небезпечних чинників і критичні точки контролю».

Перший базується на висловлюваних ідеях всіх учасників експертної групи. Суть даного методу полягає в тому, що в результаті групового обговорювання визначаються фактори, що спричиняють ризики та формується їх перелік. Другий метод дозволяє ідентифікувати небезпечні фактори та запроваджувати засоби контролю з метою запобіганню їх впливу. Це в свою чергу підвищує якість, надійність та безпечність складного технічного виробу.

Слід зазначити, що технічне регулювання базується на методології оцінки ризиків продукції. Механізм оцінки ризиків достатньо визначений. Початку оцінки передує виявлення принципово-можливих визначених ризиків та збір даних про їх рівень і наслідки до яких вони можуть привести. Далі визначають вірогідність відповідних подій і пов'язаний з ним потенційний збиток.

Існує досить багато методів, щодо оцінювання ризиків. Одними із найбільш відомих методів є аналіз дерева відмов (FTA) і дослідження небезпеки та працездатності (HAZOP).

Метод аналізу видів та наслідків відмов (FMEA) є переважно якісним методом. В основу цього методу покладено аналіз кожного основного елементу складного технічного об’єкту на предмет того, яким чином він досягає аварійного стану і як це впливає на аварійний стан об’єкта вцілому.

Метод HAZOP, як правило використовується на етапі планування. Він являє собою процедуру ідентифікації можливих небезпек по всьому об’єкту вцілому. Це особливо важливо при ідентифікації непередбачених небезпек, що закладені в об’єкті у наслідок недоліку інформації при розробці або небезпек, що виявлені в існуючих об’єктах через відхилення в процесі їх функціонування. Перевагами його є те, що він дозволяє визначати небезпеки, шляхом аналізу майбутніх конструкцій та визначення рівня можливих їх відхилень від номіналу. На практиці даний метод застосовується шляхом створення мультидисциплінарної команди з 5-6 аналітиків. Ця команда спочатку визначає різні сценарії, які можуть призвести до небезпеки складного технічного об’єкту в процесі експлуатації, а потім визначає та аналізує їх причини та наслідки.

В ході дослідження та оцінювання ризиків потрібно аналізувати такі основні елементи, як концепція ризику, перспектива ризику, невизначеність, неоднозначність та складність. Наприклад, якщо існує невизначеність даних, то причинно-наслідкове формулювання потрібно описувати та оцінювати за допомогою імовірнісних методів, зокрема у вигляді марковських процесів.

Для оцінки таких факторів ризику, як безпека доцільно використовувати методи кількісної оцінки ризику (QRA), аналіз дерева подій (ETA), матриця ризиків (RMA), підхід на основі показників (IBA) тощо. Одним із ефективних методів оцінки факторів ризику є метод моделювання структурних рівнянь, що дозволяє оцінити складні моделі причинно-наслідкових зв'язків із прихованими змінними.

У стандарті IEC 60812:2018 наведено рейтинг критичності, щодо ступеню тяжкості наслідків режимів відмов технологій, обладнання, програмного забезпечення. Особливістю даного документу є те що режими відмов можна вистроїти в ряд пріоритетності, тобто приймати рішення щодо їх підтримки виходячи з даного ряду.

Список використаних джерел

1. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT)

2. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT)

3. EN IEC 60812:2018 (Main) Failure modes and effects analysis (FMEA and FMECA).